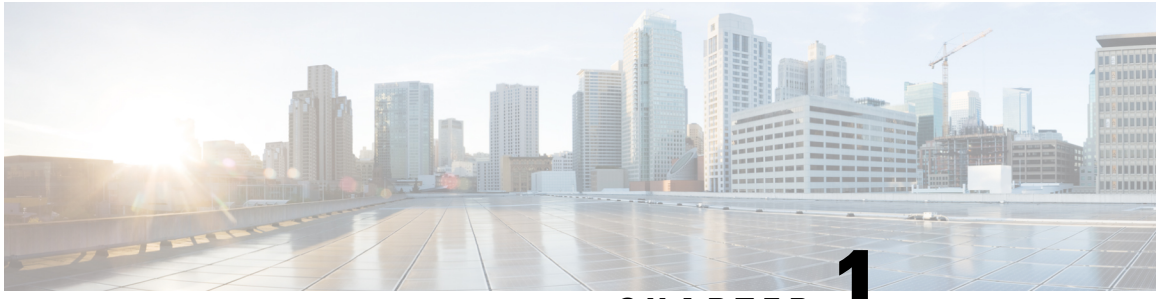
Cisco Prime Collaboration Provisioning Guide - Standard and Advanced, 12.6SU1

First Published: 2019-10-10

Last Modified: 2021-04-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Prime Collaboration Provisioning Overview

Cisco Prime Collaboration Provisioning Overview

This document provides information on features of Cisco Prime Collaboration 12.6SU1 .

Cisco Prime Collaboration Provisioning provides a scalable web-based solution to manage next-generation communication services. Cisco Prime Collaboration Provisioning manages IP communication endpoints and services in an integrated IP telephony, video, voicemail, and unified messaging environment that includes Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Unity (not applicable for Cisco Prime Collaboration 11.0 and later versions), Cisco Unity Express, Cisco Unity Connection systems, and analog gateways.

Note

- Throughout this document, any reference to Cisco Unified Communications Manager can also be understood to refer to Cisco Unified Communications Manager, unless explicitly noted.
- Video provisioning is supported for endpoints that are registered to Cisco Unified Communications Manager only. Cisco Prime Collaboration Provisioning does not support video endpoints that are registered to Video Communication Server (VCS).

Cisco Prime Collaboration Provisioning provides the following features:

- Provisioning for initial deployments and implementations, and then remains deployed to provide ongoing operational provisioning and activation services for individual users.
- A single, consolidated view of users across the organization. It provides a set of business-level management abstractions, which is policy-driven by using automation, for managing user services across the Cisco Unified Communications applications.

- Template capability, which permits defining standard configurations that can be reused for new sites or location deployments. Batch provisioning permits the rollout of large numbers of users at the same time.
- Administrators can configure policy at various levels to determine who can do delegated management, for whom that delegation applies, how business-level services apply to Cisco Collaboration Systems, and which types of users are permitted to order which standard services.

  By using this policy and standard configuration approach, you can provision and activate user services easily. At the same time, it retains the overall ability to manage and provide services that use the underlying Cisco Unified Communications applications.

Refer Cisco Prime Collaboration 12.X Data Sheet for more details on the features and benefits of Cisco Prime Collaboration Provisioning.

Cisco Prime Collaboration Provisioning allows ordering of standard services such as an endpoint, line, or voice mail for a user. You can also order Cisco Jabber Services for Tablet, Desktop, Android, BlackBerry, and iPhone. Cisco Prime Collaboration Provisioning processes all changes to the underlying Cisco Unified Communications applications as service requests or orders.

Cisco Prime Collaboration Provisioning creates an order to make a user-level change (to an endpoint, a line, and so on), or an IP communications-level infrastructure change (such as provisioning a new calling search space or route pattern). All orders in the system are tracked and viewable, both across orders and by username or ID. The order records show who initiated the order, the times of various process steps, and what the order contained.

Cisco Prime Collaboration Provisioning allows delegation of the order management capability so that requests for service additions, changes, or deletions are done without requiring an underlying knowledge of the voice applications that are delivering those services. Cisco Prime Collaboration Provisioning provides the same service management experience, regardless of the technology delivering the Cisco Unified Communications services.

Common Terminologies in Cisco Prime Collaboration Provisioning

- Device—Includes all applications such as Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Instant Messaging and Presence (IM&P), and Cisco Unity Connection. Also includes infrastructure components such as ISR Gateway devices, Cisco IOS Router.

  Processor—A proxy for each instance of a device.

  - A Call Processor is a proxy for each instance of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express.
  - A Unified Message Processor is a proxy for each instance of Cisco Unity (not applicable for Cisco Prime Collaboration 11.0 and later versions), Cisco Unity Express, and Cisco Unity Connection.
  - A Unified Presence Processor is a proxy for each instance of IM and Presence.

- Endpoint—Includes all active software and hardware voice, video, and collaboration devices with which the users interact. For example, phones (99xx, 88xx, 79xx, 78xx), tablets, Telepresence devices, Cisco Jabber clients, personal Telepresence units (DX series, EX series, MX series, SX series), mobile devices running Cisco Jabber, and so on.
- User—A person for whom an active IP Telephony service has been enabled. A user in Prime Collaboration Provisioning also represents an entity that can access Prime Collaboration Provisioning to perform various activities.

- Service—Service is the settings and integration needed to perform a series of functions expected by the user. For example, providing an endpoint service implies that the user will be able to perform dial out, ring, allow answering, have speed dials, forward to voicemail, transfer, conference and so on.
- Domains—Domains are groupings of users. One or more system users can be authorized to manage services for users within the Domain. In addition, rules or policies may be set on a Domain; those rules and policies will apply to services for users in that Domain. Common policies can also be applied on operations within a Domain. A domain administrator handles moves, adds, changes, and deletes (MACD) for users in that domain. Advanced Provisioning supports assigning individual administrators to individual groups.
- Service Areas—Service Areas are groupings within a Domain that are used to structure and manage the required IP telephony and messaging services across geographic, organizational, or technological boundaries. The Service Area typically acts as a service offering location, or site, and provides a template mechanism that determines provisioning attribute values used during order processing. A Service Area also handles Cisco Unified CM partitioning and class of service by directing which location, device pool and route partition assignments to use for any user provisioned into that Service Area.
- User roles—User roles provide policy enforcement, controlling which products and services are allowed to be ordered for different types of users such as contractors, executives or sales persons. They are also used in a filtering process that controls what choices are presented to order administrators at order time. The User Role setup also determines what services are ordered and which service templates are applied for a given user type during the Automatic Service Provisioning process. An administrator may create many User Roles to define different levels of services. The default user roles are: Employee, Executive and Room.
- Service Templates—Service Templates are a convenience for administrators setting up devices or ordering services for an end-user. Service Templates allow small or large amounts of settings to be collected into a single template which can be applied to endpoints or services. This saves time over setting many individual attributes and provides accuracy to prevent missed attributes or typos in attribute fields. Service Templates can leverage keywords and keyword truncation to customize line text displayed on endpoints. Service Templates contain provisioning attributes for a service and enables you to configure service attribute settings using provisioning attributes. Provisioning attributes are configuration settings that are applied to a service during activation.

Change History

The following table describes the information that has been added or changed in the Cisco Prime Collaboration Provisioning Guide - Standard and Advanced, 12.6 SU1.

Table 1: Change History

Release/Modified Date	First Customer Shipment (FCS)/Service Pack(s) (SP)
07- APRIL-2021	SU1 - Republished. Included the changes to Unity Connection OS Administration username and pssword. Unity Connection OS Administration username and password is the proxy username and password.

What's New in Cisco Prime Collaboration Provisioning 12.6SU1

Table 2: What's New in Cisco Prime Collaboration Provisioning 12.6SU1

Feature Name	Description

Support for Cisco Unified Communications Manager endpoints and Analog Voice Gateways.	The following Cisco Unified Communications Manager endpoints are supported:
	• Cisco Unified Communications Manager Release 11.5, 12.0, and 12.5:
	  • Cisco 8832NR
	  • Cisco 8865NR
	  • Cisco ATA 191
	  • Cisco Webex Room 70 Single G2
	  • Cisco Webex Room 70 Dual G2
	  • Cisco Webex Room 55 Dual
	  • Cisco Webex Room Kit Mini
	  • Cisco Webex Room Kit Pro
	• Cisco Unified Communications Manager Release 10.5, 11.0, 11.5, 12.0, and 12.5:
	  • Ascom IP-DECT
	
	The following Cisco Unified Communications Manager Analog Voice Gateway is supported:
	• Cisco Unified Communications Manager Release 11.5, 12.0, and 12.5:
	  • VG450
	
	Where Documented:
	Supported_Devices_for_Cisco_Prime_Collaboration_Provisioning-12.6SU1 document.

Export Service Template	Allows admin users and users with add, edit, delete, and export domains access to export a configured domain along with the service template into a batch file. **Where Documented:** Exporting a Domain, on page 91

Feature Name	Description
Global Search Enhancement	The following options are added to the global search drop-down list: • DN Description • Phone Description • VM Alias Name • EM Name **Where Documented:** Cisco Prime Collaboration Provisioning User Interface, on page 7 Using Global Search, on page 240 Ordering Service for a User, on page 253
Managing and Attaching an Orphaned VoiceMail	Allows the user to manage and attach orphaned voicemails. **Where Documented:** Managing Voicemail, on page 186 Attach Voicemail, on page 186
Managing Synchronization Failures	Monitors and notifies users if there is no progress in the synchronization. Provides an option to users to terminate the synchronization that is not progressing. **Where Documented:** Infrastructure and User Synchronization, on page 96 Synchronizing Domains, on page 100 Configuring LDAP Server Synchronization, on page 113
Managing provisioning orders during synchronization	Avoids failures by moving the system into maintenance mode on the initiation of a synchronization. During the maintenance mode, the other Cisco Prime Collaboration Provisioning Administrators aren't allowed to begin any new device provisioning. **Where Documented:** Synchronizing Processors, Users, and Domains Overview, on page 93 Schedule Synchronization, on page 104

Standard and Advanced Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration Provisioning is available in the following modes:

- Cisco Prime Collaboration Provisioning Standard: Available with Cisco Unified Communications 10.0 and above (Unified CM and Unity Connection 10.0 and above versions).

- Cisco Prime Collaboration Provisioning Advanced: Available for all Unified Communications suite 12.1 and above versions.

Cisco Prime Collaboration Provisioning Standard is a simplified version of Cisco Prime Collaboration Provisioning. It provides simplified provisioning across all collaboration services. You can provision devices and services including IP phones, soft clients, video endpoints, analog phones, Jabber clients, presence, mobility, and voicemail. Provisioning support is available for a single Unified Communications cluster with limited authorization roles.

Advanced Provisioning provides more advanced features such as delegation to individual domains, template support for configuring infrastructure instances, advanced batch provisioning and so on.

The following table lists the features available in Cisco Prime Collaboration Provisioning Standard and Advanced. For more information on Provisioning Standard and Advanced offering, see Cisco Prime Collaboration - Standard and Advanced Offerings.

Table 3: Cisco Prime Collaboration Provisioning Standard and Advanced Features

Feature	Standard	Advanced	See Prime Collaboration Provisioning - Standard and Advanced Guide
Cluster support	Manages only one cluster of Cisco Unified Communications Manager and one cluster of Cisco Unity Connection.	Manages multiple clusters with mixes of cluster revisions and cluster associations.	For more information, see the *Adding Devices* section.
Delegation of roles or Role Based Access Control (RBAC)	Allows three levels of Role Based Access Control (RBAC): system level, advanced ordering level and basic ordering level. However, access to per domain group is not available.	Allows advanced role based access control and delegation. Administrators with ordering privileges can be assigned to different domain groups of users.	For more information, see the *Adding a User* section.
Ordering workflow roles	The ordering workflow activities such as approving an order, assigning MAC addresses, shipping endpoints, or end user receipt of an endpoint are not available.	Provides ordering workflow (Optional stages between placing an order and the actual provisioning of the order; Approver, MAC Assigner, Shipper, and Receiver). The activity roles can be enabled or disabled, and assigned to different users for an efficient ordering workflow.	For more information, see the *Overview of Authorization Roles* section.

Feature	Standard	Advanced	See Prime Collaboration Provisioning - Standard and Advanced Guide
Batch Provisioning	Allows you to deploy many services by combining them into a single batch. Batch Provisioning is available for a single cluster only.	Single provisioning batch can perform infrastructure and user provisioning across many Unified Communications Manager clusters, making Prime Collaboration batches global in scope.	For more information, see the *Managing Batch Projects* chapter.
Applications Programming Interface	Support for North Bound Interface (NBI) is not available.	Support for Northbound API is supported for integration with third-party management applications, HR systems, or other custom provisioning interfaces.	For more information, see the *Managing Licenses* chapter.

To use the Getting Started Wizard for fresh Unified Communications installation, see the Getting Started Wizard for Unified Communications Applications chapter in the *Cisco Prime Collaboration Provisioning - Standard and Advanced Guide*.

Cisco Prime Collaboration Provisioning User Interface

Cisco Prime Collaboration Provisioning allows an administrator to cross-launch configured devices such as Cisco Unified Communications Manager, Unity Connection, and IM and Presence Services using single sign-on.

You can access Provisioning on the system where Provisioning application is installed, or remotely from a client system. In a browser enter the following URL: http://IP Address, where IP Address is the address of the Cisco Prime Collaboration Provisioning server.

Cisco Prime Collaboration Provisioning supports localization in:

- English-United States [en-us]
- Arabic-Saudi Arabia [ar-sa]
- Chinese-China [zh]
- Chinese-Taiwan [zh-tw]
- Danish-Denmark [da]
- Dutch-Netherlands [nl]
- French-France [fr]
- German-Germany [de]

- Italian-Italy [it]
- Japanese-Japan [ja]
- Korean-Korea Republic [ko]
- Portugese-Brazil [pt-br]
- Russian-Russia [ru]
- Spanish-Spain [es-es]
- Swedish-Sweden [sv-se]

You can enter the following characters in the Provisioning localized UI: UTF-8 characters, alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), dots (.), at sign (@), space, and apostrophe.

In the new interface, the left pane displays **Navigation** tab, **Index** tab, and **Search Menu** field. Double-click the pin icon at the top of the home page to hide the left pane or click the **Toggle Navigation** icon to view the left pane as appropriate.

The gear icon on the top right corner of the home page allows you to log out, change password, view Help file, and view information about Cisco Prime Collaboration Provisioning.

The Home Dashboard allows you to manage the real-time information about the operational status of your processor, device, domain, and users. For more details, see Provisioning Dashboards and Reports Overview, on page 189.

The global search field at the top of the view pane allows you to locate a user ID, name, MAC address, directory numbers, DN Description, Phone Description, VM Alias Name, and EM Name. For more information, see Using Global Search, on page 240.

Usage Scenarios for Cisco Prime Collaboration Provisioning

The Provisioning features are available in the Dashboard, Device Setup, Provisioning Setup, User Provisioning, Advanced Provisioning, Infrastructure Setup, Activities, Reports and Administration menus from the Cisco Prime Collaboration application.

Some common scenarios for using Provisioning may include (This is not an all-inclusive list):

- Managing existing voice services
- Deploying a new voice infrastructure
- Managing users
- Deploying a new site on an existing voice infrastructure

You can also perform several advanced activities to meet the needs of your Cisco Prime Collaboration deployment. Some of these activities include:

- Customizing the Provisioning features to meet your needs
- Performing many Provisioning activities
- Working with provisioning resources
- Setting up the server

Table 4: Usage Scenarios, on page 9 provides details on several usage scenarios for Provisioning.

Table 4: Usage Scenarios

Usage Scenarios	
Managing Existing Voice Services	If you are managing a Cisco Unified Communications Manager/Cisco Unified Communications Manager Express/Cisco Unity Connection/Cisco Unity Express through their respective interfaces, and you want to delegate management of a subset of these voice services to other users, see the following sections: • Adding Devices, on page 43 • Infrastructure and User Synchronization, on page 96 • Adding a Domain, on page 64 • Adding Service Areas, on page 66 • Synchronizing Domains, on page 100
Deploying a New Voice Infrastructure	If you are adding a new Cisco Unified Communications Manager or Cisco Unified Communications Manager Express and related voicemail systems, and you want to use a standardized approach that can be applied to every deployment, see the following sections: • Adding Service Areas, on page 66 • Synchronizing Domains, on page 100 • Ordering Service for a User, on page 253 You can create orders for endpoints and services. You can create orders for individual services, or you can order bundled services. • Managing Batch Projects, on page 151

Usage Scenarios	
Managing Services for a User	To manage services for users in your office, see the following sections: • A user is a person who has active IP Telephony services. Provisioning allows you to add users, synchronize the user information, move the services, update user information, and domain-specific user roles. See Overview of Authorization Roles, on page 210. • Orders for a single user are displayed and initiated in the User Record for that user. The User Record lists all existing products for the user, see Accessing User Records for a User, on page 239. • You can create orders for endpoints and services. See Orders Overview, on page 251. • Processing Orders, on page 297 • Canceling Services, on page 300
Deploying a New Site on an Existing Voice Infrastructure	To add a new location or site to an existing Cisco Unified Communications Manager, see: • Adding a Domain, on page 64 • Synchronizing Domains, on page 100 • Orders Overview, on page 251 • Managing Batch Projects, on page 151
Customizing the Provisioning Feature to Meet Your Needs	To change the default setting for how Provisioning applies various policies, see: • Overview of Business Rules, on page 163 • Creating Service Templates, on page 79 • Adding User Roles, on page 71
Performing many Provisioning Activities	If you are deploying many services, you can combine these activities into a single batch, see Managing Batch Projects, on page 151.
Working with Provisioning Resources	To manage Provisioning resources, see: • Managing Endpoint Inventory, on page 181 • Managing Directory Number, on page 184 • Provisioning Reports, on page 193

Usage Scenarios	
Setting Up the Server	For information on Setting up the server, see: • Managing Licenses • Users in Provisioning represent logins to the system for people who can access Provisioning to perform various activities. Users can be permitted to perform various roles within Provisioning. These roles can be system-wide (for example, administrators), or they can be associated to a single Domain, which limits the scope of changes that the user can make. See Adding Users, on page 199. • Enabling Data Purging for Provisioning, on page 328
Maintaining the Server	For information on Maintaining the Server, see: • Changing the Log Level (GUI), on page 312 • Enabling Data Purging for Provisioning, on page 328

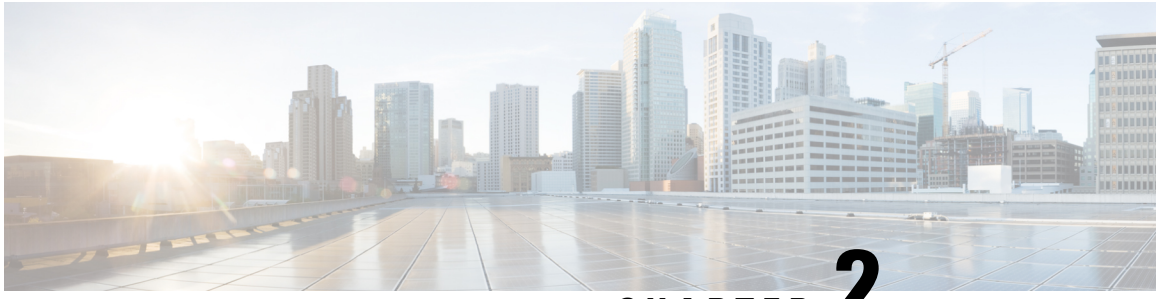
IPv6 Support in Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration Provisioning is IPv6 aware. IPv6-aware is defined as containing IPv6 functional information, but using IPv4 for transport.

As an IPv6-aware application, Cisco Prime Collaboration Provisioning continues to communicate with Cisco Unified Communications Manager devices through an IPv4 link.

The following also apply to IPv6-aware support in Provisioning Manager:

- On the Call Processor Configuration page, you can only enter an IPv4 IP address. If you enter an IPv6 address, an error message appears.
- Cisco Prime Collaboration Provisioning communicates with Cisco Unified Communications Manager using IPv4 protocol, but can provision phones that use either IPv4 or IPv6 protocol.



CHAPTER 2

Setting Up the Server

Managing Licenses

To use Cisco Prime Collaboration Provisioning, you must have the Provisioning Image license and one or more scale licenses. The image license must be present or the product remains in the evaluation mode. Scale licenses add to the number of phones you can provision.

Click **View detailed feature information** (go to **Administration** > **License Management**) to view the Feature name, Available count, Used count and Expiry.

In Cisco Prime Collaboration Provisioning Standard, the delegation, workflow, template, and NBI features are listed under unavailable features. When you purchase a license for Cisco Prime Collaboration Provisioning Advanced, these features appear in the valid features list.

Note If you have a distributed installation, when the network connection between the two servers is lost and then re-established or when only the Provisioning database (the PostgreSQL database) server is restarted, you may get login error for the Provisioning server. Sometimes a license error may appear on the Licensing Status Information page that all features are unavailable. Restart the Provisioning services on the Application server to fix such errors.

- When you purchase a license for Cisco Prime Collaboration Provisioning for the first time, the image and scale licenses may be concatenated into a single license file.
- You can purchase Provisioning image license and one or more scale licenses to cover the number of phone MAC addresses to be managed. Scale licenses are additive, up to 150,000 per one Provisioning instance. If the image license is not present, the product remains in evaluation mode.
- The installed OVA size determines the maximum scale of an instance of Cisco Prime Collaboration Provisioning.

- The Application Programmable Interface (API) for Provisioning is called the Cisco Prime Collaboration Provisioning Northbound Interface (Provisioning NBI). It is a set of web service, SOAP-based requests covering most of the provisioning functionality of Provisioning. For detailed information, see the Provisioning NBI document.

If more than one image license file is found in the license directory, Cisco Prime Collaboration Provisioning selects and uses the latest image license file (based on the file date). If the server has more than one image license, duplicates must be removed as they can interfere with each other.

When a license file is added on License Management page, Cisco Prime Collaboration Provisioning validates the license file and displays proper validation message if an error is encountered. Adding the license file may fail in the following scenarios:

- Incorrect license file (Assurance license added for Provisioning application)
- Incorrect MAC address
- Incorrect version of license
- License file corrupted or modified
- License count mismatch

You can view the manually uploaded license files in the License Management page.

For Cisco Prime Collaboration Release 12.4 and later

Cisco Prime Collaboration Provisioning Release 12.4 and later works on a hybrid model that supports two modes of licenses. Only one license mode can be active at one time.

The following are the two modes licenses:

- Traditional Licensing
- Smart Licensing

On an upgraded machine, the default mode is traditional. However, you have the option of switching over to smart licensing.

In case of backup and restore, deregister the old PCP machine before registering the new machine.

Traditional Licensing Mode:

In the Traditional Licensing Mode, Cisco Prime Collaboration Provisioning uses Traditional License. You can switch over to Smart Licensing Mode by clicking the Enable Smart License button. You can also revert to the Traditional Licensing Mode by clicking the Disable Smart License button. For Traditional Licensing Mode, see Licensing Process, on page 15 section.

Smart Licensing Mode:

In the Smart Licensing Mode, Cisco Prime Collaboration Provisioning uses Smart License. You can switch over to the Traditional Licensing Mode by clicking the Disable Smart License button. You can also revert to the Smart License mode by clicking the Enable Smart License button. For Smart Licensing Mode, see the Cisco Smart Software Licensing, on page 16.

Licensing Process

The following process applies to new installations (and upgrades), and, the scale licenses.

Procedure

Step 1 Obtain a Product Authorization Key (PAK)—The PAK is used to register Cisco Prime Collaboration Provisioning on Cisco.com, and it contains resource limitations.

For each incremental license that you purchase, you will receive a PAK, and you must use that PAK to obtain a license file.

Step 2 Obtain a license file—A license file is sent to you after you register the PAK on Cisco.com.

Step 3 Import the license file to Cisco Prime Collaboration Provisioning from the License Management page. If Cisco Prime Collaboration Provisioning is already installed and you are upgrading your license file, you must import the license file with Cisco Prime Collaboration Provisioning.

Adding a License File to Cisco Prime Collaboration Provisioning

To add a license file to Cisco Prime Collaboration Provisioning:

Procedure

Step 1 Go to License Management page.

- In the Cisco Prime Collaboration Provisioning application, select **Administration** > **License Management**.

Step 2 On the **License Management** page, click **Add**.

Note If you are updating from the Cisco Prime Collaboration Provisioning Standard mode to the Cisco Prime Collaboration Provisioning Advanced licensed mode, you must add the new license files and later delete all the old license files (see the Upload Time column) listed on the License Management page using the Delete option.

Step 3 In the **Add License File** window, upload the license file, and click **OK**.

The newly added license file information appears in the License Status pane. If you purchased more than one license, repeat **Step 2** and **Step 3** to install each additional license.

To delete a license file, on the License Management page, select the license file and then click **Delete**.

Switching Between the Standard and Advanced Modes in Cisco Prime Collaboration Provisioning

Prime Collaboration allows you to switch from the Standard mode to the Advanced mode in Cisco Prime Collaboration Provisioning.

The following table captures the different scenarios of switching:

Table 5: Switching from the Standard Mode to the Advanced Mode in Cisco Prime Collaboration Provisioning

Installation Modes	Standard to Advanced Evaluation	Standard to Advanced*	Advanced Evaluation to Advanced*	Advanced Evaluation to Standard
Cisco Prime Collaboration Provisioning	Not Applicable	Yes	Yes	Not Applicable
* To upload the license file for the advanced mode, click **Administration** > **License Management**. On the License Management page, click **Add** and upload the license file.				

Cisco Smart Software Licensing

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses between entities, represented by Virtual Accounts, within your company It is enabled across Cisco products and managed by a direct cloud-based model (Cisco Smart Software Manager) or a mediated deployment model (Smart Software Manager satellite).

This service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

You can use Cisco Smart Licensing to:

- Register with Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- See the license usage and count
- See the product licenses available on Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew License Authorization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew the License Registration
- Cisco Prime Collaboration Provisioning supports multiple types of licenses and one license is required for each feature type. You need a feature license to enable each of the following available features:

  Table 6: Available Feature Licenses

Features
Advanced Features
Assign Admin to Domain
CUM/VC or CUE

Features
IM&P Servers
Max End Points
Access to API
Max Admin Login at a Time
Access to prebuilt configuration template
Unified Communications Manager clusters or CMEs
User IDs in data base
Access to order management
Lines, EM Lines, and RDP Lines

Cisco Smart Software Manager

Cisco Smart Software Manager is hosted on software.cisco.com, allowing product instances to register and report license consumption to it.

You can use Cisco Smart Software Manager to:

- Manage and track licenses
- Move licenses across virtual account
- Remove registered product instance

For more information about Cisco Smart Software Manager, see https://software.cisco.com/.

Cisco Smart Software Manager satellite

Cisco Smart Software Manager satellite is a component of Cisco Smart Licensing that manages product registrations and monitoring of smart license usage for Cisco products. If you do not want to manage Cisco products directly using Cisco Smart Software Manager, either for policy or network availability reasons, you can choose to install Cisco Smart Software Manager satellite on-premises. Products register and report license consumption to the Cisco Smart Software Manager satellite as it does on Cisco Smart Software Manager.

For more information about Cisco Smart Software Manager satellite, see http://www.cisco.com/web/ordering/smart-software-manager/smart-software-manager-satellite.html.

Product Instance Evaluation Mode

After installation and before registration, Cisco Prime Collaboration Provisioning runs under the 90-day evaluation period. During this period, you can use all features in this product. Register Cisco Prime Collaboration Provisioning with Cisco Smart Software Manager or Cisco Smart Software Manager satellite to report the license usage to Cisco and obtain the necessary authorization for entitlement usage. After the evaluation period expires, some features like adding devices, endpoints, users, RBAC, and self-care will stop working until you register with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Note Evaluation period is before the product is registered.

License Usage

Cisco Prime Collaboration Provisioning uses multiple types of licenses and one license is required for each feature type. You need one feature license to enable each of the following available features:

Table 7: Available Feature Licenses

Features
Advanced Features
Assign Admin to Domain
CUM/VC or CUE
IM&P Servers
Max End Points
Access to API
Max Admin Login at a Time
Access to prebuilt configuration template
Unified Communications Manager clusters or CMEs
User IDs in data base
Access to order management
Lines, EM Lines, and RDP Lines

The License Manager page shows information on Cisco Prime Collaboration feature license requirements, as reported to the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The License Manager page is updated daily when Cisco Prime Collaboration Provisioning communicates with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

License Compliance

When first installed, the Cisco Prime Collaboration Provisioning is fully operational in evaluation mode for 90 days until it has successfully registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Once purchased, the new licenses are deposited to a virtual account off the customer Smart Account on Cisco Smart Software Manager. If PCP is connected to Cisco Smart Software Manager, the purchased license are reflected on Cisco SSM satellite via a synchronization process between the satellite and Cisco SSM.

Cisco Prime Collaboration Provisioning reports the total license usage to the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The Cisco Smart Software Manager or Cisco Smart Software Manager satellite totals the license requirements for all connected Cisco Prime Collaboration Provisioning product instances and compares this total license requirement to the total available installed licenses. The Cisco Smart Software Manager or Cisco Smart Software Manager satellite then reports the status back to the

product instance as Authorized or as Out of Compliance. CSSM and SSM satellite also show on its portal the Authorized or Out-Of-Compliance (OOC) status. Out-Of-Compliance occurs when the number of licenses are insufficient.

Authorization Expired occurs when the product has not communicated with Cisco Smart Software Manager or Cisco Smart Software Manager satellite for 90 continuous days. In this state, Cisco Prime Collaboration Provisioning allows you to run in Authorization Expired state for another 90 more days. After which all the 14 features of Cisco Prime Collaboration Provisioning stop working.

System Licensing Prerequisites

Complete the steps to set up Smart and Virtual accounts. For more information about this process, see https://software.cisco.com/.

Smart Software Licensing Task Flow

The following is the Smart Software Licensing Task Flow:

1. Obtain the Product Instance Registration Token: Use this procedure to generate a product instance registration token for your virtual account.
2. Configure Transport Settings: Perform this step to select transport settings through which Cisco Prime Collaboration Provisioning can connect to Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Direct option is selected by default where the product communicates directly with Cisco Smart Software Manager.
3. Register with Cisco Smart Software Manager or Cisco Smart Software Manager satellite: Perform this step to register Cisco Prime Collaboration Provisioning with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Obtain the Product Instance Registration Token

Before you Begin

Obtain the product instance registration token from Cisco Smart Software Manager or Cisco Smart Software Manager satellite to register the product instance. Tokens can be generated with or without the Export-Controlled functionality feature being enabled.

The following is the procedure to obtain the Product Instance Registration Token:

1. Log in to your Smart Account in either Cisco Smart Software Manager or your Cisco Smart Software Manager satellite.
2. Navigate to the virtual account with which you want to register the Cisco Prime Collaboration Provisioning cluster.
3. Generate a "Product Instance Registration Token".

Note Select the **Allow export-controlled functionality** on the products registered with this token check box to turn on the Export-Controlled functionality for tokens of a product instance you wish in this smart account. By checking this check box and accepting the terms, you enable higher levels of the product encryption for products registered with this Registration Token. By default, this check box is selected. You can uncheck this check box if you wish not to allow the Export-Controlled functionality to be made available for use with this token.

Note Use this option only if you are compliant with the Export-Controlled functionality.

Note The **Allow export-controlled** functionality on the products registered with this token check box is not displayed for the Smart Accounts that are not permitted to use the Export-Controlled functionality.

4. Copy the token or save it to another location.

For more information, see https://software.cisco.com/.

Configure Transport Settings

Use this procedure to select transport settings through which Cisco Prime Collaboration Provisioning can connect to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Before You Begin

Obtain the Product Instance Registration Token

The following is the procedure to configure transport settings:

1. From Cisco Prime Collaboration Provisioning GUI, choose **Administration** > **License Management**. The License Manager window appears.
2. From the Smart Software Licensing section, click the **View/Edit** link. The Transport Settings dialog box appears.
3. Select one of the following radio buttons:
   - Direct—Cisco Prime Collaboration Provisioning sends usage information directly over the internet. No additional components are needed. This is the default setting.
   - Cisco Smart Software Manager satellite—Cisco Prime Collaboration Provisioning sends usage information to an on-premise Cisco Smart Software Manager. Periodically, an exchange of information is performed to keep the databases in synchronization. Enter the details in the URL text box.

     For more information on installation or configuration of the Cisco Smart Software Manager satellite, go to this URL: www.cisco.com/go/smartsatellite.
   - Proxy Server—Cisco Prime Collaboration Provisioning sends license usage information to Cisco Smart Software Manager through a proxy server which can be an off-the-shelf proxy such as Cisco Transport Gateway or Apache. The customer would need to install this on their premises and configure the details in the following fields:
     - Host Name/IP Address
     - Port

Note If you choose to use direct connection, then you must configure Domain Name System (DNS) on Cisco Prime Collaboration Provisioning that can resolve tools.cisco.com.

Note If you choose not to use the DNS server in your deployment and not connect to the Internet, then you can select the Cisco Smart Software Manager satellite with manual synchronization in disconnected mode.

4. Click **Save**.

Register with Cisco Smart Software Manager

Use this procedure to register your product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Your product is in Evaluation Mode until then.

Before You Begin

Configure Transport Settings

1. From Cisco Prime Collaboration Provisioning GUI, choose Administration> License Management. The License Manager window appears.
2. From the Smart Software Licensing section, click the **Register** button. The Smart Software Licensing Product Registration window appears.
3. In the Product Instance Registration Token section, paste the copied or saved "Registration Token Key" that you generated using the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
4. Click **Register** to complete the registration process.
5. Click **Close**.

Note License Usage information is updated once every 24 hours automatically.

Smart Software Licensing Additional Operations

The available Smart Software Licensing additional operations are:

- Renew Authorization: Renew Authorization is performed automatically every 30 days by Cisco Prime Collaboration Provisioning; however, the user can manually do this step to renew the License Authorization Status for all the licenses listed under License Type.
- Renew Registration: Registration renewal is automatically performed by Cisco Prime Collaboration Provisioning every 6 months. However, the user can perform this step manually to renew the ID certificate that has been assigned to Cisco Prime Collaboration Provisioning.
- Deregister:

  Perform this step to disconnect the Cisco Prime Collaboration Provisioning cluster from Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The product reverts to evaluation mode as long as the evaluation period is not expired. All license entitlements used for the product are immediately released back to the virtual account and are available for other product instances to use.
- Reregister License with Cisco Smart Software Manager:

  Perform this step to reregister (register with force) Cisco Prime Collaboration Provisioning with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Reregistration means register with

force and this option is used when a product needs to be registered without deregistration first. This could be due to an error condition making the deregistration before registration not possible.

Note Product may migrate to a different virtual account by reregistering with token from a new virtual account.

Renew Authorization

Use this procedure to manually renew the License Authorization Status for all the licenses listed under the License Type.

Note The authorization renew expires after 90 days if Cisco Prime Collaboration Provisioning is not connected to Cisco Smart Software Manager or Smart Software Manager satellite. You have an additional 90-day grace period after the authorization expires, before some of the functionalities like adding devices, endpoints, users, RBAC, and self-care are affected. The authorization renew is automatically renewed every 30 days.

Before You Begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

The following is the procedure to renew authorization:

1. From Cisco Prime Collaboration Provisioning GUI, choose **Administration** > **License Management**. The License Manager window appears.
2. From the Smart Software Licensing section, click the **Actions** drop—down list box.
3. Choose **Renew Registration Now**. The Renew Registration window appears.
4. Click **Ok**.

   Cisco Prime Collaboration Provisioning sends a request to Cisco Smart Software Manager or Cisco Smart Software Manager satellite to check the "License Authorization Status" and Cisco Smart Software Manager or Cisco Smart Software Manager satellite reports back the status to Cisco Prime Collaboration Provisioning.

Note License Usage information is updated once every 24 hours automatically.

Renew Registration

During product registration to Cisco Smart Software Manager or Cisco Smart Software Manager satellite, there is a security association used to identify the product and is anchored by the registration certificate, which has a lifetime of one year (that is, registration period). This is different from the registration token ID expiration, which has the time limit for the token to be active. This registration period is automatically renewed every 6 months. However, if there is an issue, you can manually renew this registration period.

Note The initial registration is valid for one year. Renewal of registration is automatically done every six months provided the product is connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Before You Begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

The following is the procedure to renew registration:

1. From Cisco Prime Collaboration Provisioning GUI, choose Administration> License Management. The License Manager window appears.
2. From the Smart Software Licensing section, click the **Actions** drop—down list.
3. Choose **Renew Registration Now**. The Renew Registration window appears.
4. Click **Ok**.

   Cisco Prime Collaboration Provisioning sends a request to Cisco Smart Software Manager or Cisco Smart Software Manager satellite to check the "Registration Status" and Cisco Smart Software Manager or Cisco Smart Software Manager satellite reports back the status to Cisco Prime Collaboration Provisioning.

Note License Usage information is updated once every 24 hours automatically.

Deregister

Use this procedure to unregister from Cisco Smart Software Manager or Cisco Smart Software Manager satellite and release all the licenses from the current virtual account. This procedure also disconnects Cisco Prime Collaboration Provisioning cluster from Cisco Smart Software Manager or Cisco Smart Software Manager satellite. All license entitlements used for the product are released back to the virtual account and is available for other product instances to use.

Before You Begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

The following is the procedure to deregister:

1. From Cisco Prime Collaboration Provisioning GUI, choose **Administration** > **License Management**. The License Manager window appears.
2. From the Smart Software Licensing section, click the **Actions** drop—down list box.
3. Choose **Deregister**. The Deregister window appears.
4. Click **Ok**.

Note License Usage information is updated once every 24 hours automatically.

Reregister License with Cisco Smart Software Manager

Use this procedure to reregister (register force) Cisco Prime Collaboration Provisioning with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Before You Begin

Obtain the Product Instance Registration Token

The following is the procedure to reregister a license:

1. From Cisco Prime Collaboration Provisioning GUI, choose **Administration** > **License Management**. The License Manager window appears.
2. From the Smart Software Licensing section, click the **Register** button. The Registration window appears.
3. From the Smart Software Licensing section, click the **Actions** drop—down list box.
4. Choose **Reregister**. The Smart Software Licensing Product Re-registration window appears.
5. In the Product Instance Registration Token section, paste the copied or saved "Registration Token Key" that you generated using the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
6. Click **Register** to complete the registration process.
7. Click **Close**.

Note License Usage information is updated once every 24 hours automatically.

Cross-launch from Cisco Prime Collaboration Provisioning

With Prime Collaboration 10.0 and above, you can access the Cisco Unified Communication functionality through Cisco Prime Collaboration Provisioning, using the cross-launch feature of Cisco Prime Collaboration Provisioning. Cisco Prime Collaboration Provisioning redirects to the Cisco Unified CM user interface to provision the infrastructure objects, upon clicking the infrastructure objects suitable for cross launching. Any user with admin privilege can cross-launch from Cisco Prime Collaboration Provisioning to use Cisco Unified Communication products. Cross-launch enables a smooth, continuous workflow if an administrator in Cisco Prime Collaboration Provisioning requires access to the device user interface and wants to update a user configuration on the product user interface of the configured devices such as Cisco Unified CM, Unity Connection, or IM and Presence Services.

As an admin user, you can use cross-launch for the following purposes, from Cisco Prime Collaboration Provisioning:

- Cross-launching Devices from Infrastructure Configuration
- Cross-launching Serviceability from Infrastructure Setup. See Adding Devices.

- Cross-launching Related Links in Cisco Unified CM from User Provisioning. See Cross-launching Related Links in Unified Communications Manager and Unity Connection from User Provisioning.

Note

- Cross launching is available for users with administrator privileges only and is supported for Cisco Unified CM, Unity Connection, and Presence Services from 10.0 version onwards. If you add older version (earlier than 10.0) of these devices in Cisco Prime Collaboration Provisioning, you will view native-launch links only, as an admin. Native-launch link is applicable to certain infrastructure objects that can be configured in Cisco Unified CM through Cisco Prime Collaboration Provisioning user interface.

  However, Presence Services, with versions earlier than 10.0, are not listed in the Infrastructure Configuration view as native links were not supported in earlier versions of Prime Collaboration.

- Enabling Single Sign-On (SSO) for Cross-launch is not mandatory. If you have not enabled SSO for cross-launch, you must specify the login credentials when you cross launch a processor (Cisco Unified Communications Manager, Unity Connection, or Presence Services) for the first time by continuing when you are prompted to add the website in the trusted security certificate list. However, you need not login on successive attempts to cross launch the processor as long as the session is in progress and running. To enable SSO, see Single Sign-On for Cisco Prime Collaboration Provisioning, on page 25.

- Depending on browser settings, the cross-launch may open in new browser tab or a new window. Refer to the browser compatibility in the product documentation of the specific application.

Single Sign-On for Cisco Prime Collaboration Provisioning

Prime Collaboration provides users with admin privileges to enable Single Sign-On (SSO) in Cisco Prime Collaboration Provisioning using Security Assertion Markup Language (SAML).

Prime Collaboration does not support multiserver SAN certificates and end user SAML SSO.

You can enable SSO in Cisco Prime Collaboration Provisioning to cross-launch the following UC applications:

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco IM and Presence

Note To cross-launch the UC applications without the need for login credentials, ensure that SSO for those applications is configured on the same IdP server as that of Prime Collaboration.

Ensure that the following prerequisites are met before you enable SSO:

- At least one LDAP Administrative user exists in the system—through LDAP synchronization in Cisco Prime Collaboration Provisioning.

  For information on how to provide administrative privileges to a user in Cisco Prime Collaboration Provisioning, see Managing Users chapter in the Cisco Prime Collaboration Provisioning Guide.

- An Identity Provider (IdP) server that enables you to use SSO to access many other applications from a single hosted application and a Service Provider. The Service Provider is a website that hosts the applications.

  Following are the supported third-party IdP servers:

  - Open Access Manager (OpenAM)
  - Ping Identity
  - Active Directory Federation Services (ADFS)
  - Oracle Identity Manager

  For the steps to set up an IdP server, see the SAML SSO Deployment Guide for Cisco Unified Communication Applications, Release 10.0(1).

- Download the Identity Provider metadata file from the IdP server and save it in your local system.

To enable Single Sign-on:

Procedure

Step 1 Choose **Administration** -> **Single Sign-on**.

Step 2 Click **Enable SSO**.

A warning message is displayed stating, Enabling SSO redirects you to the IdP server for authentication from the next login. To access the application, you will need to be authenticated successfully.

Note **Enable SSO** is disabled if the prerequisites are not met.

Step 3 Click **Continue**.

Step 4 Follow the steps that are provided in the SSO wizard to enable Single Sign-On.

a) Locate the IdP metadata file from your local system and click **Import IdP Metadata**.

b) Click **Download Trust Metadata file**.

c) Launch the IdP server and import the downloaded Trust Metadata file.

Note This is a manual step for Enabling SSO. Create a Circle of Trust (CoT) in the IdP server and log out before proceeding with the SSO testing.

d) To run SSO Test Setup, select a username from the **Valid Administrative Usernames** drop-down.

Note Using any other username to log in to the IdP server may lock the administrator account.

e) Click **Run SSO Test** to test the connectivity among the IdP server, Prime Collaboration Applications, and Single Sign-On.

If you are prompted with an error message, Unable to do Single Sign-On or Federation:

- Manually log in to the IdP server using the end user credentials and check if the authentication is successful.
- Verify if the Trust Metadata file is successfully uploaded in the IdP server.
- Verify if the Prime Collaboration server and the IdP server are part of the same Circle of Trust.

f) Click **Finish**.

Troubleshooting and Logs for SSO

- When you are logged out of the Prime Collaboration server while enabling SSO, we recommend that you close the browser and relaunch the Prime Collaboration application. Because, though your session expires in the Prime Collaboration server, the IdP server session may be still active.
- You can find the log file (ssosp*.log) for Cisco Prime Collaboration Provisioning in the **/opt/cupm/sep/logs** directory.
- While enabling SSO, ensure that the hostname for Prime Collaboration is set and is part of DNS.

When the IdP server is down, you can:

- Use the recovery URL- https://<PCserver IP address or host name that is part of DNS>/ssosp/local/login.
- Disable Single Sign-On from CMD Utility.

To disable SSO from CMD utility in Prime Collaboration applications:

- Log in to the Cisco Prime Collaboration Provisioning server using SSH with port 22.
- Navigate to the**/opt/cupm/sep/build/bin** directory for Cisco Prime Collaboration Provisioning. Add <Operation> and <Value> entries in the **cpcmconfigsso.sh** file.

Operations can be...	Values can be...
1-To get the Single Sign-On status	Not applicable
2-To get the recovery URL status	Not applicable
3-To set the Single Sign-On status	False **Note** You cannot enable SSO through CLI. Use the UI procedure to enable SSO.
4-To set the recovery URL status	True or False

- To disable SSO, run the following command:

```
cpcmconfigsso.sh 3 false
```

Note The recovery URL is enabled by default. If you want to disable it for security reasons, set it as false.

Configuring Provisioning to Use LDAP and ACS Servers

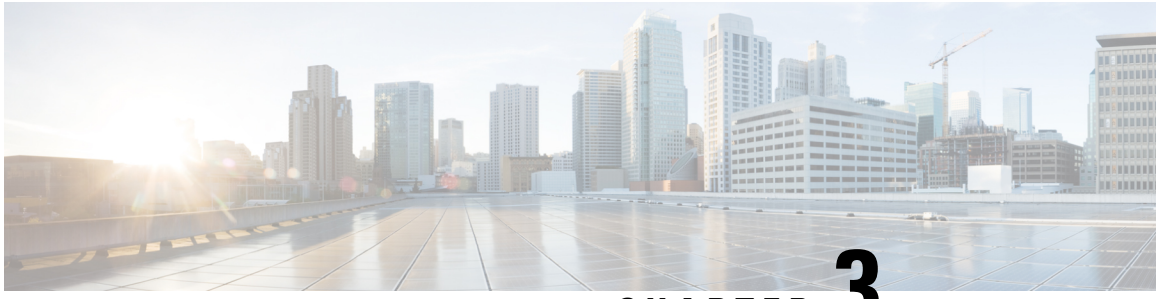
You can configure Cisco Prime Collaboration Provisioning to use Access Control Server (ACS) or LDAP server to authenticate, read, and synchronize.

Note

- If you are adding an ACS server, you must add the Provisioning server as an ACS client (with TACACS).
- To enable SSL for LDAP Server:
  1. You must upload the LDAP server certificate. For the steps to upload LDAP certificate, refer Upload SSL Certificate, on page 326.
  2. Go to the **LDAP Server Configuration** page and check the **Use SSL** check box.
- Before deleting an ACS or LDAP server, ensure that it is not assigned to a Domain. ACS or LDAP servers are enabled on a per Domain basis. After adding an ACS or LDAP server, you must assign it to a Domain. All the users in the Domain, are authenticated against that ACS or LDAP server. If an ACS or LDAP server is not associated to a Domain, all the users of that Domain are authenticated locally. Globaladmin is always authenticated locally.
- All authentication happens on the Active Directory/LDAP server when a domain has both local users and external users (LDAP or ACS), and if the domain is integrated with Active Directory/LDAP.
- We recommend, not to have a domain that has a combination of both local users and external users.

When configuring Provisioning to use Cisco Secure Access Control Server, be aware of the following:

- When you click the Test Connection button, only the connectivity of the IP address is checked.
- The Shared Secret Key is used only for authentication.
- If you entered an incorrect Shared Secret Key, when you try to log into Provisioning, you will get an incorrect secret key error. Use the SSK that is generated while configuring ACS.
- Provisioning supports only ACS 5.x.



CHAPTER 3

Getting Started Wizard for Unified Communications Applications

Getting Started Wizard for Unified Communications Applications

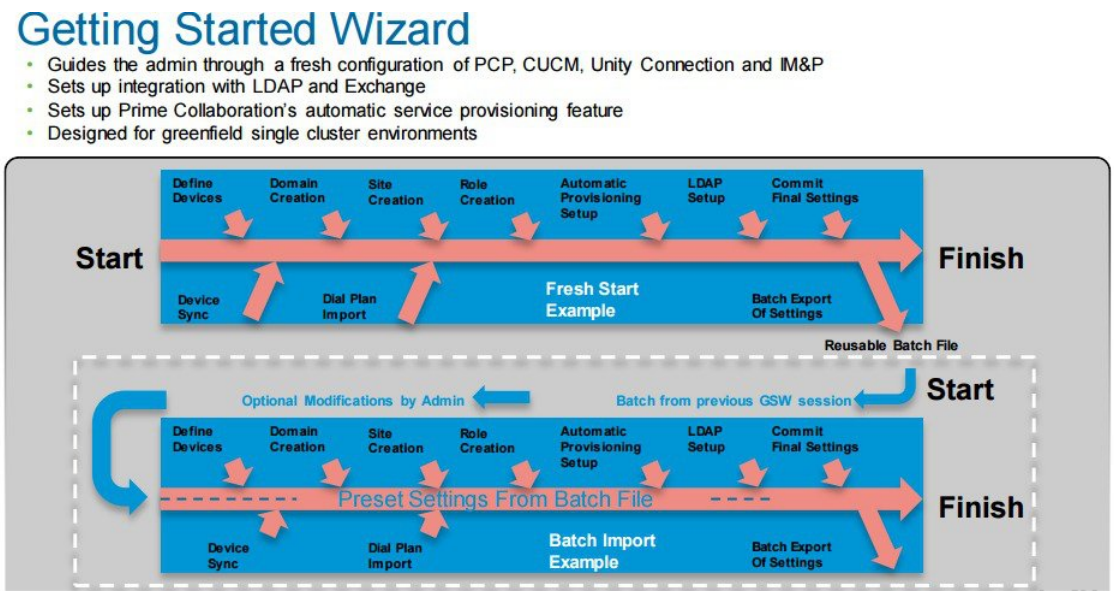
The Getting Started wizard allows you to quickly set up devices in Cisco Prime Collaboration Provisioning and provision services to the user. Using the wizard you can quickly integrate Unified Communications applications with Cisco Prime Collaboration Provisioning and configure them. The following table provides details about the Getting Started wizard.

Overview of Getting Started Wizard

Features	Description
About Getting Started Wizard	• Guides the administrator through a fresh configuration of Cisco Prime Collaboration Provisioning, Cisco Unified CM, Cisco Unity Connection and Cisco IM&P. • Sets up integration with LDAP and Exchange. • Sets up Prime Collaboration's automatic service provisioning feature.

Features	Description
Initial setup of Cisco Unified CM and Cisco Prime Collaboration Provisioning	• Define Cisco Unified CM, Cisco Unity Connection, Cisco IM&P, Exchange, and LDAP. • Integrates Applications. • Sets up a Domain (user group), a Service Areas (site) and a User Role (policy). • Sets up Prime Collaboration Automatic Service Provisioning.
Creates an initial site	• Provisions site related settings (device pool, partition, CSS, DN blocks, and so on). • Imports basic dial patterns from CSV file or Cisco Unified Configurator for Collaboration (CUCC) application. • Builds a site in UC applications.
Reentrant	• Can export the settings as a Cisco Prime Collaboration Provisioning batch file. • Batch file can be modified and fed back into the Setup Wizard to pre-populate settings for the next installation. • Batch file can be broken up into separate tasks and/or modified and fed into the PC Batch Provisioning system.
Targeted for greenfield and single cluster environments	• Designed for greenfield and single cluster environments. • Can be used during initial setup of a larger system.

Figure 1: Getting Started Wizard



You can use the wizard to deploy new Unified Communications applications in your network. The wizard helps you to add a single Domain (group of users), and a Service Area (also known as Site) to Cisco Prime Collaboration Provisioning, and enable User Role for users. You can add Unified Communications Processors (one call processor, message processor, and presence processor each) for new deployments. For adding additional processors, choose **Device Setup**. You can also integrate LDAP server and synchronize users.

Note the following when using the wizard:

- Choose **Infrastructure Setup** > **Getting Started Wizard** and click **Begin** in the dialog box that appears.
- If you close the wizard , the following options will be displayed:
  - Return—Click **Return** to go back to where you had left.
  - Quit—Click **Quit** to exit the current wizard. You will not be able to continue from this page when the wizard is restarted. Any configuration that has been made up to this point will remain in the system.
  - Continue Later—Click **Continue Later** to continue the wizard from this page later.
- If you close the wizard abruptly, navigate to another page (exit the wizard), or refresh the Prime Collaboration UI in between the wizard setup, you must log into the wizard again.
- If another user has logged into the wizard before you log in, you will not be able to launch the wizard until the other user logs out. If another user has not logged in, and you are still unable to log into the wizard, you must logout yourself (from Home > Dashboard > Logged In Users) to resume your wizard configuration.

  When you log in, you will be prompted to either continue your previous configuration, or cancel it and start from the beginning. You must click continue to resume your configuration. If your configuration is saved in Cisco Prime Collaboration Provisioning before you left the wizard, you will continue with the next step in the wizard. If the configuration is not saved, you will continue your configuration from where you had left.

For example, if you exit the wizard after adding details in the Infrastructure Setup page, and the information added was saved successfully before you left the wizard, you will launch the Domain Creation page (next page) when you log into the wizard again. If the device details are not saved, then you go back to the Infrastructure Setup page (where you had left).

- If your session times out in between the wizard setup, you will continue your configuration from where you had left when you launch the wizard again.
- Multiple instances of the wizard cannot be used at any given time.

Related Topics

Getting Started, on page 32

Getting Started

The step-by-step wizard helps you to perform the following tasks:

Note The wizard allows you to add Unified Communications processors for fresh installs only. The Unified CM Publisher and Subscriber must not be configured before running the Getting Started wizard. To add Unified Communications processors that are already configured, choose the Infrastructure Setup menu. The wizard supports Unified Communications processors 10.5 and above versions.

Step	Task and Description	Additional Information
Step 1	Begin Provisioning. Install Cisco Unified Communications Manager before proceeding to the next step in the wizard. Installing Cisco Unity Connection, Cisco IM & Presence, and Prime License Manager are optional. Verify LDAP credentials if you have added an LDAP server. See Setting Up Devices for Prime Collaboration Provisioning. On the Welcome page, you can import a configuration file that contains the configuration details required by the wizard. You can also download the sample configuration file, modify the text files based on your requirements, and upload the updated zip file.	If you exit the wizard here, you can choose **Device Setup** to continue with adding device to Cisco Prime Collaboration Provisioning.
Step 2	Add Devices. You can add devices for new deployments.	Call processor, message processor (optional) and presence processor (optional) are added to Cisco Prime Collaboration Provisioning. If you exit the wizard here, or if you want to verify, edit and add more devices after completing the wizard, choose **Device Setup**.

Step	Task and Description	Additional Information
Step 3	Create a Domain. Create a domain and associate it to the processors you have added. You can add an intra-site dial plan that you can edit or extend later using the Infrastructure Configuration page.	If you exit the wizard here, or if you want to verify, edit and add more domains after completing the wizard, choose **Provisioning Setup**.
Step 4	Create a Service Area. Create a Service Area and associate it to the Domain you have created.	If you exit the wizard here, or if you want to verify, edit and add more service areas, choose **Provisioning Setup**.
Step 5	Enable Automatic and Manual Service Provisioning for a User Role.	If you exit the wizard here, or if you want to verify the user role and its associated services after completing the wizard, choose **Provisioning Setup**.
Step 6	Add users or synchronize from LDAP server.	You can choose to add users manually or synchronize the LDAP server.
Step 7	Review configuration summary.	A summary of all the configuration performed using the wizard is available for review.
Step 8	Apply your configuration.	You have completed setting up devices, Domains, Service Areas and User Roles. You can choose **User Provisioning** to order services.

Before you begin

On the Welcome page, you can import a configuration file that contains the configuration details required by the wizard. You can also download the sample configuration file, modify the text files based on your requirements, and upload the updated zip file. You can edit the sample files (.txt) using Excel, save the updated spreadsheet as tab-delimited text file, and import the file. Note the following points while importing the configuration file:

- You can upload only zip file.
- The uploaded zip file should contain all the files that are included in the sample configuration file (downloaded from the Welcome page). The file names must be exactly the same as in configuration file. If there are extra files and directories, they will be ignored.
- The uploaded zip file should contain all the infrastructure objects present in the sample configuration file (located at /opt/cupm/sep/deploy/dfc.ear/dfc.war/ipt/gsWizard/pcp-sample-config.zip).
- It is not recommended to change the product names of the infrastructure objects that are included in the sample configuration file.
- Using the configuration file, you can add only one domain, service area, and user role at a time. Also, you can add only one Cisco Unified Communications Manager, Cisco Unity Connection, Unified IM and Presence, and LDAP server at a time.
- You can also import Cisco Unified Configurator for Collaboration (CUCC) configuration files (tar files). The CUCC configuration file can contain the configuration details for only one Site, because you can configure only one Domain and Service Area at a time using the Getting Started wizard. You can find

the sample CUCC configuration files at the following location: /opt/cupm/sep/ipt/config/sample/cucc samples in tar.

- You cannot add more devices if you re-import the configuration file in another run of the wizard per Cisco Prime Collaboration Provisioning installation.
- If you export a configuration file from Cisco Prime Collaboration Provisioning 11.1 and before and re-import it back to Cisco Prime Collaboration Provisioning 11.2 and later, you must import the batch file based on the new batch format.

Procedure

Step 1 Choose **Infrastructure Setup** > **Getting Started Wizard**.

Step 2 On the Welcome page, click **Begin** to start setting up Cisco Prime Collaboration Provisioning using the wizard.

Step 3 Click **Close** if you have not met the pre-requisites.

Step 4 Add devices to Cisco Prime Collaboration Provisioning.

The following fields will be auto-populated based on the values provided in the configuration file. If you have not imported any configuration file, Cisco Prime Collaboration Provisioning uses the values provided in the default configuration file.

Page	Field Name
Infrastructure Setup page	• Unified Communications Manager name • Username • Password
Domain page	• Domain name • Description
Service Area page	• Name • Time Zone • Directory Number Block • PSTN Gateway • Site code • Device mobility • SRST
User Role page	Some of the fields will be auto-populated in the Manual Service Provisioning page and Automatic Service Provisioning page.
Directory Synchronization (LDAP Sync) page	• LDAP Server

Related Topics

Adding Devices, on page 43
Adding Service Areas, on page 66
Adding a Domain, on page 64
Adding User Roles, on page 71
Automatic Service Provisioning, on page 75
Configuring LDAP Server Synchronization, on page 113
Batch Provisioning, on page 127

Creating a Domain

The wizard allows you to create a Domain and associate the unified processors that you have added in the Device Setup page of the wizard.

Procedure

Step 1 On the Domain Creation page, enter the domain name and description details.

Note For the domain name, valid values are alphanumeric (a-z, A-Z, 0-9), period (.), hyphen (-), at sign (@), and underscore (_), but it cannot include quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).

Step 2 (Optional) You can add an intra-site dial plan that you can edit or extend later using the Infrastructure Configuration page. The dial pattern specifies how to interpret digit sequences dialed by the user, and how to convert those sequences to an outbound dial string.

You can download the sample dial pattern file from the Domain Creation page. You can also import CUCC dial pattern file. If you have already uploaded a dial pattern file (as part of the configuration zip file) in the Welcome page, Cisco Prime Collaboration Provisioning will use the dial pattern added through the Domain Creation page, instead of the dial pattern file added as part of the configuration zip file.

If you have not imported any dial pattern file, the wizard will use the default 10-digit dial pattern file.

Step 3 Click **Save and Continue**.

You will be notified if you are trying to create a domain that already exists in Cisco Prime Collaboration Provisioning.

Step 4 Create a Service Area in the Domain.

Creating a Service Area

The wizard allows you to create a service area (Site) and associate it to the domain. You can define values for Device Pool, Location, and Route Partition, corresponding to that Service Area.

Procedure

Step 1 On the Service Area creation page, enter the service area name, Time Zone, PSTN Gateway IP address (or hostname), site code, and Directory Number Block details. You can also provide the Survivable Remote Site Telephony (SRST) and Device Mobility information, if required.

Note For the service area name, valid values are alphanumeric (a-z, A-Z, 0-9), period (.), hyphen (-), at sign (@), and underscore (_), but it cannot include quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).

Step 2 Click **Save and Continue**.

Step 3 Enabling Manual and Automatic Service Provisioning.

Enabling Automatic and Manual Service Provisioning for a User Role

The wizard allows you to enable manual and automatic service provisioning for a user role:

- Manual Service Provisioning—The endpoints and services will be manually assigned by an administrator while placing an order for a user with this user role.
- Automatic Service Provisioning—This is optional. If you enable automatic service provisioning, the endpoints and services you assign will be automatically provisioned to the user created with this user role.

You can enable automatic and manual service provisioning for only one user role using the wizard. To enable automatic and manual service provisioning for more user roles, choose **Provisioning Setup**.

Procedure

Step 1 Employee user role is created by default when creating the Domain. You can rename the user role if required, but cannot change the user role type (Employee).

Step 2 For manual provisioning, select the Line Type, Endpoint, Service and Service bundles. These services must be manually assigned by an administrator while placing an order for a user with this user role.

Step 3 Enable Automatic Service Provisioning for the user role.

Step 4 Select the endpoint, service and service bundles you want to automatically provision for the user role.

You can select the following:

- Endpoint—You can either choose a self-provisioned endpoint or a default endpoint. Cisco Unified IP Phone 7960 is the default endpoint model auto-provisioned for the user. If you choose self-provisioned endpoint, enter the maximum number of endpoints, and Interactive Voice Response (IVR) details required by the Unified Communications Manager.

  Cisco Prime Collaboration Provisioning requires the IVR Directory Number, and Auto-registration starting and ending Directory Numbers to self-provision the endpoints. These numbers are auto populated when the voicemail pilot number is provided while adding the message processor. When the user dials the IVR Directory Number from the endpoint, the IVR prompts will be played. The Starting and Ending Auto-registration Directory Numbers define the range of Directory Numbers that are used by the endpoints to auto-register.

- Line
- Single Number Reach
- IM and Presence
- Voicemail
- Extension Mobility Access
- Extension Mobility Line
- Cisco Jabber

Step 5 Click **Customize** to edit or change the default service templates. For example, Cisco 7960 service template is created by default for the default endpoint model 7960. You can either customize this default template, or choose another endpoint from the drop-down and customize it.

Note The default service templates created by the wizard will not be used for Auto-provisioning if you update it manually outside the wizard (choose Provisioning Setup, and select the default service template). To associate the template again to auto-provisioning, you must mark the **use for auto-provisioning** as yes in the Service Assignment Table on the User Role page.

You have an option to customize user services.

Step 6 Click **Save and Continue**.
The services and service bundles that you select for the user role will be automatically provisioned to the user when placing orders.

Step 7 Add users.

Adding Users

The wizard allows you to either import users manually or synchronize from the LDAP server.

Procedure

Step 1 To synchronize users, choose:

- Use Directory (LDAP) Server to synchronize users to Cisco Prime Collaboration Provisioning.

By default, the system administrator adds users. If you choose to synchronize an LDAP server, you must populate the necessary LDAP fields. If you exit the wizard here, or if you want to verify and edit LDAP Settings after completing the wizard, choose **Provisioning Setup** and select a Domain to edit.

Step 2 Click **Save and Continue**.
Your configuration is complete and the summary page appears.

Summary of Configuration

The Getting Started Wizard Summary page shows the configurations completed using the wizard.

Procedure

Step 1 Based on the processors that are configured, pre-built configuration templates are created in Cisco Prime Collaboration Provisioning. Click **Infrastructure Configuration** to see the list of pre-built configuration templates and infrastructure objects configured at the end of the wizard.
You can also see the pre-built configuration templates and the infrastructure objects from the following menus:

- Choose **Advanced Provisioning** > **Batch Provisioning** and open the list of Batch Projects. You can see one batch project created for each of the unified communications processor added through the wizard. These batch projects list all the infrastructure objects.
- Choose **Infrastructure Setup** > **Configuration Templates** and open the list of pre-built configuration templates. All the objects configured using the wizard are listed.

Step 2 You can export the wizard data to a configuration file by using the **Save the Configuration File** option in the Summary page. Click **Save the Configuration File with Keywords** option to save the configuration file with keywords.
You can use the exported file on a different server, or update the configuration file and import it during a new session of the wizard.

Step 3 After reviewing your configuration click **Apply**.

Step 4 To enable Self-Provisioning, you must restart the Self Provision IVR service in Cisco Unified Communications Manager. You can use the **Call Processor** option to cross-launch Cisco Unified Communications Manager.

You can choose to add another service area, user role or navigate to the user provisioning page to add users.

You can use the **Show Detailed Configuration** option to view the configuration details. You can use the **Save Configuration Data** option to save the wizard configuration data as a batch project.

Step 5 Click **Done** to exit the wizard.

You can relaunch the wizard again and create a Domain, Service Area and update user role for another newly installed device.

Note The Getting Started wizard creates configuration templates for the infrastructure objects. These are read-only templates and cannot be edited or deleted.

Adding Devices

Procedure

Step 1 On the Device setup page, add the Unified Communications Processors and its details. Enable Unified Messaging and provide exchange server details to add an email account. See Unified Messaging Guide for Cisco Unity Connection for exchange server details.

Step 2 Click **Test Connection**.

The test connection succeeds if you have added Unified Communication processors that are 10.5 and above. When you close the wizard, the devices are added to the Inventory Manager and is listed in the Device Setup page. If you have added processors that are already configured (not a new install), a validation message appears, and you cannot proceed to the next step.

Note To Support Unified Communications Manager with/without TLS v1.0:

- Cisco Prime Collaboration Provisioning 12.x onwards communicates with Cisco Unified Communications Manager 12 using TLS v1.2 protocol, hence the handshake is successful and the connection is secured.
- Communication between Cisco Prime Collaboration Provisioning 11.5 and Cisco Unified Communications Manager 11.5 (SU3):
  a. Cisco Prime Collaboration Provisioning sends AXL requests via TLS v1.0 protocol to Cisco Unified Communications Manager (Minimum TLS version is not configured, i.e. default setting on Cisco Unified Communications Manager): Handshake is successful, then the connection is successful.
  b. Cisco Prime Collaboration Provisioning sends AXL requests via TLS v1.0 protocol to Cisco Unified Communications Manager (Minimum TLS version is configured as TLS v1.2 or v1.1 on Cisco Unified Communications Manager): Handshake fails, then the connection is unsuccessful. In case of failed scenario, the user needs to upgrade to the Cisco Prime Collaboration Provisioning version 12.x.

Step 3 Click **Save and Continue**.
he Save and Continue button is enabled only if the test connection succeeds. When you click **Save and Continue**, Infrastructure and User synchronizations are triggered for the newly added devices. You can view the synchronization status of these devices in the Infrastructure Setup page (Quick View of the device).

You will be notified if you are trying to add and save a device that already exists in Cisco Prime Collaboration Provisioning.

Step 4 Create a Domain for the processors you have added.

Note After installing or reverting the snapshot for Cisco Unity Connection, you must launch the Cisco Unity Connection user interface and wait for 10 - 15 minutes (because the device will take some time to initialize the third party libraries), before adding the Cisco Unity Connection device in the Getting Started wizard. Otherwise, the test connection may fail.

Infrastructure Objects Created by the Wizard

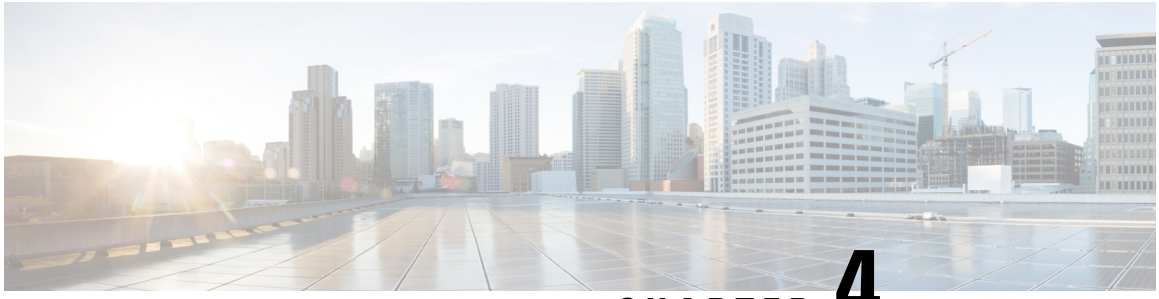
The table below lists some of the Infrastructure Objects created during the Getting Started Wizard setup.

Table 8: Infrastructure Objects

Infrastructure Objects
Route Partition (for Phones)
Calling Search Space (for Phones with Partition)
Integration Objects (Unified CM and Unity Connection) created on Unified CM
Device Mobility Group
Media Resource Group

Infrastructure Objects
IOS Enhanced Conference Bridge
IP Phone Services
Service Parameter
SIP Trunk Security Profile
SIP Profile
SIP Trunk
Partition for Voicemail
Calling Search Space
Voicemail Pilot with Pilot Number
Voicemail Profile with Voicemail Pilot
Route Pattern
Integration Objects created on Unified CM and IM&P
SIP Trunk Security Profile
Service Parameter
SIP Trunk
LDAP Integration Objects created on Unified CM
LDAP System
LDAP Authentication
LDAP Directory
Infrastructure Objects created on Unity Connection
External Service
Port
VoiceMail Port
Port Group
Class of Service
Subscriber Template with CoS
Infrastructure Objects (Cisco IM&P) created on Unified CM
Gateway Setting
TFTP Server
Presence Configuration Settings
Infrastructure Objects created for Self-Provisioning
CTI Route Point

Infrastructure Objects
Self Provisioning
Universal Device Template
Universal Line Template
Unified CM Group
Unified CM
User Profile
Infrastructure Objects created for Cisco Jabber
UCService for CTI
UCService for IM&P
UCService for Voicemail
UCService for MailStore
UCService for LDAP
SIP Profile
Service Parameter
SoftKey Template
Service Profile
Infrastructure Objects created for Service Area (Site)
Date Time Group
Device Pool
Cisco IOS Conference Bridge
Phone NTP Reference
Universal Device Template
User Profile **Note** You can refer the siteobjects.txt file located at /opt/cupm/sep/deploy/dfc.ear/dfc.war/ipt/gsWizard/pcp-config.zip to view the list of infrastructure objects created for a Service Area.



CHAPTER 4

Managing Devices in Prime Collaboration Provisioning

Managing Devices Overview

To use Cisco Prime Collaboration Provisioning, you must first add the IP communications infrastructure devices that are part of your IP telephony environment.

After adding devices, you synchronize the data in Cisco Unified Communications Manager, Cisco Unity systems, and Cisco IM and Presence with Cisco Prime Collaboration Provisioning. This populates Cisco Prime Collaboration Provisioning with the existing active users and services, and provides a consolidated view of all of the infrastructure and user information.

Provisioning also provides support for Cisco IOS routers. When a Cisco IOS router device is added to Prime Collaboration Provisioning, it appears in Cisco Prime Collaboration Provisioning as a Generic IOS Router. Through the Generic IOS Router capability, Cisco Prime Collaboration Provisioning can configure additional voice functionality on the router.

Call Processors are proxies for each instance of a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express device. Unified Message Processors are proxies for each instance of a Cisco Unity Express, or Cisco Unity Connection device. Unified Presence Processors are proxies for each instance of Cisco IM & Presence. You will find these terms used in place of their respective devices.

Adding Devices

You must add devices to Cisco Prime Collaboration Provisioning to provision services for users. For a list of devices you can add to Cisco Prime Collaboration Provisioning, see Supported Devices for Prime Collaboration Provisioning.

Note the following points while you are adding a device to Cisco Prime Collaboration Provisioning:

- Before you add devices to Cisco Prime Collaboration Provisioning, you must ensure that Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Unity Connection, Cisco Unity Express devices are configured correctly. For details on configuring these devices, see Setting Up Devices for Prime Collaboration Provisioning.
- For infrastructure devices (Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco Unified Presence) that are setup in a cluster environment, add the publisher information and credentials only.
- There are some significant differences in how a Generic IOS Router is set up in Cisco Prime Collaboration Provisioning in comparison to a Cisco Unified Communications Manager or a Cisco Unity device. Most notably, Generic IOS Routers are not synchronized and they are not associated to a Domain or a Service Area.
- Before you can create a Call Processor based on a Cisco Unified Communications Manager Express in Cisco Prime Collaboration Provisioning, you must:
  - Disable the auto-allocation of directory numbers. Do this through the Cisco IOS interface.
  - Disable the ephone auto-registration for Cisco Unified Communications Manager Express.

To add devices to Provisioning:

Procedure

Step 1 Choose **Device Setup**.

Step 2 In the Device Setup page, click **Add** to add devices to Cisco Prime Collaboration Provisioning.

Step 3 In the Add Device window, select the required application from the drop-down list and enter the necessary information such as Name, IP address, and so on. See the tables below for field descriptions.

Note For the device name, valid values are space, alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), and at sign (@).

Note In case of setting a password for Cisco Unity Connection, you cannot use a semicolon as the Cisco Unity Connection Interface does not allow it.

Note To add Unity Connection versions 10.x or higher to the Cisco Prime Collaboration Provisioning Device setup page, you need to configure a proxy user on the Unity Connection server.

Step 4 (Optional) Click **Test Connection** to check the connectivity of the device with respect to name, IP address, application, version, username, and password. You can test connection without saving the device.

Note Test Connection is not supported for Deployment Manager, Prime License Manager, Expressway Edge, and Expressway Core.

Step 5 Click **Save**.

Devices are added to Cisco Prime Collaboration Provisioning. You can see two status messages appearing at the bottom of the page. One on whether the addition of the device was successful or not, and another on the Test Connection stating whether the connectivity test was successful or not. Devices with multiple applications are added as separate devices in the table.

Note While adding Cisco Unity Connection 10.0 and above versions, you must configure both Unity Connection administrator and Operating System (OS) administrator credentials.

Cisco Unity Connection OS Administrator Name and Password are the proxy user credentials.

To create proxy user, login as administrator in Cisco Unity Connection and enter the following CLI commands:

```
utils cuc proxy usrcreate
utils cuc proxy usrpasswd
utils cuc proxy enable
```

To view the details of the device, hover over **Quick View**. You can start synchronization, view synchronization logs, test the connectivity of the device, and cross launch Cisco Unified CM Serviceability and Cisco Unity Connection Serviceability from Quick View. The Quick view also displays the status of Jabber service (enabled from Unified Communication Services pane and Getting Started wizard) and Self-Provisioning (enabled through Getting Started wizard) for the device.

To update or change the device details, click **Edit**.

Some devices have more than one application on it (devices with same IP address). If you are adding devices with more than one application on it, add the first device and save it. After the device is successfully added to Provisioning, add the device again, selecting the second application. Save the device. Both the devices appear in the Device Setup table.

You can add Prime License Manager and Deployment Manager from the Infrastructure Setup page. After you add these devices, Prime License Manager and Deployment Manager links are displayed under the Administration menu. Click on the Prime License Manager or Deployment Manager link to cross launch the Prime License Manager or Deployment Manager login page.

Note You can add only one Prime License Manager and Deployment Manager device to Cisco Prime Collaboration Provisioning. If you try to add another Prime License Manager or Deployment Manager device, an error message is displayed.

Table 9: Call Processor Fields

Field	Description
LDAP Integration	

Field	Description
	Following are the options: • None—Select this option if you have not enabled both LDAP synchronization and authentication in Cisco Unified CM, and want to push users from Cisco Prime Collaboration Provisioning user interface onto the UC applications. **Note** For Cisco Unified CM 10.5(1) and above: • For Brownfield deployments, where Cisco Unified CM and Cisco Prime Collaboration Provisioning are already LDAP-integrated separately, set the flag as "Synchronization and Authentication". • For Greenfield deployments, we recommend you to set the flag as "None". If you select this option, Cisco Unified CM need not synchronize with AD to authenticate users. When a new user is created in Cisco Prime Collaboration Provisioning, and if Cisco Unified CM is set to Authenticate Only with LDAP, then the user account is pushed into Cisco Unified CM and the user is marked as an LDAP synchronized user in Cisco Unified CM. This functionality ensures that Cisco Unified CM contains only users that have services assigned to them. • Synchronization—Select this option if you have enabled LDAP synchronization alone in Unified Communications Manager. • Synchronization and Authentication—Select this option if you have enabled LDAP synchronization and authentication in Unified Communications Manager. The value you choose must exactly match the value configured in Cisco Unified Communications Manager. If Cisco Unified Communications Manager is integrated with an external LDAP, users are not

Field	Description
	created through Provisioning; instead they are synchronized through Cisco Unified Communications Manager. While provisioning a service, if a user is not available on Cisco Unified Communications Manager, the workflow subsystem waits for a predefined period of time (24 hours by default) for the user to be available on Cisco Unified Communications Manager and then continues provisioning the service. The 24-hour period can be configured on Provisioning in the ipt.properties file. Change the following settings: • dfc.oem.extdir.retries: 24 • dfc.oem.extdir.retry_interval: 3600 **Note** To modify the ipt.properties file, contact Cisco TAC. **Note** You must restart Cisco Prime Collaboration Provisioning if you make any changes to ipt.properties file. **Note** LDAP integration is available only for Cisco Unified Communications Manager versions 5.0 and later. For details on single LDAP synchronization, refer the note below this table.
Extension Mobility Details (Optional)	
Service Name	The name of the Extension Mobility Service configured on a Call Processor.
Service URL	The URL of the Extension Mobility Service configured on the Call Processor: http://<ip-address>/ emapp/EMAppServlet?device=#DEVICENAME# Where ip-address is the name or the IP address of the server where Extension Mobility is installed. **Note** The Service Name and Service URL you enter in Cisco Prime Collaboration Provisioning should match the Service Name and Service URL in Cisco Unified Communications Manager.

Note **Single LDAP Synchronization**

Cisco Prime Collaboration Provisioning 10.5.1 and above versions along with Cisco Unified CM 10.5.1 and above versions support a feature called single LDAP synchronization, which eliminates the need to have different LDAP synchronization policies.

During single LDAP synchronization, Cisco Prime Collaboration Provisioning alone is LDAP integrated. Cisco Unified CM is configured with LDAP Directory and authentication information. Cisco Prime Collaboration Provisioning synchronizes users from LDAP. And when the user information is pushed into Cisco Unified CM, Cisco Prime Collaboration Provisioning marks appropriate flags through which Cisco Unified CM identifies the user as LDAP synchronized user. **Remember:**

- This feature is supported only with Cisco Unified CM and not with other UC applications like Cisco Unity Connection and Cisco IM & Presence.
- This feature is supported only with Cisco Prime Collaboration Provisioning10.5.1 and above, when used with Cisco Unified CM 10.5.1 and above.
- LDAP Directory information in Cisco Prime Collaboration Provisioning and Cisco Unified CM should match. Any out-of-band changes in Cisco Unified CM require Cisco Unified CM user synchronization.

For Greenfield deployments: Cisco Prime Collaboration Provisioning takes care of pushing the required LDAP configurations into Cisco Unified CM. The LDAP integration flag is set to "None".

For Brownfield deployments: Where Cisco Unified CM is already LDAP integrated and users are synchronized into Cisco Unified CM, you are recommended to use the existing LDAP policies in Cisco Prime Collaboration Provisioning and Cisco Unified CM as is. The LDAP integration flag is set to "Synchronization & Authentication".

Table 10: Unified Message Processor Fields

Field	Description
Voicemail Pilot Number This option is available only in the Getting Started Wizard.	Directory number dialed to access voicemail messages.

Field	Description
LDAP Integration **Note** This option is available only for Cisco Unity Connection.	Specifies whether Cisco Unity Connection is integrated with an external LDAP. If you select Yes, while provisioning voicemail account, Cisco Prime Collaboration Provisioning searches the LDAP users list in Cisco Unity Connection. If the user name is available in the list, it imports the user details and provision a voicemail account. If you select No, Cisco Prime Collaboration Provisioning does not search the LDAP users list and follows the normal process for provisioning voicemail account. **Note** It is always recommended to run LDAP synchronization in Unity Connection before performing LDAP synchronization in Cisco Prime Collaboration Provisioning.
Username	This field is case-sensitive. The username supplied in this field should match the following: • Cisco Unity Connection—Any user with Cisco Unity Connection administrator privileges. • Cisco Unity Express—Username of the router where Cisco Unity Express is installed.
Password	This field is case-sensitive. The password supplied in this field should match the following: • Cisco Unity Connection—Administrator password. • Cisco Unity Express—Password for the router where Cisco Unity Express is installed.

OS Administrator Name
Note This option is available only for Cisco Unity Connection 10.0 and above.
	Enter the proxy username in this field.
	To create a proxy user, login as administrator in Cisco Unity Connection and enter the following CLI commands:
	`utils cuc proxy usrcreate`
	`utils cuc proxy usrpasswd`
	`utils cuc proxy enable`

OS Administrator Password **Note** This option is available only for Cisco Unity Connection 10.0 and above.	Enter the proxy password in this field.

Field	Description
Enable Password	Enable password for the router where Cisco Unity Express is installed.
Create by Import	Indicates whether a new account should be created on an Exchange server for new voicemail accounts created in Cisco Unity. If selected, creating user accounts on the Exchange server is prevented. User accounts are associated only if they already exist on the Exchange server.
(Optional) Line User Name	Username for the Cisco Unity Express module.
Line User Password	Password for the Cisco Unity Express module.
Service Engine Interface Number	The interface number of the Cisco Unity Express service engine on the router.

Table 11: LDAP and ACS Server Configuration Fields

Field	Description
LDAP Server Type	Type of LDAP server. The types are: • Microsoft Active Directory • Microsoft ADAM or Lightweight Directory Services • AD 2012 • Sun One • Oracle Directory Server • OpenLDAP For information about the Microsoft AD versions supported by Cisco Prime Collaboration Provisioning, see Supported Devices for Prime Collaboration Provisioning.
Server Port	Port number for the AAA server. Default Non-Secure port: 389 Default Secure port: 636
Backup Server Port	Port number for the backup AAA server.
Backup Server IP Address	IP address of the backup server.

Field	Description
Admin Distinguished Name	The administrative user ID of the LDAP manager that has access rights to the LDAP directory. For example, a user, John Doe, with userID = jdoe must enter John Doe. **Note** If admin is a user in windows domain Cisco, just enter admin (username with domain prefix such as cisco\admin does not work).
Admin Password	The administrative users password (LDAP manager).

Field	Description
LDAP User Search Base	

Field	Description
	This should be the search base of the Admin user account entered in "Admin Distinguished Name". This is used for connection tests. **Note** Domain LDAP Synchronization and User LDAP Authentication uses the search base defined in domains for synchronization and authentication. LDAP server searches for users under this base. You must enter the CN or OU details when you enter the search base. Just dc=cisco, dc=com do not work; you must also specify the CN or OU part. For example, cn=users, dc=eta, dc=com. If you have configured two different user groups, for example, • OU=Organization, OU=Accounts, DC=aaa, DC=com • OU=Service, OU=Accounts, DC=aaa, DC=com The search base to be entered is OU=Accounts, DC=aaa, DC=com. If a user in OU=Organization user group is configured as Admin DN, then all the users in Organization user group can login to Prime Collaboration, but the users in Services user group cannot login. Similarly, if a user in OU=Services user group is configured as Admin DN, then all the users in Services user group can login to Prime Collaboration, but not the users in Organization user group. If you configure a user in top level as Admin DN, then all the users under that level can log into Prime Collaboration. For example, if a user in OU=Accounts user group is configured as Admin DN, then all the users in Organization and Services user groups can login to Prime Collaboration. **Note** • LDAP authentication fails if you enter special characters in the search base. • OU is for Oracle, and CN is for Windows LDAP Example: • For Windows LDAP Server: Admin Distinguished

Field	Description
	Name-CN=administrator, CN=Users, DC=pcp, DC=cisco, DC=com LDAP User Search Base--CN=Users, DC=pcp, DC=cisco, DC=com • For Oracle Server: Admin Distinguished Name-OU=Oracle, OU=Users, DC=pcp, DC=cisco, DC=com LDAP User Search Base--OU=Users, DC=pcp, DC=cisco, DC=com
Use SSL	You should check this check box if Cisco Prime Collaboration Provisioning should use Secure Socket Layer (SSL) encryption for the transmission channel between Cisco Prime Collaboration Provisioning and the AAA server.
ACS Authentication Protocol	Protocol used by the ACS server for authentication.
Enable Data Encryption	Enables data encryption between Cisco Prime Collaboration Provisioning and the ACS server.

Working with Cisco Unity Connection Device

Cross-launching Serviceability from Infrastructure Setup

For Cisco Unity Connection clustering and failover support, be aware of the following:

- When adding a Cisco Unity Connection that includes a Cisco Unity Connection cluster server pair, add the publisher and Subscriber server of the pair.

If a network has more than one location, individually add all of the locations for either the Cisco Unity Connection server or Cisco Unity Connection cluster to Cisco Prime Collaboration Provisioning.

If Cisco Unity is used in the configuration, configure the Cisco Unified Communications Manager voicemail ports.

For more information on these devices, see Setting Up Devices for Prime Collaboration Provisioning.

Cisco Prime Collaboration Provisioning allows an administrator to cross launch Cisco Unity Connection Serviceability and Cisco Unified Serviceability from the configured Cisco Unity Connection and Cisco Unified Communications Manager respectively.

Note Cross launching serviceability is supported for Cisco Unified Communications Manager and Cisco Unity Connection devices only.

When you cross-launch serviceability, you can access the serviceability UI and perform any operation directly on the server of that device. To learn about serviceability in Cisco Unified Communications Manager, see theCisco Unified Serviceability Administration Guide. Similarly, to learn about serviceability in Cisco Unity Connection, see Administration Guide for Cisco Unity Connection Serviceability for details.

With the cross-launching serviceability feature, Cisco Prime Collaboration Provisioning facilitates you to activate, deactivate, start and stop services (directly) on all managed nodes. Rest your mouse pointer over Cisco Unified Communications Manager or Cisco Unity Connection in the device table, and click the quick view icon to view the **Serviceability** cross launch link under the Actions pane.

Adding Cisco TelePresence Management Suite

You can enable scheduling for video endpoints by adding a Cisco TelePresence Management Suite (TMS) device that synchronizes with Cisco Unified Communications Manager to discover devices. Note that the scheduling is executed only in Cisco TMS and you can launch the scheduling UI from Prime Collaboration Provisioning.

Procedure

Step 1 Add Cisco TMS (see the procedure on Adding Devices).

Step 2 Associate an application user to Cisco TMS. For each Cisco Unified Communications Manager that you want to provision, you can select the application user to be associated with Cisco TMS. Choose **Device Setup. Hover over Quick View and Click UC Services tab**. Under **TMS Service**, select an application user for a Cisco Unified Communications Manager, and click **Apply**.

Note that the application user must belong to these groups: Standard CCM Admin Users and Standard CTI Enabled and have one of the following roles:

Standard AXL API Access, Standard CCM Admin Users, Standard CTI Enabled, Standard CUReporting, Standard RealtimeAndTraceCollection, Standard SERVICEABILITY

Step 3 Provision an endpoint. See Ordering Service for a User.To enable scheduling: In the **Service Specific Configuration Layout**, click **Enable Scheduling**.

The endpoint is added and provisioned on the Cisco Unified Communications Manager for an application user that is associated to the specific Service Area.

Note When you create a new order for an endpoint, you could have many services pointing to different Cisco Unified Communications Managers. In this case, you must select the Service Areas applicable for the respective Cisco Unified Communications Manager (under Unified Communication Services).

Deleting Devices

To completely remove a device from Cisco Prime Collaboration Provisioning, you must delete it through the Infrastructure Setup page. Note the following points when you are deleting a device:

- No active released orders, including unrecoverable or recoverable errors.
- No active batch projects.
- No synchronizations in progress.

  If these conditions are not met, a message appears on the page when you attempt to delete a device. Avoid performing any activities until the deletion is complete.

- Before deleting a AAA server, ensure that it is not assigned to a Domain.
- There must not be any pending orders on the device.
- Before deleting a device, ensure that you perform a domain synchronization to avoid any stale entries into the system.

To delete devices:

Procedure

Step 1 Put Cisco Prime Collaboration Provisioning in maintenance mode. (See Maintenance Mode, on page 329.)

Step 2 Choose **Device Setup**.

Step 3 In the Device Setup page, select the device you want to delete and click **Delete**.

Step 4 In the confirmation dialog box, click **OK** to confirm deletion.

Enabling Cisco Jabber Services

You can enable Cisco Jabber services for devices in Cisco Prime Collaboration Provisioning. Cisco Jabber services allow you to interact with instant messaging and presence.

From 10.6, with the Administrator privileges, you can select up to four Cisco Jabber types:

- Cisco Jabber for Desktop
- Cisco Jabber for Android
- Cisco Jabber for iPhone
- Cisco Jabber for Tablet

Note Cisco Jabber service is available for Cisco Unified Communications Manager 9.1.1 and above version, and Cisco Unified Presence only.

To enable Cisco Jabber service for a call processor:

Procedure

Step 1 Choose **Device Setup**.

Step 2 Hover over Quick View of the device and click the UC Services tab and click **Enable**

Step 3 Enter the SIP Profile, Service Profile, Softkey template fields and Service Parameter information, and click Apply. See Infrastructure Data Object Fields, on page 337 for information on these fields. You can click View Order to see the order details in the User Record page. The date when the Jabber Service is enabled is displayed.

Note Once you enable Cisco Jabber service for a call processor, you cannot edit or disable it.

Configuring Conference Now Service

You can enable, disable or edit Conference Now services for devices. By enabling Conference Now service, you can setup an IVR (Interactive Voice Response) guided conference calls from your device. You can enable Conference Now service using batch provisioning or quick UI.

After enabling the Conference Now service, you can provision this service to the user in the User Service Ordering page. To enable this service to the user see,Table 66: User Services Entry Fields, on page 289.

The user can modify the Conference Now end-user settings in the self-care UI, only if Conference Now service is enabled for the user. For more details see, Table 55: User Settings, on page 248.

Note Conference Now service is available only for Cisco Unified CM 11.x and later versions.

You must have minimum one media resource group list and calling search space configured in the Unified Communications Manager to enable Conference Now service.

To enable or edit Conference Now service:

Procedure

Step 1 Choose **Device Setup**.

Step 2 Mouse over the information icon against the desired device name. The **Device Details** quick view appears.

Step 3 In the **Device Details** quick view, click the **UC Services** tab.

Step 4 Click **Enable/Edit** against the Conference Now service.

Note The **Edit** button appears, when the conference now service is enabled for the device.

The **Enable** button will be dimmed if there are no media resource group list or calling search space configured in the Unified Communications Manager.

Step 5 Enter the required details in the **Conference Now Service** page and click **Apply**. For details about these fields, see Table 12: Conference Now service fields. An asterisk next to a field indicates a mandatory field.

Note To disable Conference Now service, click **Disable**.

Table 12: Conference Now service fields

Field	Description
Conference Now IVR Directory Number	Enter a DID (Direct Inward Dial) number for a Cisco Unified Communication Manager cluster so that external callers can access this number
Description	Enter the description.
Route Partition	Select an existing route partition or create a new route partition as required. • To Select an existing route partition, click **Use Existing** radio button, and choose an existing partition from the drop-down list. • To create a new route partition, click **New** radio button, and enter the route partition name in the text box. Route partition is used to restrict access to the Conference Now number or pattern
Maximum Wait Time For Host	Choose the time in minutes for the participants to wait for the host to join the conference. This field specifies the maximum wait time for an attendee before a host joins the meeting. If the host has not yet joined the meeting. After the timer expires, the attendee is disconnected automatically.
MOH Source While Participant is Waiting	Choose an MOH (Music On Hold) source to be played, while the participant is waiting for the host to join the conference. If nothing is selected, the default Network Hold MOH/MOH Source configured on the service parameter is used.
Media Resource Group List	Choose the media resource group list to associate with IVR (Interactive Voice Response) Media Resource.
Calling Search Spaces	Choose a calling search space to add to the selected route partition.

Troubleshooting

Issue : Conference Now Service button is dimmed.

Recommended Action

Check whether the required objects (Media Resource List and Calling Search Space) are configured in Cisco Unified CM.

- If the objects are configured in Cisco Unified CM, perform infrastructure synchronization.
- If the objects are not configured in Cisco Unified CM, add them via batch provisioning or infrastructure configuration UI.

Configuring Emergency Location Service

Emergency location service is used to determine the caller's location when an emergency call is placed. It is designed for very small customer environments of about 100 emergency numbers.

The following infrastructure object must be configured to use Emergency Location Service. You can configure these objects using batch provisioning or quick UI.

- Route Pattern.
- Translation Pattern.
- Device Pool.
- Emergency Location (ELIN) Group.

You can view the details of the Emergency Location (ELIN) group associated with the device pool defined in respective service area in the Service Area report page. You can also view the status of Emergency Location (ELIN) Service associated with the service area in the service area quick view, while ordering service for the user.

Note Emergency Location service settings are applicable only if the emergency location support is enabled in the Cisco Unified Communications Manager.

You must have minimum one route pattern and translation pattern configured in the Unified Communications Manager to enable Emergency Location service.

Emergency Location service is available only for Cisco Unified CM 11.x and later versions.

You can enable, disable or edit the existing settings of Emergency Location service in Cisco Prime Collaboration Provisioning.

To enable or edit Emergency Location service:

Procedure

Step 1 Choose **Device Setup**.

Step 2 Mouse over the information icon against the desired device. The **Device Details** quick view appears.

Step 3 In the **Device Details** quick view, click the **UC Services** tab.

Step 4 Click **Enable/Edit** against the Emergency Location service.

Note The **Edit** button appears, when the Emergency Location service is enabled for the device.

The **Enable** button will be grayed out if no route pattern or translation pattern is configured in the Unified Communications Manager.

Step 5 In the Emergency Location service page add ELIN group. To add ELIN group, see Adding ELIN Groups.

Select the required **Route Patterns** and **Translation Patterns**. For details about these fields, see Table 13: Emergency Location service fields, on page 62.

Note To disable Emergency Location Service, click **Disable**. Disabling emergency location service results in the following changes in Unified Communications Manager : ELIN groups will be deleted, device pools will be disassociated from the ELIN groups, and ELIN settings in translation and route patterns will be disabled. These changes are updated in Cisco Prime Collaboration Provisioning after the subsequent infrastructure synchronization or change notification.

Troubleshooting

- **Issue :** Emergency Location Service button greyed out

  Recommended Action :

  Check whether the required objects (Translation Pattern and Route Pattern) are configured in Cisco Unified CM.

  - If the objects are configured in Cisco Unified CM, perform infrastructure synchronization.
  - If the objects are not configured in Cisco Unified CM, add them via batch provisioning or infrastructure configuration UI.

- **Issue :**Emergency Location Service is enabled in the device, but Service Area quick view shows Emergency Location is disabled.

  Recommended Action : Enable Emergency Location on the Device Pool associated with the Service Area using batch provisioning.

Adding ELIN Groups

ELIN group is a collection of ELIN numbers, each group should have as many ELINs created as are needed to support simultaneous emergency calls. For example, to support five simultaneous calls five ELINs would be needed in an ELIN group.

To add ELIN groups :

Procedure

Step 1 Click **ADD** in the emergency location service page.

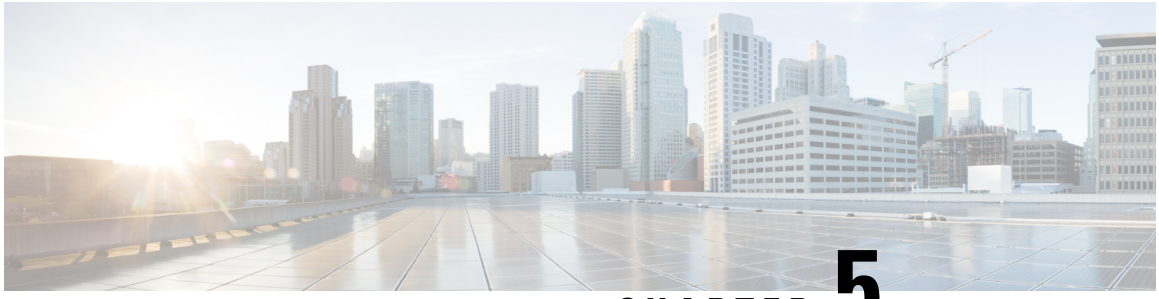
Step 2 Enter the ELIN group name, ELIN number and select the partition. You can add or remove ELIN number and partition by clicking the + or - button. Select the required device pool to associate with the ELIN group.

Step 3 Click **Save**.

Note To update the ELIN group details, select the required ELIN group and click **Edit** .

Table 13: Emergency Location service fields

Field	Description
ELIN group name	Enter a unique name for the emergency location group. ELIN group name can only contain alphanumeric characters (a-z, A-Z, 0-9), period (.), space, underscore (_) and hyphen (-).
ELIN number	Enter unique DID numbers registered in the Public Safety Answering Point (PSAP).
Partition	Select the partition that contains the numbers used by the PSAP to call into the network.
Device Pool	Select the device pools to which the ELIN group must be associated. You can associate ELIN group to multiple device pool. You can also associate ELIN group to the device pool in Device Pool Infrastructure Configuration Product Fields. For details, see Device Pool Infrastructure Configuration Product Fields.
Route Pattern	Select the route pattern that can route emergency calls to the local public safety answering point (PSAP). You can configure the route pattern to route the emergency call by checking **Is an Emergency Services Number** checkbox in Route Pattern Infrastructure Configuration Product Fields. For details see, Route Pattern Infrastructure Configuration Product Fields.
Translation Pattern	Select translation pattern that can manipulate and identify the dialed digits as emergency service number before it routes a call. You can configure the translation pattern to identify the emergency call numbers by checking **Is an Emergency Services Number** checkbox in Translation Pattern Infrastructure Configuration Product Fields. For details see, Translation Pattern Infrastructure Configuration Product Fields.



CHAPTER 5

Managing Domains, Service Areas, User Roles, and Service Templates

Overview of Domains, Service Areas, User Roles and Service Templates

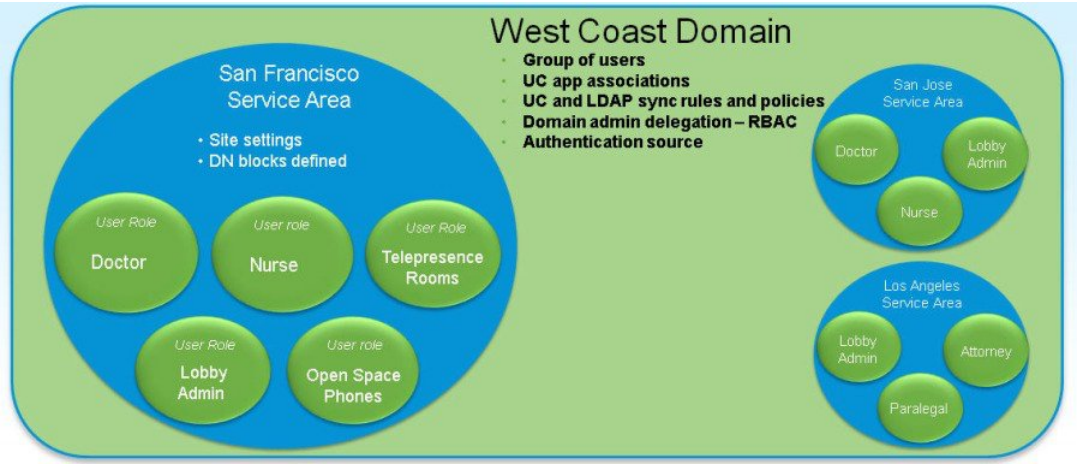
After adding devices, you must first create domains, and then add Service Areas, User Roles and Service Templates.

To set up user provisioning:

1. Add and configure Domains—Includes adding and configuring domains, which defines the operational capabilities for a group of users.
2. Add and configure Service Areas—Includes configuring Service Areas, that is, selecting route partitions, and device pool; specifying user types that have access to the Service Area; and configuring directory number blocks.
3. Add and configure User Roles—Includes adding User Roles and assigning services that can be provisioned by a specific user role type.
4. Add and configure Service Templates—Includes configuring Provisioning Attributes which are configuration settings applied to a service at the time of activating the service.

In Cisco Prime Collaboration Provisioning 10.0 and above versions, the User Provisioning Setup page (choose Provisioning Setup) is simplified to set up all your user provisioning tasks. A centralized view allows you to manage Domains, Service Areas, User Roles and Service Templates in a single user interface.

Figure 2: Domains, Service Areas, and User Roles



Deployments can be based on the geographical location. In the above example, the voice deployment is planned for cities in the West Coast region. West Coast is the Domain. The domain sync rules, policies and administrator permissions are defined in the West Coast domain. San Jose, Los Angeles, and San Francisco are the Service Areas. Doctor, Nurse and Lobby assistant user roles within these cities must be provisioned with IP Telephony and Messaging Services. These IP telephony and messaging services are defined within the service templates. The Doctor and Nurse user roles are assigned with service templates that allow them to make international calls, whereas the service templates defined for Lobby user role allow local calls only.

In the User Interface (Provisioning Setup), you can see the Domains, Service Areas, User Roles, and Service Templates listed in the left pane. The corresponding tables are listed in the right pane. The Domains table is displayed by default when you enter the Provisioning Setup page. Click **All Domains** to see a list of all the domains. Click the arrow icon to expand. When you expand a Domain, you can see the Services Areas, User Roles and Service Templates of that Domain. Further, when you expand Service Areas and User Roles, you can see multiple service areas, and list of User roles associated to that Domain.

Adding a Domain

Domains are groupings of users. For each grouping, one or more system users can be authorized to manage services for users within that Domain. In addition, rules or policies may be set on a Domain; those rules and policies apply to services for users in that Domain. Common policies can also be applied on operations within a Domain.

A user can manage more than one Domain (if the user is assigned the proper authorization role). All of the user's services are provisioned in the Service Area that you specify while adding the user (to add a user, choose User Provisioning).

After creating a Domain, you can add Service Areas and User roles that have access to your new Domain. You can also create service templates and assign them to a Service Area and User Role. A Service Template can be associated to several such combinations of Service Areas and User Roles.

To create a domain:

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 Click **Add**, to add new domains in the **Domains** page.

Step 3 Enter the necessary fields such as Call Processors, Message Processors, synchronization rules, LDAP settings and so on, and click Save. You need to provide a Domain Name for the Name field. Valid values are space, alphanumeric characters (A-Z, a-z, 0-9), and the following special characters: _ - . / : ; = ? @ ^ ‘ { } [ ] | ~.

You can set the Domain Synchronization rules in the Synchronization Rules pane. Select the Synchronization Rules for Cisco Unified Communications Manager and Unity Connection. Mouse over the (?) icon for details on the specific synchronization rule.

- Perform Domain synchronization after configuring a Domain.

To edit an existing domain, expand the list of Domains in the left pane, and click a particular Domain to edit. You can also click **All Domains** and then select a domain from the table and click **Edit**.

Related Topics

Adding Service Areas, on page 66
Adding User Roles, on page 71
Business Rules for Domain Synchronization, on page 102
Configuring Business Rules, on page 176
Overview of Domain Synchronization, on page 99
Synchronizing an LDAP Server with Provisioning, on page 108

Deleting a Domain

When a Domain is deleted, Service Areas, users roles, Service Templates, rules, directory number blocks, and user roles are removed. Endpoint, Directory Number, license capabilities, and instances of Unified Presence user settings are moved to Global Resources namespace.

While the Domain deletion is in progress, avoid performing any activities in that Domain until the Domain deletion is complete.

Before you delete a Domain, the system must be in maintenance mode. Also, the following prerequisites must be satisfied for deleting a domain:

- No active released orders, including unrecoverable or recoverable errors.
- No active batch projects.
- No Domain synchronization in progress.
- No Call Processor or Unified Message Processor synchronization in progress.

Procedure

Step 1 Put Cisco Prime Collaboration Provisioning in maintenance mode (see Maintenance Mode, on page 329).

Step 2 Choose **Provisioning Setup**.

Step 3 Select the Domain you want to delete, and click **Delete.**

Step 4 Click **OK**.

Refresh the Domain list page to see the status.

Service Areas

Service Areas are groupings within a Domain that are used to structure and manage the required IP telephony and messaging services across geographic, organizational, or technological boundaries. The Service Area typically acts as a service offering location and provides a template mechanism that determines provisioning attribute values used during order processing.

The Service Area determines the mappings from the business view of the service to the technology delivering those services.

A Service Area also handles Cisco Unified CM partitioning and class of service by directing which location, device pool and route partition assignments to use for any user provisioned into that Service Area.

For example, on a Service Area associated to a Cisco Unified Communications Manager, the Service Area defines the device pool, route partition, location, and external phone number mask that the products will use within Cisco Unified Communications Manager.

In this case, when you configure a Service Area, you have a list of route partitions that can be assigned to it based on the selected Call Processor for the Service Area. If the Service Area does not have any associated route partition, then the directory numbers and lines are created in the default route partition in Cisco Unified Communications Manager. Service areas also determine the key voicemail settings and call forwarding behaviors.

Ensure Synchronization is completed for the Cisco Unified CM while creating the Service Area. You can map the call processor objects (such as Route Partition, Device Pool, and Location) to the Service Area only after the synchronization.

For Cisco Unity Connection Unified Message Processors, if you assign a Unified Message Processor to a Service Area, the Subscriber Template (with or without the TTS feature) and Subscriber CoS (with or without the TTS feature) can be configured. These templates can be used for voicemail provisioning of users in the Service Area.

Note For Service Areas with Call Processors based on Cisco Unified Communications Manager Express, only device pools are available for selection. Route partitions are not available.

Adding Service Areas

When configuring a Service Area, you can do the following:

- Map the Service Area to the corresponding Call Processor objects by specifying its Call Processors and related objects (for a Cisco Unified Communications Manager, some examples are route partition, and device pool), Unified Message Processor, and Unified Presence Processor.

If you have added a Call Processor in the domain through the Getting Started wizard, the fields like Calling Search Spaces (CSS), Region, Location, and device pool are automatically configured.

- Specify the user types for the Service Area (only users within a Service Area can order products from it).

  The Employee user role is the default based on the Domain rule DefaultUserType.

- Create directory number blocks for the Service Area users.
- Unified Presence Processor settings will list the Presence processor if the selected Call Processor has associated Presence processors.

Note After a Service Area is assigned to a Domain, it cannot be moved to a different Domain. Further, after a Call Processor, Unified Message Processor, or Unified Presence Processor is assigned to a Service Area, it cannot be changed.

To add a Service Area:

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 In the**All Domains** pane, expand a specific domain, and click **Service Areas**.

Step 3 Select the Domain for which you want to create a Service Area.

Step 4 Click **Add**.

Step 5 In the **Service Area Configuration** page, enter the necessary fields and click **Save**. The table below describes the necessary fields.

To edit an existing Service Area, expand the list of Service Areas in the left pane, and click a particular Service Area to edit. You can also select a Service Area from the table and click **Edit**.

You can select a Service Area from the table and click **Copy** to take a copy of existing service area information.

Table 14: Service Area Configuration Fields

Field	Description
Common Device Config	Configuration of common device settings for the Service Area. The following settings are controlled by Common Device Configuration: • Softkey Template • User Hold MOH Audio Source • Network Hold MOH Audio Source • User Locale • MLPP Indication • MLPP Preemption • MLPP Domain **Note** This field appears only if you select Cisco Unified Communications Manager 6.0.
Location	Location to be assigned to a device. When adding a service area, this field is optional provided you have added one of the call processors associated with the domain through the Getting Started wizard.
Partition	Route partition for the Service Area. This is the same as a partition in Cisco Unified Communications Manager.
Device Pool	Device pool for the Service Area.
Voice Gateway References	Voice gateway references for the Service Area.
Exchange Server	To configure an external Exchange Server for IMAP in Cisco Unity Connection, on the Cisco Unity Connection system, go to **System Settings > External Services > Add New**, and fill in the required fields.
Subscriber Template	Subscriber Template to be used to enable unified messaging for a user in the Unified Message Processor.
Directory Number Blocks	Directory number block assigned for that Service Area.

- Common Device Config, Location, and Partition fields apply only to Cisco Unified Communications Manager.
- Subscriber CoS with TTS Enabled, and Subscriber CoS without TTS Enabled fields apply only to Unity and Unity Connection.

Related Topics

Automatic Service Provisioning, on page 75
Adding a Directory Number Block, on page 71

Deleting a Service Area

Before a Service Area can be deleted, the following conditions must be met:

- The system must be in maintenance mode.
- No active released orders, including unrecoverable or recoverable errors.
- No active batch projects.
- No Domain synchronizations in progress.
- No Processor synchronizations in progress.

If these conditions are not met, a message appears on the page when you attempt to delete a Service Area, telling you the operation will not start.

While the Service Area deletion is in progress, avoid performing any activities until the deletion of that Service Area is complete.

Procedure

Step 1 Put Cisco Prime Collaboration Provisioning in maintenance mode (see Maintenance Mode, on page 329).

Step 2 Choose **Provisioning Setup**

Step 3 Expand Domain, and click **Service Areas**.

Step 4 Select the required Service Area, and click **Delete**.

Step 5 In the confirmation dialog box, click OK to delete the service area.

Directory Number Blocks

Numbers within a directory number block are relative to the Cisco Unified Communications Manager on which they are being created. Cisco Prime Collaboration Provisioning handles directory numbers the same way as they are handled by Cisco Unified Communications Manager.

While creating an order for a service, if you are selecting a Service Area that does not have a directory number block, you can use only the chosen line number.

You can set up individual directory numbers using the Directory Number Inventory component. For more information, see Managing Directory Number, on page 184.

The table below describes the fields for creating a block of directory numbers.

Table 15: Directory Number Blocks Field Descriptions

Field	Description
Prefix	Directory number prefix.

Field	Description
First Number	Starting number for the block of directory numbers.
Last Number	Last directory number in the block.
Minimum Length	The minimum number of digits that a directory number can contain before the prefix is added. Used by the system to pad numbers with zeros.
Block Size	This field is populated after you save the Service Area page.

E.164 Support

If you are using Cisco Unified Communications Manager version 7.x or later, you can configure the international escape character, +, in Provisioning to allow your phone users to place calls without having to remember and enter the international direct dialing prefix/international escape code that is associated with the called party. Depending on the phone model, for example, dual-mode phones, your phone users can dial + on the keypad of the phone. In other cases, the phone user can return calls by accessing the call log directory entries that contain +.

The international escape character, +, signifies the international access code in a complete E.164 number format. For example, NANP numbers have an E.164 global format in the format +1 214 555 1234. The + is a leading character that gets replaced by service providers in different countries with the international access code to achieve global dial plans.

You can enter + or \+ to indicate the international escape character.

Remember the following while using E.164 format directory numbers:

- For directory numbers, you can configure the international escape character at the beginning of the number (prefix) only (for example, \+5678, +0034).
- To configure the international escape character for supported patterns, you can enter \+ or + in the pattern or directory number field.
- You can assign the E.164 format directory numbers to the ordered lines by using the Chosen Line option.
- E.164 support is not available for Cisco Unified Communications Manager Express.
- Unity Connection 9.0 and above versions support E.164 format Directory Number, so the original directory number (along with the + symbol) will be displayed in the extension number field.
- While ordering bundled products like Enhanced Phone Service, Unified Messaging Service, Messaging Service, and so on, if you select Auto-assigned Line type option, the Alternate Extension field will not be auto populated for voicemail product while creating the order. Alternate extension will be added at the back end at the available position and will be displayed when the order is completed.

  If you select Choose Line type option, Alternate extension will be auto populated at the available index (for example, 1, 2, 3, and so on) in the Voicemail Advanced Order Configuration page.
- Meet-Me patterns, Call Park patterns (and related call park features; for example, Directed Call Park), and Call Pickup patterns do not support the international escape character (+). Therefore, you cannot enter \+ in the pattern fields that are configured for these features in the Infrastructure Configuration page.

Provisioning supports "+" character in the Directory Number fields for the following:

- Directory Number (DN) Block (under Service Area)
- EM Access Line and RDP Line products
- Provisioning Attributes
  - Speed Dial
  - Busy Lamp field
  - Call Forward
- Infrastructure products
  - Distribution List
  - Basic Call Queuing

Adding a Directory Number Block

To add a new directory number block:

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 Expand Domain and Service Area in the left selector pane, and select the required Service Area.

Step 3 In the Directory Number Block(s) field, click the **Add Row**.

Step 4 Complete the fields as required and click **Save**.

Note The Minimum Length field indicates the minimum number of digits that a directory number can contain before the prefix is added. This is used by the system to pad numbers with zeros. For example, if prefix = 408, first number = 0, last number = 100, and minimum length = 4, then the range of the directory number block will be 4080000 through 4080100.

To Edit, select the Directory Number Block, and click **Edit**. Make the necessary changes and click **Save**. To discard the changes, click **Cancel**.

To delete a Directory Number Block, click **Delete**.

Adding User Roles

Cisco Prime Collaboration Provisioning is a user-centric provisioning product and requires human users and open space locations to be defined with a userID. This method provides a convenient way to identify users, and devices in shared spaces. User roles can be used for several purposes. User roles provide policy enforcement, controlling which products and services are allowed to be ordered for different types of users such as contractors, executives, or sales persons. They are also used in a filtering process that controls what choices are presented

to order administrators at order time. The User Role setup also determines what services are ordered and which service templates are applied for a given user type during the Automatic Service Provisioning process. An administrator may create many User Roles to define different levels of services.

The default user roles are:

- Employee—Default role that is assigned to new users.

  Note The default role is configured in the Domain Rules.

  Configure the Employee user role to match the typical setup of employees in your organization. If you do not configure the employee user role to meet your needs, you may not see all the desired options during the service ordering process.

- Executive—An additional role with more service settings.
- Room—The role labeled Room is provided as a general role for shared spaces, lobby phones and other open area endpoint devices.

Note

- From Prime Collaboration 11.0 and later versions, pseudo role is represented as a Room role. While upgrading Prime Collaboration from 10.x to 11.0, the pseudo role is retained.
- Changing the role of the user from User to Open Space or Open Space to User is allowed.
- Changing the role of the user from pseudo to non-pseudo or non-pseudo to pseudo is not allowed.

The following table shows the user account creation status on Cisco Unified CM based on the role.

Role	Pseudo	Non-Pseudo
User	User account is not created on Cisco Unified CM	User account is created on Cisco Unified CM
Open Space	User account is not created on Cisco Unified CM	User account is created on Cisco Unified CM

When a user is added, the administrator specifies the role of the user. When an Open Space role is added, the administrator specifies the room role.

A pseudo user can have one or more endpoints that are associated with it. For example, conference rooms can be pseudo users with one or more endpoints, whereas a building can be a pseudo user with hundreds of endpoints that are associated with it.

These user roles exist in each Domain in Cisco Prime Collaboration Provisioning. Each set of user roles maybe customized in each Domain by adding, removing, or changing these predefined user roles.

To add a user role:

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 In the **All Domains** pane, expand a specific domain and click **User Roles**.

Step 3 In the User Roles for a specific domain page, click **Add**.

Step 4 In the **User Role Configuration** page, enter the required details for user role name, type, domain, lines, services, service bundles, and check the check box below the **Room Role** to designate the user as a Pseudo user, and click **Save.**

Note For the user role name, valid values are alphanumeric (a-z, A-Z, 0-9), period (.), hyphen (-), at sign (@), and underscore (_), but it cannot include quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%) .

Step 5 (Optional) Enable Automatic Service Provisioning, to provision services along with the user role creation.

When you are adding users, you can choose to Auto-Provision Parameters based on the user role. Auto-Provisioning automatically provisions services you chose for the user role that is assigned to the user.

If Automatic Service Provisioning is not enabled, the user role is created without any provisioned services. You can manually provision services for the user (choose **User Provisioning**).

Step 6 (Optional) The Service Template Assignment table lists the templates available for auto-provisioning and quick service provisioning. The default templates that are used for auto-provisioning are marked as yes in the **Default** column. To edit a template, you can either select the suitable row and edit the fields or click the suitable radio button and then the Edit icon. You can choose a different Service, Service Area, Endpoint Model, and Template from the respective columns and save them.

(For Cisco Prime Collaboration Release 11.1 and later) You must select Endpoint from the service drop-down list to enable the Endpoint Model column for quick service provisioning. Based on the Endpoint Model you choose, the Template drop-down list displays the templates.

(For Cisco Prime Collaboration Release 11.2 and later) You must select Extension Mobility Access from the service drop-down list to enable the Endpoint Model column, which gets populated with the endpoints supported for EM Access. You are recommended to associate Service Area with the Service Template. While ordering EM Access, Service Template drop-down is populated with the templates based on the endpoints selected on the User Role page and Universal Phone. On selection of an endpoint model, Service Template drop-down is populated with Universal Phone templates and the templates that are created for the selected phone model.

The following types of service templates can be created for endpoint models:

- A template that is specific to the endpoint model.
- A template that is applicable to series of the endpoint model.
- A universal template that is applicable to all the endpoint models.

For example:

- If you choose Cisco 7861, Template column displays all the three templates.
- If you choose Common 78*xx*, Template column displays only the series and universal endpoint templates.
- If you choose a Universal Endpoint, Template column displays only the universal endpoint templates.

- While provisioning Cisco 7861, if the model-specific default template is not available, and 78*xx* and universal templates are selected as default, the 78*xx* template is applied.
- If both Cisco 7861 model specific and 78*xx* templates are not available, and universal template is selected as default, the universal template is applied.
- If the universal template is also not available, the default template is applied.

Note You can assign only one service template per endpoint model. Choose a different combination of service area and endpoint model to assign a new service template for both auto-provisioning and quick service provisioning.

Step 7 Click **Save** to continue.

- To change a user role configuration, select a user role, click **Edit** in the User Role for a specific domain, and save the modifications.
- To delete a user role, select a user role, click **Delete** in the User Role for a specific domain, and click **OK**.
- The user role quick view displays the domain, number of endpoints, services, and service bundles selected for that user role.

  It also displays whether auto-provisioning is enabled or disabled. If enabled, the user role quick view lists the endpoints, services, and service bundles that are selected for auto-provisioning. The service template quick view also displays whether auto-provisioning is used for a particular service area and user role combination.

Troubleshooting

Issue: You cannot create new Users or Open Space if you add a user with open space role or adding an open space with user roles. Similarly, you cannot create new Users or Open Space if you add a user with both pseudo and non-pseudo roles or add an open space with pseudo and non-pseudo roles. **Recommended Action:** Use appropriate roles for **SubscriberType** column in the batch file.

Issue: You cannot create an Open Space without any role specified in batch. **Recommended Action:**Select an available Open-space role. If no Open-space roles are available, create an Open-space role, then select the role to create a Room.

Note While adding or editing a user, you can select multiple user roles. In the Mulitple User Role box, if the popup quickly opens and disappears, then you need to long-press the arrow icon for a few seconds and the popup reappears.

Related Topics

Adding Users, on page 199
Creating Service Templates, on page 79
Automatic Service Provisioning, on page 75

Associating User Roles with Services

A user whose role is associated with specific endpoints can order them. You can create orders for endpoints and services, individual services, or you can order bundled services. See Table 59: Provisioning Services, on page 255.

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 In the **All Domains** pane, expand a specific domain, click **User Roles**.

Step 3 In the User Roles for the selected domain pane, click **Add.**

Step 4 Specify a name for the user role and associate it with the necessary Endpoints, Lines, Services and Service Bundles. You can check or uncheck as many Endpoints, Services and Service Bundles as needed.

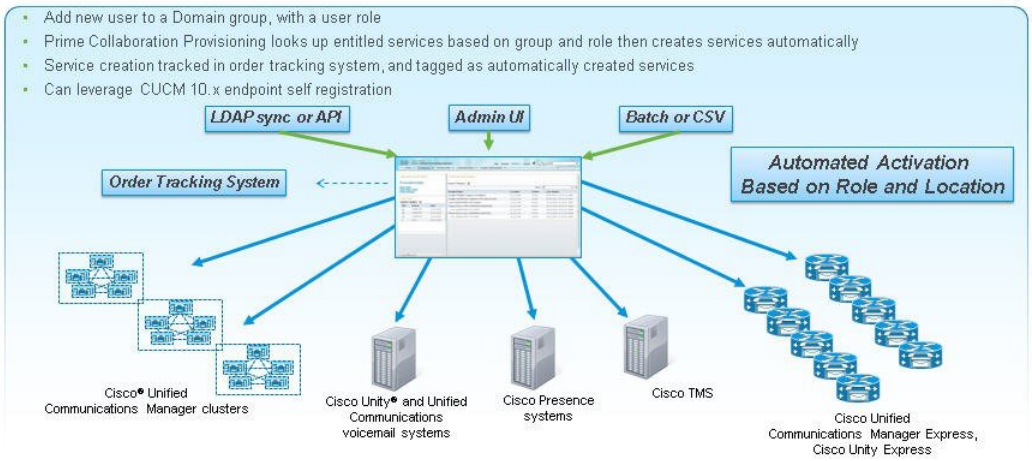
Note To modify the user role configuration, select **User Roles**. In User Roles for a specific domain, select a user role and click **Edit.**

Step 5 Click **Save**.

Automatic Service Provisioning

The Automatic Service Provisioning (ASP) feature enables you to automatically provision services for new users at user add time. Automatic Service Provisioning is generally driven by LDAP import, CSV/batch import or new user add function in the user interface. Automatic Service Provisioning is supported for Unified Communications applications 10.x and above.

Figure 3: Automatic Service Provisioning



Automatic Service Provisioning allows to create many services for a user automatically when that user is created. For example , using ASP, you can have Cisco Prime Collaboration Provisioning automatically add a phone, line, voicemail, IM&P, EM, SNR, Jabber for iPhone, and Jabber for desktop simultaneously.

The list of services can be different by creating different roles with different sets of services. For example, two user roles called "Director" and "Director-Full Features" can be created with matching manual order-time services but different settings in the Automatic Service Provisioning section of the user roles. The first role may just have phone, line and voicemail turned on for ASP. The second role may have phone, line, voicemail, IM&P, EM, SNR, Jabber for iPhone and Jabber for desktop turned on for ASP.

While enabling Automatic Service Provisioning for a user role, you must select the service area (to be used for auto-provisioning) and the services that can be automatically provisioned for the users who are assigned to this user role. For information on adding a user role, see Adding User Roles, on page 71.

You can enable Automatic Service Provisioning for the following services:

- Endpoint
- Line
- Single Number Reach (Enable Mobility, Remote Destination Profile, and Remote Destination Profile Line)
- IM & Presence
- Voicemail
- Extension Mobility Access
- Extension Mobility Line
- Cisco Jabber

While enabling Automatic Service Provisioning for Endpoint service, you have the following options:

- Default Endpoint—If you select this option, you must select the endpoint model that will be auto-provisioned for the user by default.
- Self-Provisioned Endpoint—If you select this option, the users will be able to provision their endpoints without contacting the administrator. The user can add the endpoint by plugging it into the network and following a few prompts to identify the user.

  You can also specify the maximum number of endpoints that the user can self-provision.

  If you have enabled self-provisioning for a user, a Line without endpoint will be automatically created for the user. The self-provisioned endpoints can be added to this Line later.

  If you have enabled auto-provisioning for Single Number Reach service, the user must go to the Self-Care portal of Cisco Unified Communications Manager to activate Single Number Reach. For information about the Self-Provisioning feature available in Cisco Unified Communications Manager, see Cisco Unified Communications Manager Administration Guide.

Note the following points while you are enabling Automatic Service Provisioning for a user role or user:

- Automatic Service Provisioning is applicable only for new users (added through Provisioning user interface, batch provisioning, Add User NBAPI, or synchronized from LDAP server). For the existing users, Automatic Service Provisioning cannot be initiated.
- Automatic Service Provisioning is not supported for users who are added to Cisco Prime Collaboration Provisioning through domain synchronization and Cisco Unified CM Change Notification.
- While creating user role, if you are selecting more than one Line service for Automatic Service Provisioning, the directory number which is used for provisioning the Line will be shared among the Line services.

- User roles for LDAP synchronized users will be mapped based on the domain filters.
- While creating a new user, you can choose multiple user roles for the user, but you can select only one default user role for auto-provisioning.

Note While adding or editing a user, you can select multiple user roles. In the Mulitple User Role box, if the popup quickly opens and disappears, then you need to long-press on the arrow icon for a few seconds and the popup reappears.

- While enabling Automatic Service Provisioning for new users, you must also specify the default service area to be used for auto-provisioning.
- If you are selecting Auto-assigned Line as line type for auto-provisioning, the service area that you have selected should have Directory Number blocks configured and Directory Numbers available for provisioning. If Directory Number blocks are not available in the service area, Auto-assigned line type option will not be displayed in the Add User page, when you select that service area for auto provisioning.
- If you are choosing the line type as Chosen Line, you must also provide the Directory Number, otherwise user details will not be saved for auto provisioning (a validation message will be displayed when you click Save and Continue).
- Extension Mobility line can be auto-provisioned only for users having Extension Mobility Access.
- Cisco Prime Collaboration Provisioning assigns dummy MAC address for phones that are automatically provisioned.
- You cannot provision SNR and EM Access/EM Access Bundle if the user id contains UTF characters. For RDP Name, the following characters are supported: A-Z, a-z, 0-9, hyphen (-), period (.) and underscore (_). For EM Access Name, the following characters are supported: A-Z, a-z, 0-9, and the special characters period(.), comma(,), - , _ ,! , @ , # , $, (,) , * , ^ , ; , : , + , = , ~ , ` , ? , / , ' , [,] , { , }
- While enabling Automatic Service Provisioning for a user role, if you have selected Jabber service, users that are assigned to this user role will be automatically provisioned with Jabber and associated Line service. If you have selected both Endpoint service and Jabber for a user role, Cisco Prime Collaboration Provisioning will automatically provision 2 lines with shared DN while auto-provisioning Endpoint and Jabber service.
- The user has to update the Unity Connection Web password using the Provisioning Self-Care portal or Manage PIN/Password option to configure the Voicemail/Visual Voicemail features in the Jabber client.

Quick Service Provisioning

For Cisco Prime Collaboration Release 11.1 and later

The Quick Service Provisioning feature offers an easy and quick way to provision initial or additional services for a user already defined in Cisco Prime Collaboration Provisioning, without using the ordering wizard that involves multiple steps to order a service. A new dialog box called **Provision Services** is included on the User Provisioning page to perform quick service provisioning for existing users. The quick service provisioning for an existing user can be enabled either through

- the user record page (see the procedure below)
- or the user provisioning page (select user and click **Provision Services** to proceed with the process).

In addition, a new button called **Custom Services Wizard** in the user record page enables the users to provision the services in the usual way.

To enable quick service provisioning through the user record page:

Before you begin

Before you enable quick service provisioning, note the following:

- While quick provisioning a custom group under an end user profile using the default service template, **Standard CCM Admin Users** and **Standard CTI Enable** groups are provisioned automatically even if they are not part of the default service template.
- You must select a service area. You must add a service area to the domain or you must associate the user role with the service area to proceed with Quick Service Provisioning.
- The user role associated with the user is displayed in the **Apply Service Template based on** drop-down. In the user role page, the service template associated with a Service Area is set as a default template. This template is applied during quick service provisioning if the user role is chosen in **Apply Service Template based on** drop down.
- If you do not choose any service template as **Default**, then a built-in template is applied during quick service provisioning. Built-in template is a default template which has only basic configuration.
- While quick provisioning a custom group under an end user profile using the default service template, **Standard CCM Admin Users** and **Standard CTI Enable** groups are provisioned automatically even if they are not part of the default service template.
- Based on the user role, only the service template is applied and the services under **Unified Communication Services** area are enabled.
- To apply a user service template for **User Services**:
  - You must select **User Services** under Services section in the User Role configuration page.
  - You must create a user service template and mark it as default in Service Template Assignment table.
  - For new and existing users: Select IM & Presence in the quick service provisioning dialog box.
  - If IM and Presence is already enabled for a user, the service is greyed-out in the quick service provisioning dialog box and you cannot apply the template.
- You must select the Line Type when you select or check any one of the following services: Line, Single Number Reach, EM service, and Cisco Jabber.
- You must specify a Directory Number when you select Chosen Line from the Line Type drop-down list.
- You must select the Line Type if you choose to provision EM Service, both EM Access and EM Line.
- You must select any of the UC services, else you cannot quick provision services.
- You cannot enable EM Access service if Cisco Unified CM does not have EM service name and URL configured in the device setup.
- You must check whether Directory Number blocks are configured in the selected Service Area or the "Auto- Assigned" option is selected for the user role, if Auto-Assigned Line is not shown in the Line Type drop down.

- You must enable either Single Number Reach Service under bundle services or Enable Mobility, Remote Destination Profile, and Remote Destination Profile Line in the user role policy to enable Single Number Reach.
- You cannot provision SNR and EM Access/EM Access bundle if the user id contains UTF characters. For RDP Name, the following characters are supported: A-Z, a-z, 0-9, hyphen (-), period (.) and underscore (_). For EM Access Name, the following characters are supported: A-Z, a-z, 0-9, and the special characters period(.), comma(,), - , _ ,! , @ , # , $, (,) , * , ^ , ; , : , + , = , ~ , ` , ? , / , ' , [,] , { , }.
- You must select any one of the following services to provision a voicemail:
  - Line
  - Single Number Reach
  - EM service
  - Cisco Jabber
- You must enter the MAC Address or the suitable Device Name based on the selected phone type. Dummy MAC Address of the endpoint is provisioned if no value is specified in the MAC Address field.

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click a specific user. In the user record page:

- Click **Custom Services Wizard** and proceed with the steps to provision the services in the legacy way.

Or

- Click **Provision Services** and select the Service Area.

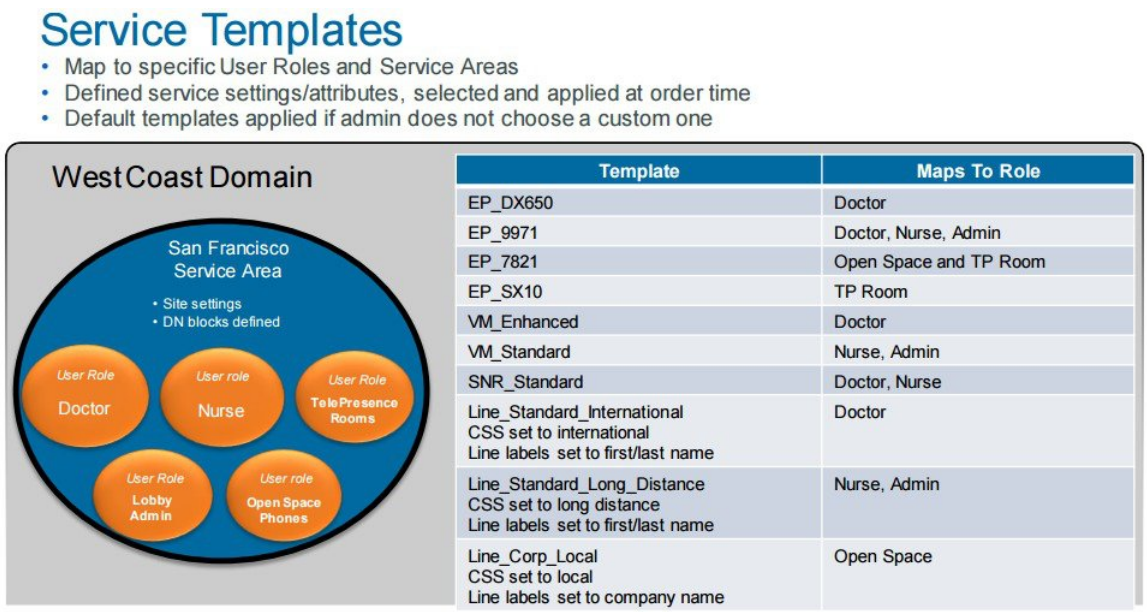
Based on the Service Area and the associated user role that is displayed, services in the dialog box are enabled.

a) Check the relevant check boxes next to each service to proceed with quick provisioning.
b) Click **Provision Services** in the dialog box to complete the service provisioning and to go back to the user record page. See Accessing User Records for a User, on page 239 for details on Add-on Service.

Creating Service Templates

Service Templates are a convenience for administrators setting up devices or ordering services for an end user. Service Templates allow small or large amounts of settings to be collected into a single template which can be applied to endpoints or services. Service Templates save time over setting many individual attributes and provide accuracy to prevent missed attributes or typos in attribute fields. Service Templates contain provisioning attributes for a service and enable you to configure service attribute settings using provisioning attributes. Provisioning attributes are configuration settings that are applied to a service during activation.

Figure 4: Service Templates



While ordering, Cisco Prime Collaboration Provisioning considers the configured provisioning attributes in addition to the Service Area settings to determine the final product configuration for provisioning.

Note You must complete the infrastructure synchronization before creating Service Areas and service templates.

Note The service areas and user roles must be defined before creating Service Templates. Service Templates require selecting service areas and user roles as part of the service template creation process. Associations can be added or deleted but the Service Templates will not be available for use if the associations are not present. You must assign the Service Templates to a service area and user role combination for the templates to be visible in the Add Order and Change Order wizards.

Templates only relate to a single domain. A domain may have one or more clusters associated.

You must have administration privileges to configure the content of the provisioning attributes .

Not all attributes are applicable for all Endpoint types or for all Cisco Unified Communications Manager versions. Depending on your Provisioning setup, all attributes may not be available to you.

The generic service template that is created under the service template area with the All keyword for the Service Area and/or the User Role is listed under the user role in the syndication table.

To create a Service Template:

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 In the All Domains pane, expand a Domain and click **Service Templates**.

Step 3 Click **Add** in the Service Template pane and enter the Template Name and select the Processor.

Step 4 Select a Service and enter the necessary provisioning attributes for the service. All default provisioning attributes are populated by default.

Step 5 When you choose Endpoint from the Service drop-down list, an additional drop-down field, namely Endpoint Model is displayed. Select the Endpoint Model based on the service you have selected.

You can use a common template that can be applied to several endpoint models or lines, thus reducing the need to create each template for each endpoint model or line. A common template groups a set of attributes that is common across the endpoint family. Common templates are described in the following table.

Table 16: Common Template Description

Common Template	Description

Family Endpoint Template	• Many family types: Jabber Phones, DX Phones, 69*xx*, 78*xx*, 88*xx*, and 89*xx*.
	• Superset of one endpoint family.
	• Apply only to endpoints belonging to the family.
	• Cover all the attributes for the endpoint in the family (superset) including:
	  • Common Attributes - Example: Calling Search Space and Common Phone Profile.
	  • Model-Specific Attributes - Example: iPhone Country Code.
	• For each attribute, only the common values (intersection) across those models which contain this attribute in the family is available.
	• Some Family Endpoint Template such as Common 69*xx* and 89*xx* supports **SIP** and **SCCP** protocols and **Either (determined by Endpoint)** protocol.
	• The **Either (determined by Endpoint)** protocol lists all the attributes available in the family regardless of the protocol.
	• You can further reduce the template creation by choosing **Either (determined by Endpoint)** to serve both the SIP and SCCP protocols as it covers all the attributes, thus leaving protocol selection during ordering.

Common Template	Description
Universal Endpoint Template	• Only one type: Universal Endpoint. • Subset of all endpoint attributes. • Apply to all endpoint types. • Only contain common attributes - Example: Calling Search Space and Common Phone Profile. • Target for provisioning endpoints with a common set of attributes. • The attribute set is similar as the Universal Device Template in Cisco Unified CM. • For each attribute, only the common values across all those models which contain this attribute is available. • Supports **SIP**, **SCCP**, **Either (determined by Endpoint)** protocols. • The **Either (determined by Endpoint)** lists all the Universal Phone attributes available regardless of the protocol. • You can further reduce the template creation by choosing **Either (determined by Endpoint)** to serve both the SIP and SCCP protocols as it covers all the attributes, thus leaving protocol selection during ordering.
Universal Line Template	• Only one type: Universal Line. • Subset of Line, EM Line, and RDP Line attributes. • Apply to Line, EM Line, and RDP Line. • Only contain common attributes. • Target for provisioning Line, EM Line, and RDP Line with a common set of attributes. • The attribute set is similar as the Universal Line Template in Cisco Unified CM. • For each attribute, only the common values across Line, EM Line, and RDP Line which contain this attribute is available.

The following table provides details of the common template and its supported models.

Table 17: Common Template Details and Supported Models

Common Template	Supported Endpoint Models/Lines
Common Jabber	**a.** Android **b.** iPhone **c.** Tablet **d.** Desktop
Common DX	**a.** Cisco DX650 **b.** Cisco DX70 **c.** Cisco DX80
Common 69*xx*	**a.** Cisco 6901 **b.** Cisco 6911 **c.** Cisco 6921 **d.** Cisco 6941 **e.** Cisco 6945 **f.** Cisco 6961
Common 78*xx*	**a.** Cisco 7811 **b.** Cisco 7821 **c.** Cisco 7841 **d.** Cisco 7861
Common 88*xx*	**a.** Cisco 8811 **b.** Cisco 8831 **c.** Cisco 8841 **d.** Cisco 8845 **e.** Cisco 8851 **f.** Cisco 8851NR **g.** Cisco 8861 **h.** Cisco 8865

Common Template	Supported Endpoint Models/Lines
Common 89*xx*	**a.** Cisco 8941 **b.** Cisco 8945 **c.** Cisco 8961
Universal Endpoint	All Models. Example: Android, DX 80 and other phones.
Universal Line	Line, EM Line and RDP Line

The common templates are supported for batch and API.

You can add, update, delete and copy the Family Endpoint, Universal Endpoint and Universal Line templates. In addition, you can apply a Family Endpoint, Universal Endpoint and Universal Line templates to update and provision an endpoint/line as appropriate.

As a result, one common template can be used to multiple endpoints/lines, thereby optimizing the service template creation process.

Note For endpoints, Common Templates feature is supported on Cisco Unified CM 10.*x* and above only.

If you encounter discrepancy on supported endpoint models between Cisco Prime Collaboration Provisioning and Cisco Unified CM, install Cisco Options Package (COP)-file on Cisco Unified CM to get all those missing endpoint models into Cisco Unified CM. Refer Manage Device Firmware section in Administration Guide for Cisco Unified Communications Manager, Release 11.0(1) for the procedure.

Step 6 To add a Service Area and User Role to the Service Template, Click **Add Row**. Select a Service Area and User Role, and click **Save**. To edit, click **Edit** and change the assignment.

You can select the All keyword from the Service Area and User Role drop-down lists as required to ignore template filtering during user provisioning. The following table shows the possible combinations for the Service Area and User Role selection:

Service Area	User Role
All	Specific
Specific	All
Specific	Specific
All	All

You can edit or delete the templates you have created. To copy the service template to a different domain with a new name, click **Copy**.

Note

- While configuring the service templates for Remote Destination Profile, if you select a User Locale that is not available in the device, the order may fail.
- If Line, EM Line, and RDP Line service templates are created and assigned for auto provisioning at the same time (line is shared), then the values displayed in Line Description, Alerting Name, and ASCII Alerting Name depend on the line template only.

Note To set a created Service Template as a default one, you need to explicitly go under the UserRole and select the Service Template and mark it as 'Yes' under Service Template Assignment.

While creating a new order, you can choose the Service Template you have created from the Service Template drop-down list.

The service template quick view displays the template's association with service area and user role. It displays whether the service template chosen is used for auto-provisioning for a particular user role or not.

Troubleshooting

- If you cannot find the attribute to set in the Universal Phone Template, you are recommended to use Family Endpoint Template if available or try to use its own Template.
- If you cannot find the attribute to set in the Universal Line Template, you are recommended to use its own Line, EM Line or RDP Line Template.
- If you cannot find the attribute to set in the Common Template, you are recommended to use its own Template. If the attribute is not a required attribute in template, but a required attribute in model, the default value in model is set during ordering.

Related Topics

Overview of Authorization Roles, on page 210
Provisioning Attribute Description in Batch Help, on page 335
Ordering Service for a User, on page 253

Adding Keywords for Service Templates

Cisco Prime Collaboration Provisioning provides an option to add keywords to the provisioning attributes at the time of creating Service templates or when ordering a service. You can add multiple keywords and can also specify the length of each keyword.

These keywords are automatically replaced on screen with the actual values immediately after moving to the next field. When replacing the keyword, the characters will be limited to the limit defined. For example, ${COMPANY}(3) – Cisco will be limited to "Cis".

Note The following exceptions are applicable to the keyword replacement:

- The keyword EXTENSION is replaced only at the backend.
- If you do not provide any values for the Domain Rule attributes, the values are taken from the domain rules and are displayed only in the summary page.

The following keywords are supported for Service templates:

- FIRSTNAME
- LASTNAME
- USERID
- EXTENSION
- COMPANY
- MIDNAME
- DEPT
- EMAIL
- EMPID
- MANAGER
- COUNTRY
- TITLE
- CITY
- STATE
- RANDNUM: A random 12 digit hexadecimal numeric sequence
- ZIP
- CORPEMAIL: Used while ordering a phone, line, and voicemail. If you have more than one voicemail account, this keyword will be mapped to the first voicemail account corporate email and upon deleting the first corporate email, it will fall back to the second one.

To edit the keywords, click **Edit Keyword List**. In the Keyword List page, you can change the keywords and its values. You can check the Remove check box to remove a keyword from the list. To remove the entire keyword List, click the **Remove Keyword List** icon.

The following table lists the Provisioning attributes that support new keywords for each service type:

Table 18: Keyword Support for Provisioning Attributes

Endpoint Type	Provisioning Attributes	Domain Rule
Endpoint\Extension Mobility Access\Remote Destination Profile	Device Description	DescriptionString

Endpoint Type	Provisioning Attributes	Domain Rule
Line\ Extension Mobility Line\ Remote Destination Profile Line	• Line Description • Alerting Name • ASCII Alerting Name • Display (Internal Caller ID) • ASCII Display (Internal Caller ID) • ASCII Line Text Label • Line Text Label (this attribute is applicable for Line and Extension Mobility Line only.) • External Phone Number Mask	LineDisplayString
Voice Mail	• Voicemail Alias • Voicemail Display Name • Initials • Title • Employee ID • Voicemail Corporate Email Address • City • State • Postal Code • Department • Manager • Billing ID	-
User Service	Self-Provisioning User ID	-

Troubleshooting

Issue: If keywords are not getting transformed to the values during ordering, the keyword may have an incorrect format. **Recommended Action:** Correct any typographical error or check for appropriate usage of keywords.

Issue: Auto Assigned Line EXTENSION Keyword is not getting transformed to the value during ordering. **Recommended Action:** Proceed ordering with EXTENSION keyword as it is.

Using System Default Values

In the Add Order wizard, Change Order wizard, and Template Settings page, "Use System Default" is displayed in the drop-down lists for non-mandatory attributes. System default values will be provisioned for these attributes, if you are not selecting any option from the drop-down list and Use System Default is a valid value in the device. If a default value is already set for a non-mandatory attribute, the specified value will be displayed for that attribute, and Use System Default will be displayed as one of the options in the drop-down list.

Use System Default will not be displayed in a drop-down list, if the word "default" is included in the options available in the drop-down list (for example, Use Default Language, Use Phone Default, Use Default System Policy, Default, and so on).

Note Use System Default will not be displayed for the Protocol field.

Note All the attributes are non-mandatory while saving the configuration in the Add Order wizard, Change Order wizard, and Template Settings page. However, some of them become mandatory attributes during Provisioning. If these attributes are set to Use System Default, the Cisco Prime Collaboration Provisioning uses the first value from the drop-down for provisioning.

For mandatory attributes, if a default value is already set, the specified default value will be displayed. If a default value is not set, then the first option in the drop-down list will be displayed, before you select a value from the drop-down list. If a drop-down list is empty and a default value is not set for that attribute, then "Make a Selection" will be displayed. Make a Selection will be displayed for the following provisioning fields:

- Selected Endpoint
- Selected Line
- Line Type
- Endpoint Type
- EM Phone Type

Use System Default or Make a Selection will not be displayed for Voicemail and Unified Messaging products.

"Not Selected" will be displayed for the Service Template field, if you are not selecting any value from the drop-down list.

For Cisco Unified Communications Manager 9.0 and below, you must select the Use System Default option for Softkey Template attribute, while creating Extension Mobility Access service template for Cisco 8961, 9951, and 9971 IP phones.

While ordering Extension Mobility Access for iPhones, order may fail if you use the default values for the following attributes:

- DND Option
- DND Incoming Call Alert (Set-only Attribute)
- MLPP Indication

For ordering Extension Mobility Access for iPhones, it is recommended that you create a service template with the following values for these attributes and apply the template while creating an order:

- DND Option—Call Reject
- DND Incoming Call Alert—Disable
- MLPP Indication—Off

Phone Provisioning Attributes Limitations

Any change order via batch using CUPM_BLANK keyword (see Keyword Usage in Batch Action Files, on page 150) will not have any effect for Phone provisioning attributes that have override common settings check box in Cisco Unified Communications Manager user interface. This occurs because the Cisco Unified Communications Manager does not return default values to Provisioning for these attributes when provisioning a phone. This applies to the following provisioning attributes:

- Join And Direct Transfer Policy
- Phone On Time
- Phone Off Time
- Phone Off Idle Timeout
- Enable Audible Alert
- EnergyWise Domain
- EnergyWise Endpoint Security Secret
- Allow EnergyWise Overrides
- Automatic Port Synchronization
- Display Idle Timeout
- Display On When Incoming Call

Configuring a Transformation Template for Provisioning Attributes

For Line Text Label and ASCII Line Text Label attributes, you can enter a transformation template in the provisioning attribute field to manipulate the digits of the directory number displayed on the phone. The digit transformation of the masking of the directory number allows you to choose what to display.

The template allows you to delete, insert, reorder, or change any digits of the directory number by embedding transformation masks inside the text string of the provisioning attribute.

A transformation template contains one or more transformation masks.

In the transformation mask, the following characters are allowed:

- W or w—Allows the directory number digits to appear in the same position, starting from the left.
- X or x—Allows the directory number digits to appear in the same position, starting from the right.
- . (period)—Ignores the digits in the directory number at the same position.
- Any number—Appears as itself in the output.
- % (percent)—Delimiter.

- \ (backward slash)—Delimiter (escape character).

If any other characters are used in a mask, the mask is not recognized as a mask and the characters are treated as normal text.

(For Cisco Prime Collaboration Release 11.2 and later) You can:

- Perform transformation masking on a directory number for keyword supported attributes.
- Provision services with attribute values containing leading sequence and trailing sequence of the respective keyword value.

Note The keyword supported attributes accept an additional keyword to fetch the trailing sequence of characters from the specified keyword and set it as the value for the attribute. To fetch the trailing sequence of characters, the leading character count is specified as zero.

- Hovering over the information icon next to the keyword supported attributes displays a help text. The help text shows examples of valid transformation templates that can be specified in the attribute value. When you place your cursor in the keyword supported attribute field, the user-entered pattern appears and when the cursor goes away from the keyword supported attribute field, the actual value appears.

When configuring the template, remember the following:

- If a transformation mask contains both a W and an X, it is not recognized as a valid mask and is treated as normal text. But if the template contains multiple masks, you can use a W and an X in different masks inside the same template.
- Any delimiter character without a prefixed escape character (\) is treated as a normal character when it is not recognized as a valid delimiter as part of a transformation mask. The escape character can be used only in places where you need to separate the normal context from the transformation mask.
- The template is limited to 60 characters.

The table lists examples of transformation templates. The directory number used in the examples is 1234567891.

Table 19: Transformation Template Examples

Template	Results
%XXX%	891
%WWW%	123
%XXX.....%	123
%XXXX%	7891
%.....WWWW%	7891
%...WWW%	456
%XXX….%	456

Template	Results
%9XXX0000%	94560000
%..9WWW0000%	94560000
%55585XX000%	5558567000
%55585WW000%	5558567000
%WWXX%	%WWXX%
(%WWW%) %...WWW%-%XXXX%	(123) 456-7891
John Smith x%XXXXX%	John Smith x67891
%John Smith\%x%XXXXX%	%John Smith%x67891
%WWW% Engineering	123 Engineering
(For Cisco Prime Collaboration Release 11.2 and later) ${FIRSTNAME}(3)(3) Example: John Smith ${FIRSTNAME}(0)(3) Example: John Smith ${EXTENSION}(3)_%XXX%	**(For Cisco Prime Collaboration Release 11.2 and later)** FIRAME Example: Johith FIRAME Example: ith 123_891

Exporting a Domain

Admin users and users with add, edit, delete, and export domains access can export a configured domain including service areas, user roles, and service template into a batch file.

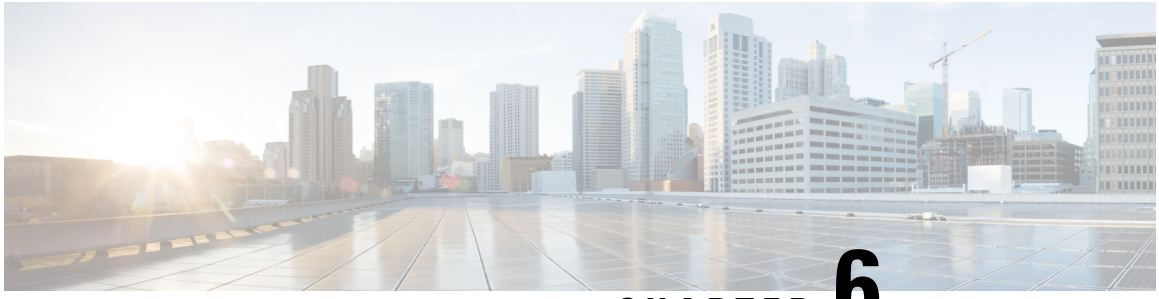
To export a domain:

Procedure

Step 1 From the Cisco Prime Collaboration Provisioning navigation pane, choose **Provisioning Setup**.

Step 2 On the Domains page, select the required domain.

Step 3 Click **Export**.



CHAPTER 6

Synchronizing Processors Users and Domains

Synchronizing Processors, Users, and Domains Overview

There are three types of synchronizations in Cisco Prime Collaboration Provisioning:

- Infrastructure Synchronization—Discovers all the objects in the device that Cisco Prime Collaboration Provisioning uses and that are not specific to individual users. The infrastructure data are the configurations that are required to exist on the device before Cisco Prime Collaboration Provisioning can configure user services.
- User Synchronization—Discovers all objects related to individual users.
- Domain Synchronization—Puts existing users discovered during user synchronization into the Domain.

Synchronizing the data in Cisco Unified Communications Manager and Cisco Unity systems, and then synchronizing with the Domains, populates Cisco Prime Collaboration Provisioning with the existing active users and services, and provides a consolidated view of all of the infrastructure and user information.

Remember the following before running any synchronization:

- Infrastructure and user synchronizations retrieve information from the device. They are unidirectional synchronizations. Provisioning does not update devices during these synchronizations. Infrastructure and user synchronizations should be completed on all devices before a Domain synchronization is started.
- You can execute the synchronizations independently and in any order. However, to preserve the integrity of the data, it is recommended that you run the synchronizations consecutively, and in the following order:
  1. Infrastructure synchronization.
  2. User synchronization.

- After a new Provisioning installation, the infrastructure synchronization must be executed first. You should not run more than one synchronization at a time.
- Ensure that you have checked the connectivity of the device. Click **Test Connection** (under Actions) from the Device details Quick View before running any synchronization. The test results appear in the Device details Quick View.
- The test connection results must be successful before synchronizing Unified Message Processors. If you start synchronization for a Unified Message Processor when the test connection status is "In Progress" or "Failure", the synchronization will fail.
- After a Call Processor or Unified Message Processor is synchronized, do not change the type of device. For example, if you add a Cisco Unified Communications Manager, do not change the Call Processor type to Cisco Unified Communications Manager Express.
- After a Domain synchronization, you can use Cisco Prime Collaboration Provisioning to directly manage the individual user account. You no longer have to use the underlying Cisco Unified Communications Manager or Cisco Unity systems.
- Any out-of-band configurations (meaning configurations that are performed directly on the processor but not synchronized with Provisioning) can result in failed orders. You must always keep Cisco Prime Collaboration Provisioning synchronized with the processors that it is provisioning.

Note When you click on Device's infrastructure or user synchronization, a popup window appears with the message 'Start Synchronization will put the system into maintenance mode'.

If you click **OK**, the system enters into maintenance mode and then the sync starts. Once the sync completes, the system comes out of the maintenance mode automatically.

If you click **Cancel**, the system does not enter into maintenance mode and the sync does not start.

If a parallel sync is already running, then the system waits for the other sync activity to complete and then comes out of the maintenance mode.

Change Notification feature will be automatically enabled for Cisco Unified Communications Manager 10.0 and above versions. This feature is not supported for Cisco Unified Communications Manager versions less than 10.0.

Note From 10.6 release, Change Notification feature is supported when the Cisco Prime Collaboration Provisioning is running in maintenance mode.

Any updates to infrastructure or user configuration of Cisco Unified Communications Manager will be automatically synchronized to Provisioning every 5 minutes. This avoids the need for daily or frequent synchronization with Cisco Unified Communications Manager.

As part of change notification, the user records are also updated to include the newly added services. To view the start and end time of change notification synchronization for a Cisco Unified Communications Manager, launch the quickview and click View Detailed Log in the Actions pane.

The following services and infrastructure objects are automatically synchronized from Cisco Unified Communications Manager, through the Change Notification feature:

- Call Park
- Call Pickup Group
- CallManagerGroup
- CSS
- CmcInfo
- CommonPhoneConfig
- CommonDeviceConfig
- Conference Now
- CTIRoutePoint
- Device Profile
- DateTimeGroup
- DeviceMobility
- Endpoint
- Emergency Location (ELIN) Group
- FacInfo
- GeoLocation
- Hunt List
- Hunt Pilot
- H323Gateway
- Line
- Line Group
- Location
- MediaResourceList
- MediaResourceGroup
- MeetMe
- PhysicalLocation
- Remote Destincation Profile
- Route List
- Route Pattern
- RoutePartition
- Route Group
- SIPProfile
- SIPTrunk
- TransPattern
- UcService
- User
- VoiceMail Profile
- VoiceMail Pilot
- VG224
- VG310
- VG320

Infrastructure and User Synchronization

You use the infrastructure synchronization to synchronize the infrastructure data in the devices. The infrastructure synchronization retrieves device information that is used across multiple users.

To synchronize infrastructure configuration products and users:

Procedure

Step 1 Choose **Device Setup**.

Step 2 Hover over Quick View of the device for which you want to run synchronization.

Step 3 Do one of the following:

- To initiate Infrastructure Synchronization, click **Start Infrastructure Synchronization**
- To initiate User Synchronization, click **Start User Synchronization**

The progress of synchronization is displayed in the Quick View under Synchronization Status.

Step 4 Click **View Detailed Logs**.

A synchronization log is created, listing the objects that could not be assigned. It also shows a warning message if an unknown element is received from the device. This log is replaced each time a synchronization occurs.

Note If you see the warning message "Skipped unexpected element," you can ignore it. The message indicates that Provisioning does not support the item that was sent back from the device.

If the status of an infrastructure or user synchronization does not change for an extended period of time, verify that the Nice service is running.

If the Nice service is stopped, restart the service, and then restart the infrastructure or user synchronization.

If you wish to manage the Analog Phones, you have to update the ipt.properties file. In this file, update the dfc.ipt.cisco.callmanager.analog_phone_support to Y and then do the user synchronization. You must restart Provisioning after the user synchronization is completed.

For the list of Cisco Unified Communications Manager objects that Provisioning synchronizes, see Cisco Unified Communications Manager Objects that Are Synchronized, on page 97.

You use the infrastructure synchronization to synchronize the unified messaging infrastructure data in Provisioning with the Unified Message Processor:

- SubscriberTemplate—A Subscriber Template in Cisco Unity Connection, and the e-mail message processor.
- UnifiedMessagingFeatureSpecification—A class of service in Cisco Unity Connection, and the e-mail message processor.

You use the user synchronization to synchronize the unified messaging user data in Provisioning with the Unified Message Processor.

- UMInfo—A user in Cisco Unity Connection, and Cisco Unity Express in conjunction with their user's voicemail and e-mail information.
- VoiceMailInfo—A user in Cisco Unity Connection, and Cisco Unity Express in conjunction with UMInfo and EmailInfo.
- EmailInfo—A user in Cisco Unity Connection in conjunction with VoiceMailInfo and UMInfo.

Note If during the synchronization of Cisco Unity Express you encounter device connection errors, close all Telnet sessions on the Cisco Unity Express system and restart the synchronization. Cisco Unity Express only allows one Telnet session at a time. Cisco Prime Collaboration Provisioning cannot synchronize with a Cisco Unity Express device that has another telnet session open.

Note If you observe that the synchronization is not progressing, click the **Stop Stuck Synchronization** link to terminate the selected infra or user synchronization.. The system creates a log about this event in the Audit Logs. Stop Stuck synchronization option does not work if the process runs successfully.

Note PCP monitors the Device (infra/user) sync status every one hour. If the sync remains stuck for one hour, the configured user gets an email notification. Audit trail is updated with the following message and the synchronization stops:

'Automatic synchronization status check Failed'.

Note IM and Presence 9.0 and higher versions are integrated with Cisco Unified Communications Manager. Due to this, user synchronization will be disabled for IM and Presence 9.0 and higher versions. User information will be directly synchronized from Cisco Unified Communications Manager.

For IM and Presence, use the Infrastructure synchronization to synchronize the User Settings Infrastructure data with Provisioning.

Note After upgrading your Cisco Unified Communications Manager, you must perform User Synchronization manually to synchronize change notification settings.

Cisco Unified Communications Manager Objects that Are Synchronized

The following tables list the Cisco Unified Communications Manager objects that are synchronized during an infrastructure and user synchronization in Provisioning.

Table 20: Cisco Unified Communications Manager Objects Synchronized During an Infrastructure Synchronization

• AAR Group • Call Park • Calling Search Space • Client Matter Codes • Cisco Unified CM Group • Call Pickup Group • Common Device Config • Conference Bridge • Conference Now • Date Time Setting • Date/Time Group • Device Mobility Info • Device Mobility Group • Device Pool • Device Profile • Dial Plan • Dial Plan Tag • Digit Discard Instruction • Enable Password Router • Emergency Location (ELIN) Group • Forced Authorization Codes	• Gatekeeper • Geo Location • Geo LocationConfiguration • Geo Location Filter • Hunt Group • Hunt List • Hunt Pilot • H323 Gateway • H323 Trunk • Interactive Voice Response (IVR) • Line Group • Location • MLPP Domain • Media Resource Group • Media Resource List • Meet-Me Number/Pattern • Message Waiting • MOH Audio Source	• Partition • Phone Profile • Phone Template • Presence Group • Physical Location • Region • Remote Destination Profile • Resource Priority Namespace List • Resource Priority Namespace Network Domain • Route Filter • Route Group • Route List • Route Partition • Route Pattern	• SIP Trunk • SIP Profile • Softkey Template • SRST • Translation Pattern • UC Service Profile • VG202 • VG204 • VG224 • VG310 • VG320 • VG350 • VGVoicemail Pilot • Voicemail Port • Voicemail Profile

Table 21: Cisco Unified Communications Manager Objects Synchronized During User Synchronization

• Calling Search Space • Device Pool • Directory Number	• IP Phone • License Capabilities	• Line • Location • Phone	• Remote Destination Profile • Remote Destination Profile Line • User

Error Messages While Synchronizing a Call Processor

Some of the error messages you encounter while synchronizing a call processor:

The Detailed Log page lists items that could not be synchronized from the Cisco Unified Communications Manager device. For example, on the page, you will see the following message:

```
Completed. But the following objects could not be
synchronized: [SecurityProfile, DialPlanTag, SIPTrunk, PhoneTemplate, DigitDiscardInstruction]
```

Incomplete synchronization can occur because of the following:

- Network problems that did not allow the items to be properly synchronized. To determine if this is the cause, analyze the nice.log file. A network problem can be the cause if the file displays the following information:

  ```
  java.security.PrivilegedActionException:com.sun.xml.messaging.saaj.SOAPExceptionImpl:Message
   send failed.
  ```

- Configuration issues with the items. In this case, copy the nice.log file and contact the Engineering Team.

Overview of Domain Synchronization

Domain synchronization aggregates data from synchronizations. Devices are not accessed during a Domain synchronization.

During a Domain synchronization, Cisco Prime Collaboration Provisioning does the following:

- Synchronizes users and their services with the Provisioning inventory, creates new users, and updates the records.
- Synchronizes user accounts and updates Cisco Prime Collaboration Provisioning so that users can log in (logins are created only if the self-care rule is enabled; see Business Rule Descriptions, on page 163.
- Associates services to Service Areas.
- Synchronizes the assigned voicemail directory numbers in Unity Connection or Unity Express to those in Cisco Unified Communications Manager.

Business rules determine the criteria used for synchronizing Domains (see Configuring Business Rules for Domain Synchronization, on page 103).

To fully synchronize a Domain, you must perform an infrastructure and user synchronization for each device in the Domain, and then perform a Domain Synchronization.

Note If a device in the Domain is already synchronized, it is recommended that a Domain synchronization also be done.

While running Domain synchronization, remember the following:

- If you use a user synchronization on Cisco Unified Communications Manager Express to add users to Provisioning, the first name, last name, phone number, and department data are not obtained by Provisioning. The Manage Users page, displays “Unknown” in these fields.

  You can update the user information through Provisioning, but be aware that this information will be pushed to the Cisco Unified Communications Manager Express system, and will overwrite any existing information for the user in the ephone description field.

- You should not run more than one synchronization at a time. Run all synchronizations sequentially.
- If a Cisco Unified Communications Manager Express is the only device present in a Domain and Service Area, during Domain synchronization users are not created in Provisioning if the ephone username command is not configured in Cisco Unified Communications Manager Express. Ensure that the ephone username command is configured in Cisco Unified Communications Manager Express for all users.
- A device profile is added to a user’s record as an Extension Mobility Access product only if the device profile is subscribed to the extension mobility service in Cisco Unified Communications Manager.
- If the Cisco Unified Communications Manager and Cisco Unified Presence added to the service area are upgraded to 9.0 versions, the following services will be removed from the user records:
  - Enable Presence
  - Enable Presence Client
  - Client User Settings

    The user records will be updated with the User Services product details.

- Cisco Prime Collaboration Provisioning allows you to provision device profiles with services enabled or disabled at enterprise level.

  If a device profile has associated services, the device profile will be associated to a user only if a matching service URL is found.

  Note Extension Mobility service can be associated to a user, even if the device profile has no associated services or if the services are enabled at enterprise level.

- Cisco Prime Collaboration Provisioning allows you to provision device profiles with services enabled or disabled at enterprise level.

  If a device profile has associated services, the device profile will be associated to a user only if a matching service URL is found.
- After domain synchronization, all services related to users are updated in the user record. You can change, cancel or edit services related to users without configuring a service area.
- In an upgraded server, you must run the user synchronization followed by domain synchronization to remove the Email services and merge Unified Messaging service with Voicemail.

Synchronizing Domains

To synchronize domains:

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 From the Domains table, hover over quick view of the Domain you want to synchronize, and click **Start Domain Synchronization**.

A popup appears saying that the Domain Synchronization has started successfully. The Last Synchronization field in Quick View displays the status of synchronization along with the start and completion time.

Domain synchronization cannot be started without configuring synchronization rules.

Note If you observe that the synchronization is not progressing, click the **Stop Stuck Synchronization** link to terminate the selected domain or LDAP synchronization. The system creates a log about this event in the Audit Logs. Stop Stuck synchronization option does not work if the process runs successfully.

Note PCP monitors the Domain sync status every one hour. If the sync remains stuck for one hour, the configured user gets an email notification. Audit trail is updated with the following message and the synchronization stops:

'Automatic synchronization status check Failed'.

Note For Cisco Prime Collaboration Provisioning 12.3 and later, after the domain synchronization is completed, if admin and globaladmin users exist in any of the devices, then those users are restricted during user sync operation.

Related Topics

Configuring Business Rules for Domain Synchronization, on page 103
Overview of Domain Synchronization, on page 99
Business Rules for Domain Synchronization, on page 102

Change Notification

Change notification allows you to sync information and includes maximum number of scenarios where the information is synced from Unified Communications Manager to Cisco Prime Collaboration Provisioning.

However, in certain cases, when you perform provisioning from Unified Communications Manager directly, information isn't synced in Cisco Prime Collaboration Provisioning after the change notification.

To remove data inconsistencies between the Cisco Prime Collaboration Provisioning and the Unified Communications Manager, we highly recommend that you use Cisco Prime Collaboration Provisioning to perform all provisioning activities. We don't recommend that you use Unified Communications Manager to perform provisioning.

For Cisco Prime Collaboration Provisioning 12.3 and later

Note When you add users to Unified Communications Manager, change notification updates all users except admin and globaladmin in Cisco Prime Collaboration Provisioning.

Business Rules for Domain Synchronization

Business rules determine the criteria used for adding users to a Domain.

For Domain synchronization to work properly, you must configure at least one of the following rules:

- Sync All Users (Unified CM)—If enabled, all user accounts in all of the Call Processors in the Domain are assigned to the Domain being synchronized. This rule overrides the Match Department rule.
- Sync Only Existing Users—If enabled, the Domain synchronization does not create new users. Only services of existing users in the Domain are synchronized.
- Sync by Attribute—You have the following options:
  - Match Department—If enabled, the Domain synchronization associates only the Call Processor user accounts whose department code matches one in the list specified in the rule configuration.
  - Match Location—If enabled, the Domain synchronization associates only the Call Processor user accounts whose phone location matches one in the list specified in the rule configuration.
  - Match Device Pool—If enabled, the Domain synchronization associates only the Call Processor user account whose Phone or Remote Destination Profile has a device pool value that matches one in the list specified in the rule configuration.

The rest of the Domain synchronization rules coreside (do not have a priority level) with the above rules. Following are the coresident Domain synchronization rules:

- Sync All Users (Unity Connection)—If this rule is enabled, all user accounts in a given Message Processor are assigned to a Provisioning Domain. Otherwise, only user accounts in the given Message Processor with a matching Call Processor user account are assigned.
- Sync Primary User From Unity Connection—If enabled, user information is updated from the associated Message Processor account; otherwise it is updated from the Call Processor.

Note If you try to run a Domain synchronization when none of the required rules are enabled, a message appears in the Synchronize Domain page stating that you are required to enable one of the rules. You can click the Configure Synchronization Rules link on this page to open the Configure Domain Sync Rules page, where you can configure the desired Domain synchronization rule. For more information, see Overview of Domain Synchronization.

If more than one of the required rules are enabled, only one of the rules will be in effect.

The rule priority is applied in the following order:

1. Sync All Users (Unified CM)
2. Sync Only Existing Users
3. Match Department
4. Match Location
5. Match Device Pool

If Sync All Users (Unified CM) rule is enabled, the settings of all the other rules are ignored. If Sync Only Existing Users rule is enabled, the settings for the last three rules are ignored. The last three rules are additive, meaning that if two of the rules are enabled, then only users that satisfy both constraints are synchronized.

Configuring Business Rules for Domain Synchronization

For Domain synchronization to work properly, you must configure Domain synchronization business rules.

Tip A description of each business rule appears when you place your cursor over the information icon next to the rule.

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 In the Domains listing page, select a Domain and click **Edit**.

Step 3 Scroll down to the Synchronization Rules area on the Domain Configuration page.

Step 4 Select the required rules.

You must select at least one Call Processor synchronization rule for the domain synchronization to work properly. If you select the Sync by Attribute rule, you must select at least one of the options listed under Sync by Attribute rule.

For more information on Domain synchronization rules, see Business Rules for Domain Synchronization, on page 102.

Step 5 Click **Save**.

Domain Synchronization Log Messages

This section provides explanations for some of the messages that can appear in the Domain Synchronization Log report.

Duplicate username encountered. So skipping the creation of this user: TestUser from the Call Processor: TestCCM

Indicates that another user exists in Provisioning with the same ID, but the ID uses a different case. Services which belong to this user will not be synchronized.

To fix this problem, remove one of the users from Cisco Unified Communications Manager.

No matching voicemail info found for directory number 123400000

The synchronization could not find a voicemail for the directory number. This problem can occur when either a synchronization was not run on the Unified Message Processor (so the voicemails are not present in Provisioning), or no matching voicemail information was found for the directory number.

To fix this problem, either run user synchronization on the Unified Message Processor, or create a Service Area with the correct settings.

The device profile line Line 1 - 123400000 could not be added to the customer record because a service area with the following properties could not be determined in the domain Cisco: Call Processor: TestCCM

A device profile line could not be assigned to a Service Area with the listed settings.

To fix this problem, either create a Service Area with the same settings or change the line settings on Cisco Unified Communications Manager.

For Blocking Users

If admin and globaladmin users are restricted during user sync operation, then, the information about the restricted users appears in the log.

Schedule Synchronization

For Cisco Prime Collaboration Release 11.1 and later

Using Schedule Synchronization, you can synchronize Call Processors, Message Processors, Presence Processors, Active Directories, and Domains.

The **Schedule Synchronization** page lists the existing jobs along with its job name, start synchronization time, frequency, job status, synchronization status, and logs. You can click **View** under the logs column to view synchronization log file of the job. Using these log files, you can analyze the cause of synchronization failure. You also have options to add, delete, edit, and run the job immediately.

Prerequisite: You must have administrator privilege to perform this task.

Note After upgrading to Cisco Prime Collaboration Provisioning 11.1, all cron jobs (scheduled for synchronization) from the system are migrated as synchronization jobs to the **Schedule Synchronization** page. These jobs will be displayed with the job status as scheduled.

To add schedule synchronization job:

Procedure

Step 1 Choose **Administration** > **Schedule Synchronization**.

Step 2 Click **Add** to create a new synchronization job for the device.

Step 3 In the **Create New Synchronization Schedule** window, enter the required details. Refer Table 22: Schedule Synchronization Configuration Fields for field descriptions.

Step 4 Click **Synchronization Preview** to run the script without performing any synchronization and to display the list of processors and domains that will be synchronized in the **Preview Synchronization Log**. Using synchronization preview logs, you can easily identify and correct syntax errors in custom granular synchronization data.

Step 5 Click **Save and Run Now** to execute the job immediately. If you do not want to execute the job immediately, you can choose **Save and Close** option.

- To edit an existing job, check the required job name and click **Edit**. Make the necessary changes and click **Save and Run Now**.
- To delete one or more jobs, check the required job name and click **Delete**.
- To execute one or more synchronization jobs immediately, check the required job name and click **Run Now**.
- To cancel an existing job, check the required job name and click **Cancel**.

Note
- You can cancel multiple synchronization jobs simultaneously if synchronization status is in progress.
- Job status will be displayed as "canceled" after the cancel is completed.
- Job status will be displayed as "canceling" while cancel is in progress.
- Synchronization status will not be available for a canceled job.

Note When any infrastructure or user scheduled sync starts, the system enters into maintenance mode automatically and exits when the sync completes.

If a parallel sync is already running, then the system waits for the other sync activity to complete and then comes out of the maintenance mode.

Table 22: Schedule Synchronization Configuration Fields

Field	Description
Job Name	Unique job name. Accepted charters are alphanumeric(A-Z, a-z, 0-9), space, underscore(_), and hyphen(-).

Synchronize Every	Frequency at which the synchronization job should run. Choose one of the following type and enter a numeric value in the text box for options except One Time: • One Time • Hour(s) • Day(s) • Week(s) By default, **One Time** is selected.
Start Date	Choose the date and time when the synchronization operation must start. By default current client date and time is displayed.
Synchronization Type	Click the appropriate configuration method. • Synchronization Schedule Builder—Click **Synchronization Schedule Builder**, when you want to perform mass synchronization of the processors. Both infrastructure and subscriber synchronization are run for each processor. • Custom Granular Synchronization—Click **Custom Granular Synchronization**, when you want to synchronize specific processor.
Synchronization Schedule Builder	You can invoke mass synchronization operation for, • All • All Call Processors • All Message Processors • All IMPs • All LDAPs • All Domains By default, option **All** is checked.

Custom Granular Synchronization	Granular Synchronization invokes synchronization operations for objects specified in the text area. The data should be in the format: *<object class>.<object name>: <sync type>* The valid values are: • *object class* : cp (Call Processor), mp (Message Processor), pp (Presence Processor), ad (Active Directory), or domain. • *object name* : all or specific object name. • *sync type* : infra(infrastructure), sub(subscriber), or both. For example : • cp.Test-UCM: infra • mp.all: sub • pp.all: both - equivalent to the [presenceprocessor] mass sync • ad.all: - ActiveDirectory mass sync • domain.Test-Dom:
Synchronization Options	You can check the required synchronization option from the following: • Force Domain Synchronization—Allows the domain synchronization to be performed even after the device synchronization failure. • Run Device Synchronization in Parallel—Runs synchronization for all the devices in parallel. • Abort Synchronization on Device Synchronization Failure—Instructs the script to quit after a synchronization failure

Configuring Directory Search Synchronization Source

To configure user data service (UDS), you must set the directory source. Directory source can be either LDAP server or Call Processor. If LDAP server is set as the directory source, UDS will be disabled in Cisco Prime Collaboration Provisioning. By default, LDAP server is set as the directory source. For enabling UDS, you must set the directory source as Call Processor.

You cannot enable UDS, if any of the Call Processor is integrated with LDAP. After enabling UDS, if a LDAP integrated Call Processor is added to Cisco Prime Collaboration Provisioning, Cisco Prime Collaboration Provisioning will disable the UDS automatically by setting the directory source as LDAP server.

The processor against which the first service is ordered for a user will be set as the home cluster for the user.

If UDS is enabled, when a user is removed from the home cluster, Provisioning will delete the corresponding user details from the other Call Processor clusters.

You can enable directory search synchronization while adding a new Call Processor or choose to do it later.

To configure the directory search synchronization source:

Procedure

Step 1 Choose **Advanced Provisioning** > **Unified Communication Services**.

Step 2 Click **Use Communication Manager for Directory Data**.

Step 3 Click **Apply**.

A warning message is displayed stating directory search synchronization will add the user details to all Call Processors that are 10.x and above. Depending on the number of users, this operation may take several hours and may impact system performance.

Step 4 Click **Yes** to continue.

Enable button appears next to **Use Communication Manager for Directory Data** option.

Step 5 Click **Enable** for directory search synchronization to happen.

Note After clicking **Enable** and on adding the call processors if the sync is not auto-initiated then you must manually initiate the sync from UCS or disable and re-enable Directory Search. This may take several hours to complete.

Unified Communication Services page will be updated to show the synchronization status for each affected cluster. If synchronization fails, an error message and links to the log files will be displayed.

Synchronizing an LDAP Server with Provisioning

You can synchronize the accounts in a Lightweight Directory Access Protocol (LDAP) server with Cisco Prime Collaboration Provisioning. Cisco Prime Collaboration Provisioning can use this information to create new users accounts in itself automatically, update already existing user information, or delete users.

Cisco Prime Collaboration Provisioning can populate its user database with user IDs directly from an associated LDAP source. Configuring and scheduling LDAP synchronization are done through domain configuration.

You can configure a filter query at the domain level to allow Cisco Prime Collaboration Provisioning to identify the exact users that have to be imported into Cisco Prime Collaboration Provisioning, as opposed to importing the entire LDAP directory into each domain. You can create complex filters based on the available fields in Microsoft Active Directory.

Administrators can control how Cisco Prime Collaboration Provisioning removes users. They can configure the “Always Delete” option when a user is no longer in the LDAP directory so that when the synchronization between Cisco Prime Collaboration Provisioning and Active Directory runs, the user will be removed from Cisco Prime Collaboration Provisioning and the user’s services will be moved to the global namespace. The “Delete if user has no services” option prevents a user from being deleted if the user still has associated

services. These optional settings can help remove unused services and free directory numbers after employees have left a company.

Note If users are not given admin privileges in AD, they cannot write to the DN.

The following table shows the step-by-step workflow to add and synchronize an LDAP server with Cisco Prime Collaboration Provisioning.

Table 23: LDAP Workflow in Provisioning

Step	Task and Description
Step 1	Configuring Provisioning to Use LDAP and ACS Servers In this step, you can configure Cisco Prime Collaboration Provisioning to connect to an LDAP or ACS server to authenticate, read, and synchronize.
Step 2	Adding LDAP Server, on page 110 In this step, you add details such as device name, IP Address, admin distinguished name and user search base. You also choose the suitable server type.

Step	Task and Description
Step 3	Configuring LDAP Server Synchronization, on page 113 **Note** Before you configure LDAP settings and perform synchronization, refer the following sections under Before LDAP Synchronization, on page 111 for more understanding. • Greenfield Deployments • Brownfield Deployments • General Information About LDAP Synchronization In this step, you select a Domain and the Directory Source you have configured in the Device Setup page. Then, you configure the information Cisco Prime Collaboration Provisioning gets from these servers in the settings pane. These settings synchronize and authenticate the users from the Directory/ACS server to Cisco Prime Collaboration Provisioning. You also schedule synchronization and then choose the domain, and start LDAP Synchronization. LDAP Synchronization Report, on page 125 You can find explanations for some of the messages that can appear in the LDAP Synchronization report.

Adding LDAP Server

To add LDAP server in Cisco Prime Collaboration Provisioning:

Procedure

Step 1 Choose **Device Setup**.

Step 2 Click **Add** to add devices to Cisco Prime Collaboration Provisioning.

Step 3 In the Add Device window, enter the necessary information such as Name and IP address.

Note For the device name, valid values are space, alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), and at sign (@).

Refer Adding Devices for field descriptions of Call Processor Fields, Unified Message Processor Fields and LDAP and ACS Server Configuration Fields.

Step 4 In the Application drop-down list , select Directory Server (LDAP) and choose the suitable LDAP Server Type. For more information on the server type, see LDAP and ACS Server Configuration Fields table.

Step 5 If the Active Directory is enabled for secure connection, check **Use SSL** checkbox and change the Server Port to 636. For non-secure connection, the Server Port field is populated with 389 by default.

Note LDAP port when LDAP server is a Global Catalog server:

- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the **Use SSL** check box.)

Step 6 Enter details of Backup Server IP Address and Backup Server Port as appropriate.

Step 7 Enter details of LDAP manager in Admin Distinguished Name and Admin Password fields. The Admin Distinguished Name field contains details of the user who has admin privileges in Active Directory.

Note
- For Admin Distinguished Name, be sure to use complete canonical name, for example, CN= Administrator, OU =Sales, DC=ca, DC=com.
- Refer Distinguished Names for more information on how to configure the Distinguished Names.
- For more information on Admin Distinguished Name, see LDAP and ACS Server Configuration Fields table.
- Admin user account entered in "Admin Distinguished Name" should have permissions to perform read and write operations.

Step 8 Enter CN or OU search base details in LDAP User Search Base of an administrator. For more information on LDAP User Search Base, see LDAP and ACS Server Configuration Fields table.

Step 9 Click **Save**.
Test Connection validates details entered as part of Device Setup and gives a Success or Failure message.

Before LDAP Synchronization

Before you configure LDAP settings and perform synchronization, refer the following sections for more understanding.

Greenfield Deployments

For greenfield deployments, remember the following:

When a service is ordered for a user that is imported from LDAP server, the Getting Started Wizard pushes the LDAP server details like LDAP directory, authentication and system settings to Cisco Unified Communications Manager. Cisco Unified Communications Manager marks the user as LDAP user. The users that are marked as LDAP user can log into the Self-Care portal of Cisco Unified Communications Manager, using the credentials configured in the LDAP server.

Note After you upgrade to latest version of Cisco Prime Collaboration Provisioning, you must run LDAP synchronization in Provisioning. Otherwise, LDAP imported users will not be marked as LDAP users in Cisco Unified Communications Manager.

Brownfield Deployments

For brownfield deployments, you must do the following:

1. Create an Infrastructure template (Advanced Provisioning > Batch Provisioning > Add > Add Batch Actions > AddLDAPAuthentication.txt or ChangeLDAPAuthentication.txt batch files) for LDAP authentication to disable authentication in Cisco Unified Communications Manager (you must choose the option "No" for "Use LDAP Authentication for End Users" attribute). Push this configuration to Cisco Unified Communications Manager through batch project.

Note **From Cisco Prime Collaboration Provisioning 11.6 and later**

- You can access all templates under the **Batch Provisioning** menu option.
- System does not provide Configuration template feature.

2. Create an Infrastructure template for LDAP System to disable LDAP synchronization in Cisco Unified Communications Manager. You must provide the value, "sAMAccountName" for "LDAP Attribute for User ID" field, if you have selected Microsoft AD server. You must provide the value, "uid" for "LDAP Attribute for User ID" field, if you have selected Microsoft ADAM or Lightweight Directory Services. Push this configuration to Cisco Unified Communications Manager through batch project.
3. Create an Infrastructure template for LDAP authentication to enable authentication in Cisco Unified Communications Manager again (you must choose the option "Yes" for "Use LDAP Authentication for End Users" attribute). Push this configuration to Cisco Unified Communications Manager through batch project.
4. You must run Infrastructure synchronization from Provisioning UI to identify LDAP directory in Cisco Unified Communications Manager, before you start provisioning the services for users in Cisco Prime Collaboration Provisioning.

Note Single LDAP synchronization is compatible with Cisco Unified CM 10.5.1 and above only.

General Information About LDAP Synchronization

- Cisco Prime Collaboration Provisioning allows writing DN back to the LDAP server.
- The following servers are supported as LDAP servers:
  - Microsoft Active Directory servers 2000, 2003, and 2008
  - Open LDAP
  - Oracle Directory
  - AD 2012
- LDAP synchronization only creates the users; it does not add their services to their user records. Make sure you run domain synchronization after LDAP synchronization so that the users' services are added to their user records.

- The user search base configured in LDAP services in the domain is used to synchronize LDAP users into the Cisco Prime Collaboration Provisioning user database.
- You cannot delete an LDAP server which is associated to a Domain. You must remove the LDAP server from the Domain to delete it.

Configuring LDAP Server Synchronization

To Configure LDAP Server Synchronization:

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 In the Domains pane, select a Domain and click **Edit**.

Step 3 On the Domain Configuration page, select the Directory Source that is configured on the Device Setup page.

Step 4 In the settings pane, you configure the information Cisco Prime Collaboration Provisioning gets from the servers by entering or choosing the details as suitable in the respective fields. These settings are used to synchronize and authenticate the users from the Directory/ACS server to Prime Collaboration.

The LDAP Settings pane contains the following sub-panes:

- LDAP Sync Policy
- LDAP Field Mappings
- Domain LDAP Filters
- Service Area LDAP Filters
- User Role LDAP Filters
- Write Back LDAP Settings

For more information on LDAP Sync Policy and Field Mappings sub-panes, see the Table 24: LDAP Settings Fields table.

While synchronizing users from the LDAP server, you can use the Domain, Service Area, and User Role LDAP filters when the User Type is enabled for Automatic Service Provisioning. These filters help identify the default Service Area and User Role to be used during Automatic Service Provisioning.

For more information on LDAP Filters, see the Table 26: LDAP Synchronization Filters table.

Step 5 For all the changes on the LDAP server to be synchronized to Cisco Prime Collaboration Provisioning, select the following:

- Mode—**Authentication and Synchronization** under LDAP Sync Policy sub-pane.
- Update existing user details—**All fields** under LDAP Sync Policy sub-pane.
- Action when LDAP users deleted—**Delete user only** under LDAP Sync Policy sub-pane.
- User Search base—Enter a user search base under LDAP Sync Policy sub-pane.
  - Unlike Cisco Unified CM, Cisco Prime Collaboration Provisioning supports only one user search base for a domain. However, you can create multiple domains for multiple user searches.

- When adding an LDAP user in Cisco Unified CM through Provisioning UI, the user search base in Provisioning domain and Unified Communications Manager must be the same.

- Filter query for synchronization—Synchronize all users. Cick the **Edit** icon under Domain LDAP Filters sub-pane and choose the necessary detail. Click **Save**.

Step 6 Click **Save**.

Note PCP monitors the LDAP sync status every one hour. If the sync remains stuck for one hour, the configured user gets an email notification. Audit trail is updated with the following message and the synchronization stops:

'Automatic synchronization status check Failed'.

Scheduling and Performing LDAP Synchronization

To schedule synchronization, set the **Synchronization Interval** and **Synchronization Start Date** in the LDAP Settings pane.

After saving the Domain Configuration page, select the Domain and hover over Quick view. Select **Start LDAP Synchronization**.

You can view the LDAP synchronization details in the domain quick view. You can click the **View Detailed Log** option available in the domain **Quick View** to view LDAP synchronization logs.

After an LDAP synchronization, a report is created. The report lists the operations that could not be performed during synchronization. Operation failure can be due to incorrect data entered into the LDAP server or incorrect user settings.

You cannot delete an LDAP server which is associated to a Domain. Remove the LDAP server from the Domain to delete it.

The following table provides details about the LDAP Configuration fields.

Table 24: LDAP Settings Fields

Field	Description
Mode	• Authentication Only—The LDAP server is used only for user authentication. • Authentication and Synchronization—The LDAP server is used both to provide user authentication and to obtain user information.
Update Existing User Details	• All fields—If any user information is changed in the LDAP server, the same information is updated in Provisioning. • Do not update—User information in Provisioning is not updated when there are changes to the user information in the LDAP server.

Field	Description
Action for stale LDAP users	**Note** A stale LDAP user is a user account that no longer matches the user search base and/or the Domain LDAP filters. • Do not make changes in Provisioning—The corresponding user in Cisco Prime Collaboration Provisioning is not deleted. • Delete user if there are no services in Provisioning—The corresponding user in Cisco Prime Collaboration Provisioning is also deleted, if the user does not have any services in Cisco Prime Collaboration Provisioning. The user is not deleted in Cisco Prime Collaboration Provisioning, if the user has any services in Cisco Prime Collaboration Provisioning. • Delete user in Provisioning—The corresponding user in Cisco Prime Collaboration Provisioning is also deleted, even if the user has any services in Cisco Prime Collaboration Provisioning. • Delete user, but keep services in Provisioning and CUCM—The corresponding user is deleted in Cisco Prime Collaboration Provisioning and Cisco Unified Communications Manager. • Delete user and all services from Provisioning and CUCM—The corresponding users and their services are deleted in the device and in Cisco Prime Collaboration Provisioning. The user is deleted in Cisco Prime Collaboration Provisioning and Cisco Unified Communications Manager, if the user is not an LDAP user in Cisco Unified Communications Manager. The user is deleted in Cisco Unified Communications Manager, if the user is an LDAP user in Cisco Unified Communications Manager.

Field	Description
User Search Base	The user search base of a domain. Provisioning searches for users under the base under Active Directory. For example, CN=Users, DC=Cisco, DC=com. This search base is used only for LDAP synchronization. In the Microsoft Active Directory server, you can use the command dsquery user to list the complete user search base. **Note** Cisco Prime Collaboration Provisioning supports only one user search base per domain.
(For Cisco Prime Collaboration Provisioning 11.5 and later) Sync Inactive (Disabled) Users	Synchronizing disabled users enables you, as an administrator, to manage disabled LDAP user accounts, and autoprovision services. When this check box is checked, LDAP Sync pulls the disabled LDAP users. Applicable when the **LDAP Sync Policy** Mode is **Authentication and Synchronization**. Applicable only for Microsoft Active Directory server or Microsoft ADAM or Lightweight Directory Services. Not configurable through the Getting Started Wizard. Mapping of user roles for disabled users is same as for active LDAP users. If disabled users are not synchronized even though Sync Inactive (Disabled) Users is enabled, you may have set the advanced query not to synchronize the disabled users. It is recommended not to use "msDS-UserAccountDisabled" attribute in the advanced query.

Field	Description

Field Mapping	Lists which user fields in Cisco Unified Communications Manager correspond to certain LDAP user fields. The only fields that you can configure in Cisco Prime Collaboration Provisioning are the following:
	• Contact phone number—Select either telephone number or ipPhone.
	• Contact email—Select either mail or sAMAccountName.
	• User ID—User ID can be mapped to the following fields in LDAP server:
	  • employeeNumber
	  • mail
	  • sAMAccountName
	  • telephoneNumber
	  • userPrincipalName
	• Middle Name—Select either middleName or initials.
	• Directory URI—Select mail, msRTCSIP-primaryuseraddress, or none.
	
	For a list of all field mapping between Provisioning and the LDAP server, see Table 25: LDAP Field Mapping, on page 120.

Field	Description
Filter Query for Synchronization	

Field	Description

	• Synchronize all users—All users are synchronized.
	• Simple query—You can configure a query by using a combination of the following fields:
	  • User ID
	  • Department
	  • Contact phone number
	  • Title
	  • First Name
	  • Last Name
	  • Manager ID—Provide a manager ID that is fully qualified as in the Active Directory integration. For example, a user, John Doe with user ID jdoe is:
	  CN=jdoe,<*user search base*>
	  • Directory URI
	  • Contact email
	  • City
	  • State
	  • Office
	  • Company
	  • Street
	  • P. O. Box
	  • Zip Code
	  • Country
	  • Fax Number
	  • IP Phone Number
	  • You can use an asterisk (*) for a partial string search.
	Advanced query—You can enter any LDAP query; for example:
	(&(sAMAccountName=johndoe)(department=Cisco*)(mail=john@cisco.com)).
	You can enter custom attributes in the Advanced

Field	Description
	Query textbox. You can use the advanced query functionality in Automatic Service Provisioning to choose the Service Area to provision the user services in and also for the User Role so that users coming in can be assigned to a particular user role.

Note Using "IN" filter in Automatic Service Provisioning, you can configure multiple queries. For example:

- To fetch multiple Directory Numbers, separate the search string using semicolon. For example: 4930;5930.
- To fetch multiple combinations of Directory Numbers, separate the search string using an asterisk and semicolon. For example: 40105*;40116*;40127*;.
- For contact phone numbers, you can use:
  - '+' symbol in search criteria such as +44*
  - '/+' symbol in search criteria such as /+44*
- For contact phone numbers, using "IN" filter with multiple values in search criteria with comma as delimiter, you can use '/+' symbol such as /+44*, /+55*,/+33*.
- Similarly, using "IN" filter you can synchronize multiple users from the LDAP server with comma as delimiter. For example: User1, User2, User3.
- Wildcard character (*) is allowed in the filter, it can be used either in beginning or in the end of the field.

Likewise, you can use '=' and '!=' operators to configure queries. For example, if you provide a single userID:

- The '=' operator synchronizes only that user from the LDAP server.
- The '!=' operator does not synchronize that user alone from the LDAP server. All other users are synchronized.

Using * with userID such as User123* fetches all the users whose id starts with User123.

The table below lists the field mapping between Cisco Prime Collaboration Provisioning and the LDAP server. The data in the specified Provisioning field is synchronized with the user data in the corresponding LDAP field.

Table 25: LDAP Field Mapping

Provisioning Field	LDAP Field
Phone Number **Note** For Provisioning users, if this field is empty, the line directory number is assigned automatically to this field during the time of line ordering.	telephoneNumber or ipPhone number. **Note** For LDAP users, if this field is empty, the line directory number is not assigned to this field during the time of line ordering.

Provisioning Field	LDAP Field
Email	mail
User ID	User ID can be mapped to the following fields in LDAP server: • employeeNumber • mail • sAMAccountName • telephoneNumber • userPrincipalName
First Name	givenName.
Last Name	sn.
Middle Name	middleName or initials
Directory URI	mail, msRTCSIP-primaryuseraddress, or none
Manager ID	manager
Department	department
Title	title
Home Number	homephone
Mobile Number	mobile
Pager Number	pager

Note If you have configured LDAP server type as Microsoft ADAM or Lightweight Directory Services or Oracle directory server or OpenLDAP, uid is listed in the User ID drop-down list instead of sAMAccountName.

Note **(For Cisco Prime Collaboration Release 11.2 and later)** The following LDAP attributes are not supported in the domain user interface for openLDAP and Oracle directory server:

- msRTCSIP-primaryuseraddress
- userPrincipalName
- ipPhone number
- middlename

While synchronizing users from the LDAP server, you can use the following filters when the User Type is enabled for Automatic Service Provisioning. These filters help identify the default Service Area and User Role to be used during Automatic Service Provisioning:

Table 26: LDAP Synchronization Filters

LDAP Filter	Description
Domain LDAP filter	Use this filter to specify which users should be assigned to each domain.
Service area LDAP filter	Use this filter to specify which users should be assigned to each service area. Service area LDAP filter is not enabled if there is no service area configured in that domain. **Note** This filter is only applicable for Auto-Provisioning. **(For Cisco Prime Collaboration Release 11.2 and later)** Cisco Prime Collaboration Provisioning can support the common LDAP attributes in the Service Area LDAP filter by extending the filters to accept advanced queries.

LDAP Filter	Description
Role LDAP filter	Use this filter to specify which User Role should be applied for autoprovisioning the default services. If this filter is not configured, users that are synchronized from the LDAP server are mapped to the default role configured in Business Rules and autoprovisioning happens only if the default User Role in domain Business Rules is enabled for autoprovisioning. Both the default User Role and the User Role that matches with the filter is assigned for the user if: • The User Role specified in the filter is different from default Business Rule, and • The filter criteria matches. **Note** This filter is only applicable for Auto-Provisioning. **(For Cisco Prime Collaboration Release 11.2 and later)**Cisco Prime Collaboration Provisioning can support the common LDAP attributes in User Role LDAP filter by extending the filters to accept advanced queries. Service Area and User Role filters are not enabled, if you have selected the synchronization mode as "Authentication Only." Also, both the filters are applied only when autoprovisioning is enabled.

While creating the service area filter, you can configure the following settings:

- Assign new line from the extension block.
- Apply mask to LDAP synchronized telephone numbers. You can enter the mask value that needs to be applied on the LDAP synchronized number in the Mask field. Note the following points while entering the mask value:
  - The valid values for Mask field are 0-9, plus symbol (+), upper case x (X), and backslash followed by plus symbol (\+).
  - It can start with +, \+, X, or numerals (0-9).
  - It can be a combination of numerals and character X (for example, 12XXX, +XX234, XX231XXX).
  - E.164 characters (+ and \+) can be used only at the beginning of the value. These characters should not be used in between the numbers or X.

  Provisioning applies the mask to the LDAP synchronized number after removing the non-numeric characters and provisions the line accordingly.

Note Mask field is enabled only if you have checked the Apply Mask to LDAP Synchronized Telephone Numbers check box.

Mask option is available only for users who are synchronized from the LDAP server. Also, masked numbers are used only during autoprovisioning Line for LDAP users.

- If you have checked the Assign New Line from the Extension Block check box, even if there is an LDAP synchronized number, Provisioning selects the directory number from the DN block and provision the line accordingly.
- If you have checked the Apply Mask to LDAP Synchronized Telephone Numbers check box:
  - When there is no LDAP synchronized number, Cisco Prime Collaboration Provisioning does not provision Line service for the user.
  - When there is LDAP synchronized number, Cisco Prime Collaboration Provisioning applies the mask on LDAP synchronized number and uses the masked number for auto provisioning the line.
- If both the check boxes are checked, LDAP synchronized number is masked and masked DN is used for autoprovisioning the line. If there is no LDAP synchronized number, Cisco Prime Collaboration Provisioning selects a number from the DN block and provision the line accordingly.
- If both the check boxes are unchecked, LDAP synchronized number is used for provisioning the line.

Note Ensure that the LDAP synchronized number is different from the numbers that are generated in DN Block during autoprovisioning the line.

Write Primary DN to LDAP

For Cisco Prime Collaboration Release 11.2 and later

You can write the Primary DN chosen from Cisco Prime Collaboration Provisioning back to the LDAP server, thus reducing the manual update of the AD fields and masking of DNs. This feature gets triggered at the ordering and domain level.

Note the following points during write-back:

- You can write Primary DN's to AD if LDAP user, Primary DN, and write back settings are enabled at domain level.
- You can perform the write-back while ordering Line and User Services through the user interface and batch.
- You cannot perform the write-back during Cisco Unified CM user synchronization and change notification. If the Primary DN is changed directly in Cisco Unified CM, then you need to wait for the sync / change notification changes to complete and reflect in Cisco Prime Collaboration Provisioning.
- You can configure the write-back settings through domain user interface, and batch.
- You can update the write-back settings through the add or change functionality of batch.
- You cannot configure the write-back settings at domain level through Getting Started Wizard.

Write Back Settings

To write the Primary DN to LDAP, choose **Provisioning Setup** and select a Domain to edit. Expand LDAP Settings pane to view Write Back Settings subpane. Enter the necessary fields and click **Save** .

- The default LDAP Attribute drop-down is **Do not write to LDAP** with the **Apply Mask** field disabled.
- When you choose ipPhone or telephoneNumber or mobile from the LDAP Attribute drop-down, **Apply Mask** field is enabled.
- You have the option to enter a mask value that is applied to the Primary DN before writing to LDAP. The valid values for **Apply Mask** field are 0-9, plus symbol (+), upper case x (X), and backslash followed by plus symbol (\+). E.164 characters (+ and \+) can be used only at the beginning of the value.

From the Domains table, hover over **Quick View** of the domain you want to write back, and click **Start Write Back to LDAP**.

Note If the LDAP attribute is set to **Do not write to LDAP**, write back does not happen and **Start Write Back to LDAP** is disabled.

Once **Start Write Back to LDAP** action starts, other actions such as **Start Domain Synchronization** and **Start LDAP Synchronization** are disabled.

Primary DN is not written to LDAP while ordering due to any one of the following reasons:

- LDAP server is unreachable or incorrect LDAP credentials.
- Admin user account entered in "Admin Distinguished Name" does not have permission to perform a write operation.
- The Domain level LDAP attribute is set to **Do not write to LDAP.**
- User does not have any primary directory number.

Check the LDAP test connection and the order status or select any attribute from the LDAP attribute drop-down list.

To view detailed log information, hover over **Quick View** of the desired domain, and then click **View Detailed Log**.

An error message is displayed in the order details page (go to the user record of the user on the **User Provisioning** page) if any error occurred during the write- back. You cannot view the write-back status for all the orders.

LDAP Synchronization Report

This section provides explanations for some of the messages that can appear in the LDAP Synchronization report.

The following users were not created because they are already present in another Domain: user1, user2

The listed users are present in the LDAP server, but could not be created in Provisioning in the current Domain, because they are already present in another Domain.

To fix this problem, delete the users from the other Domain and run the LDAP synchronization again.

Deletion of User and associated services failed for the following users: UserId, OrderId, Status

This message appears when Delete user with Services is enabled, and deleting the user and services from the device and from Provisioning fails. In order to delete the services in a device, a single order is created for each user and the order status is shown in the above report with the order ID. You have to manually delete these users and corresponding services. You can click on the link provided for the user ID in the above report to access these user records.

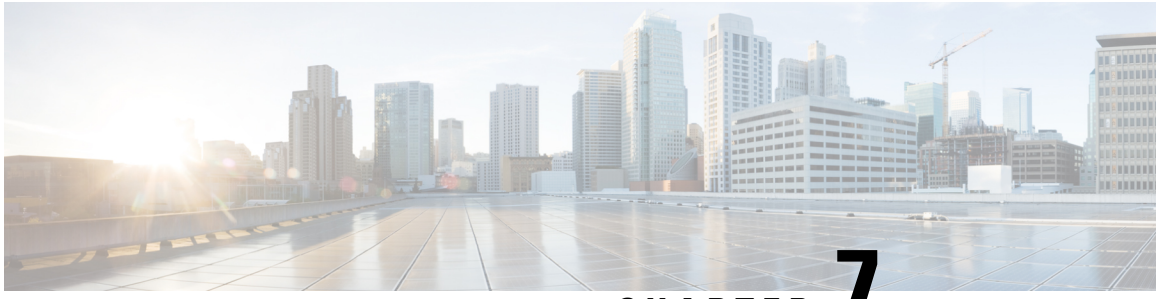
The following user and associated services were deleted successfully: UserId, OrderId, Status

This message appears when Delete user with Services is enabled, and deleting the user and services from the device and from Provisioning succeeds.

The following users were not deleted because the delete option was not set: user1 user2

The users were deleted in the LDAP server, but they were not deleted during the LDAP synchronization, since Do not delete is enabled.

To fix this problem, enable either Delete User Only or Delete User with Services option, and run the LDAP synchronization again.



CHAPTER 7

Batch Provisioning, Infrastructure Configuration, and Business Rules

Batch Provisioning

Note For Cisco prime Collaboration Provisioning 12.3 and later, only Administrator group can access the Batch functions.

To create users and provision their services automatically use batch provisioning. Batch provisioning enables you to easily roll out a new office, or transition from legacy systems.

You can order user services on an individual basis for a single user. But when deploying a large number of services, you should combine them into a single batch. Batch provisioning enables you to create a single batch that contains multiple types of orders.

You can use batch provisioning to add, update, or cancel a Domain (with or without LDAP settings). You can also add, update, or delete user roles using batch provisioning.

Unlike BAT files that run only on the Cisco Unified Communication application they are deployed, Provisioning batches can run on one or many applications managed by Provisioning.

Batches can be run immediately upon uploading to Cisco Prime Collaboration Provisioning, or they can be scheduled to run at a later time. For more information on Batch Projects, see Managing Batch Projects, on page 151.

You can also combine multiple types of services into a single batch operation. For example, a batch can contain a combination of phone and voicemail additions or changes.

You can add, change, or cancel the following infrastructure objects through batch provisioning:

- App User

- Call Search Space
- Cisco IOS Conference Bridge
- Class of Service
- Conference Now
- CTI Route Point
- Date Time Group
- Device Mobility Group
- Device Pool
- Emergency Location (ELIN) Group
- External Service
- Gateway Settings
- Interactive Voice Response (IVR)
- LDAP Authentication
- LDAP Directory
- Location
- Media Resource Group
- Media Resource Group List
- Message Waiting On/Off
- Phone NTP Reference
- Physical Location
- Port Group
- Proxy Configuration Setting
- Restriction Table
- Route Partition
- Route Pattern
- Service Parameter
- Service Profile
- SIP Profile
- SIP Route Pattern
- SIP Trunk
- SIP Trunk Security Profile
- SRST

- Subscriber Template
- TFTP Server
- Transfer Rule
- Translation Pattern
- Trunk
- UC Service - CTI
- UC Service - IM and Presence
- UC Service - Voicemail
- Unified CM Group
- Universal Device Template
- Universal Line Template
- User Profile Provision
- Voice Region
- Voicemail Pilot
- Voicemail Profile

- Called Party Transformation Pattern
- Calling Party Transformation Pattern
- Intercom Directory Number
- Intercom Translation Pattern
- Intercom Calling Search Space
- Intercom Route Partition
- Recording Profile
- SIP Realm

- Directed Call Park
- Feature Control Policy

Note You can only add the Directed Call Park and Feature Control Policy infrastructure objects using batch. You cannot change or cancel using batch. These infrastructure objects are not supported through Configuration Templates (Infrastructure Configuration and the Infrastructure Templates User Interface).

- SoftKey Template
- Feature Group Template

Note You can add, change and cancel SoftKey Template and Feature Group Template.

You cannot update or delete a standard template. Only user-defined templates can be updated and deleted.

Note In case of EM Access batch provisioning (AddEMAccessServiceTemplate), you need to use the Unified Communications Manager Processor name as 'cucm', instead of 'cucm-CiscoUnifiedCM'.

For Cisco Prime Collaboration Provisioning release 12.5 and later

Enabling Spark Hybrid Services

To enable Spark Hybrid Services, perform the following steps:

1. Add Expressway Core or Expressway Edge devices to Cisco Prime Collaboration Provisioning by navigating to **Device Setup** >**Add.**
2. Navigate to **Advanced Provisioning** > **Batch Provisioning**, and add a new batch project by clicking on the **ADD** button.
3. Click **Add BatchAction** and search for the following files:
   - ChangeSIP_CertificateRevocationChecking.txt
   - ChangeSIP_Configuration.txt
   - ChangeSIP_RegistrationControls.txt
   - ChangeSIP_Advanced.txt

   Note If you want to add all the above files together, search for the ExpresswaySparkHybridCombinedBatch.txt file that contains all the four files.
4. Select the files that you want to add.
5. Go to **Keywords** and configure processor and User ID.
6. Click **Run Now**.

Note The procedure for batch provisioning to enable Spark Hybrid Services is similar for both Expressway Core and Expressway Edge.

For Cisco Prime Collaboration Provisioning release 12.5 and later

Configuring Disk Usage using Batch Template

To configure disk usage:

1. Navigate to **Advanced Provisioning** > **Batch Provisioning**, and add a new batch project by clicking on the **ADD** button.
2. Click **Add BatchAction** and search for the following file:

   ConfigureDiskUsage.txt
3. Select the file and click on **Add to Project**.
4. Click **Edit** and configure the following parameters by clicking on them:
   - DiskUsage: Input any value between 50 to 95
   - OrderType: Do not change the default order type configdiskusage
   - ProductName: (The inputs for this field are not mandatory)
   - ServiceArea: (The inputs for this field are not mandatory)
   - UserID: Some inputs need to be present in this field.
5. Click **Save**.

Creating Batch Action Files

To complete batch provisioning, you must:

1. Create a spreadsheet of users and services to be provisioned (including phones and lines).
2. Convert the spreadsheet to a tab-delimited text file called a batch action file.

Note When you edit the batch file (.txt) using Excel and save the updated spreadsheet as a tab-delimited text file, Excel may add double quotes for the values that contain special characters, especially comma. Remove the double quotes from the tab-delimited text file before running the batch project to avoid errors.

You can use the BulkAddMobility.txt and BulkCancelMobility.txt batch files to enable and disable mobility support for all the users in the selected Domain.

3. Upload the batch action file into a Provisioning batch project.
4. Run the batch project or schedule it to run later. Provisioning creates the users and provisions the lines and the phones based on the file data.

You can also view a list of scheduled projects and the details of the projects that are in progress.

While provisioning the orders, you can see the status as Completed. Click the Completed link to view the device-related updates.

Batch action files must contain a single row of column headers. The data columns can be in any order in the tab-delimited text file. You can compile the data in any text editor if the resulting file conforms to these guidelines.

Batch Action File Fields

Batch Action File Required Columns

The table below describes the columns that are required for every batch action file.

Table 27: Batch Action File Required Columns

Column	Description
Order Type	The order type. Valid options are (they are case sensitive): • add • cancel • change—Cannot be used for Voicemail, Email, or Unified Messaging. • addUser—Add multiple users at one time. If you are adding one user and the product for the user, you can use the Add order type. If you are adding multiple users at one time, you can use the addUser order type. • changeUser—Change multiple users' information at one time. • deleteUser—Delete multiple users at one time. • addServiceArea—Add multiple Service Areas at one time. • changeServiceArea—Change multiple Service Areas at one time. • deleteServiceArea—Delete multiple Service Areas at one time. • addServiceTemplate—Add multiple Service Templates at one time. • changeServiceTemplate—Change multiple Service Templates at one time. • addDomain—Add multiple Domains at one time. • changeDomain—Change multiple Domains at one time. • deleteDomain—Delete multiple Domains at one time.

Column	Description

	• The following are specific to Distribution List batch provisioning:
	  • Add-New-Members—Add new members to the Distribution List.
	  • Remove-Members—Removes members from the Distribution List.
	• addDevice—Add multiple devices at one time.
	• updateDevice—Change multiple devices at one time.
	• deleteDevice—Delete multiple devices at one time.
	• The following are specific to Analog Phone batch provisioning:
	  • add—To add an Analog phone or an Analog phone and the line. Adds an Analog phone where the analog voice gateway configurator will be loaded and Voice port IOS template and Dial peer IOS template are provisioned.
	  • change—To change or replace an Analog phone.
	  • cancel— To cancel an Analog phone. The phone is cancelled in the Unified Communications Manager and the voice port and dial peer configurations are removed from the device.

User ID	Provisioning user ID for which to provision the order. For addServiceArea, changeServiceArea, and deleteServiceArea, the field can be left empty. For all infrastructure products, the user ID is *icadmin*.

Column	Description
Product Name	The product name. Note that the input varies depending on the order type: • Add orders—Must be an orderable product (including bundles), but cannot be a subtype (for example, you must use “Endpoint” instead of “Cisco 7960”). If you are ordering an Analog Phone, update the dfc.ipt.cisco.callmanager.analog_phone_support to Y in the ipt.properties file. • Cancel—Can be any product name that appears in the user’s record. Note that this does not include bundles. Dependent objects are automatically deleted when their parent is deleted. • Change—Must be an orderable product. • addUser and deleteUser—Leave empty (even if something is entered, it will be ignored). • addServiceArea, changeServiceArea, deleteServiceArea, addServiceTemplate, changeServiceTemplate—Leave empty.
Service Area	Name of the Service Area to order against. For addUser and deleteUser, leave empty (even if something is entered, it will be ignored). For all infrastructure products, the Service Area is not required if the processor name is provided. If the processor name is not provided, Service Area and Domain name are required.
Domain	Name of the Domain associated with the users or services.
Endpoint Type	Type of the Endpoint. If you have chosen endpoint type as phone, select a supported phone model (for example, Cisco 7960).
MAC Address	MAC address of the endpoint. moveService—For Cisco IP Communicator, Call Processor versions less than 5, use the MAC address. If the version is 5 or greater, use the device name.

Batch Action File Columns for New User

The following table lists the additional columns that are used when new users are being created (lists the required columns for all batch action files).

Table 28: Batch Action File Columns for New User

Column	Description
User ID	The Provisioning user ID to be created. **Note** For Cisco Prime Collaboration Provisioning 12.3 and later, the admin and globaladmin users cannot be created using the Batch Provisioning page.
First Name	(Optional) User's first name.
Last Name	User's last name.
Domain	Domain to place the new user in.
Phone Number	(Optional) Phone number for the new user.
Email	(Optional) Email address for the new user.
Department	(Optional) Department for the new user.
User Role	(Optional) User role for the new user. Multiple user roles can be added for a user (use a semicolon to separate the user roles). **Note** User roles which are not supported by the Domain will be ignored. If there are no valid user roles assigned to the user, the user will not be created and the batch order will fail.
PMPassword	(Optional) User password for Provisioning.

Batch Action File Columns for Deleting Users

The table below lists the additional columns that are used when deleting users (lists the required columns for all batch action files).

Table 29: Batch Action File Columns for Deleting Users

Column	Description
Domain	(Optional) Domain where the user exists.

Column	Description
OnlyFromCUPM	(Optional) If this column is enabled (set to Y), any services on the user record for the user will be moved to the Global Resources namespace, and their services on the actual device will not be removed. If this column is not enabled (set to N), the user will be removed from both Provisioning and the device. Existing batch file for 'DeleteUser' is used for both delete user with no services(existing functionality) and with services. Tip: When a user is deleted with OnlyFromCUPM enabled, a subsequent Domain synchronization creates the user (provided it matches the Domain synchronization rules), and the matched services appear in its user record. Alternatively, the user can be manually created in the correct Domain followed by a Domain synchronization to match the services. This provides you with a way to move users between Domains or move user services across Service Areas.

Batch Action File Columns for Adding, Modifying, or Deleting Devices

The table below lists the additional columns that are used while adding, updating, or deleting the devices.

Note Before running the batch project for deleting the devices, you must ensure that Cisco Prime Collaboration Provisioning is in Maintenance mode (see Maintenance Mode, on page 329).

Table 30: Batch Action File Columns for Adding, Modifying, or Deleting Devices

Column	Description
DeviceType	Type of the device.
IPAddress	IP Address of the device.
DeviceName	Name of the device.
NewDevicename	To change the name of the device and give a new name.
Capability <number>	Number assigned to the capability.
If Capability<number> is Unified Communications Manager, following are the valid headers:	
• Capability<number> Version	Version of the Unified Communications Manager device.
• Capability<number>IPAddress	IP Address of the Unified Communications Manager device.

Column	Description
• Capability<number>Action	Action to access the Unified Communications Manager device.
• Capability<number> UserName	Username to access the Unified Communications Manager device.
• Capability<number> Password	Password to access the Unified Communications Manager device.
• Capability<number> ConfirmPassword	Confirmation of the password to access the Unified Communications Manager device.
• Capability<number> Protocol	Protocol of the Unified Communications Manager device.
• Capability<number> LDAPDirectoryIntegration	Specifies whether LDAP integration is needed or not.
• Capability<number> EMServiceName	Name of the Extension Mobility service.
• Capability<number> EMServiceURL	URL of the extension mobility service.
If Capability<number> is Unity Connection, following are the valid headers:	
• Capability<number> Version	Version of the Unity Connection device.
• Capability<number>IPAddress	IP Address of the Unity Connection device.
• Capability<number>Action	Action associated with Unity Connection device.
• Capability<number> UserName	Username to log into Unity Connection device.
• Capability<number> Password	Password to access the Unity Connection device.
• Capability<number> ConfirmPassword	Confirmation of the password to access the Unity Connection device.
If Capability<number> is Unity Express, following are the valid headers:	
• Capability<number> Version	Version of the Unity Express device.
• Capability<number> CUELineUserName	Username to log into the Unity Express device.
• Capability<number> CUE Line Password	Line password associated with the username.
• Capability<number> ConfirmCUELinePassword	Confirmation of the password to access Unity Express device.

Column	Description
• Capability<number> Service EngineInterfaceNumber	Service engine interface number.
The following columns apply if the Unity columns are defined:	
• IP Address	IP Address of Unity device.
• Version	Version of Unity device.
• Username	Username for accessing the Unity device.
• Password	Password associated with the username.
• Capability<number> createbyImport	Creating the device by importing the details.
• Capability<number> UMPPORT	Port of the Unity.
The following columns apply if the Unified Presence columns are defined:	
• Capability<number> Version	Version of the Unified Presence device.
• Capability<number> IPAddress	IP Address of the Unified Presence device.
• Capability<number> Action	Action associated with Unified Presence device.
• Capability<number> UserName	Username for accessing the Unified Presence device.
• Capability<number> Password	Password associated with the username.
• Capability<number> ConfirmPassword	Confirmation of the password.
• Capability<number> Protocol	Protocol of the Unified Presence device.
The following columns apply if the Call Manager Express columns are defined:	
• Capability<number> Version	Version of the Call Manager Express device.
The following columns apply if the Router with IOS columns are defined:	
• DeviceProtocol	Protocol of the Cisco IOS Router device.
• DeviceUserName	Username associated with the Cisco IOS Router device.
• DevicePassword	Password associated with the username.

Column	Description
• DeviceConfirmPassword	Confirmation of the password.
• DeviceEnablePassword	Enables the password for the Cisco IOS Router device.
• ConfirmDeviceEnablePassword	Confirmation of the password for enabling the device.

Note You can also add an LDAP server through batch provisioning using IP address. Adding an LDAP server using hostname is not supported.

Batch Action File Columns for Adding and Changing Multiple Service Areas

The table below lists the additional columns that are used when deleting users (lists the required columns for all batch action files).

Table 31: Batch Action File Columns for Adding and Changing Multiple Service Areas

Column	Description
Domain	The name of the Domain to which the Service Area belongs.
User role	Used only for addServiceArea. It can be left empty. If used, enter a semicolon separated list of user roles.
Call Processor Name	Name of the Call Processor in the listed Service Area.
The following columns apply only if the Call Processor Name column is defined:	
• Endpoint Protocol	The value can be either SCCP or SIP. If no value is specified, the default is SCCP.
• Endpoint Call Search Space	The Calling Search Space for the Endpoint.
• Line Call Search Space	Calling Search Space for the Line.
• Common Device Config	Common Device Configuration for the Endpoint.
• Location	Location for the Endpoint.
• Route Partition	Route Partition for the Line.
• Device Pool	Device Pool for the Endpoint.
Unified Message Processor Name	Name of the Unified Message Processor in the listed Service Area.

Column	Description
The following columns apply only if the Unified Message Processor Name column is defined:	
• Subscriber Template	One of the TTS enabled or disabled subscriber templates, that is defined on the listed Unified Message Processor.
Directory Number Blocks	Adding Directory Number Blocks in Service Area is an enhancement of Service Area batch provisioning. The data format will be <Prefix> :< First Number> :< Last Number> :<Minimum Length>; <Prefix> :< First Number> :< Last Number> :< Minimum Length> Delimiter ";" is used to configure multiple Directory Number Blocks. User can remove all existing Directory Number Blocks using CUPM_BLANK keyword during changeServiceArea operation. CUPM_SKIP keyword can be used to retain the previous value during changeServiceArea operation.

Batch Action File Columns for Adding Analog Phone or Analog Phone Service

Table 32: Batch Action File Columns for Adding Analog Phone or Analog Phone Service

Column	Description
Analog Voice Gateway Reference	Analog Voice Gateway Reference field associated with the selected Analog phone.
VoicePort	Voiceport associated with the Analog Voice Gateway Reference.
Directory Number	Directory number associated with the Analog phone.

Note To order Analog Phones for VG450, VG310, VG320, and VG350 Analog Voice Gateway models, you must include Slot and Subunit columns in the batch file.

Batch Action File Columns for Replacing Analog Phones

Table 33: Batch Action File Columns for Replacing Analog Phones

Column	Description
Analog Voice Gateway Reference	New Analog Voice Gateway Reference field that will replace the existing Analog Voice Gateway Reference.

Column	Description
VoicePort	New Voiceport field that will replace the existing Voiceport.

Note To replace Analog Phones for VG450, VG310, VG320, and VG350 Analog Voice Gateway models, you must include Slot and Subunit columns in the batch file.

Batch Action File Columns for Changing Analog Phones

Table 34: Batch Action File Columns for Changing Analog Phones

Column	Description
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.

Note To change Analog Phones for VG450, VG310, VG320, and VG350 Analog Voice Gateway models, you must include Analog Voice Gateway Reference, Slot, Subunit and Voice Port columns in the batch file.

Batch Action File Columns for Adding, Modifying, or Deleting an ELIN group

The table below lists the additional columns that are used while adding, updating, or deleting the ELIN group.

Table 35: Batch Action File Columns for Adding, Modifying, or Deleting an ELIN group

Column	Description
Processor Name	Name of the Unity Connection server.
Name	ELIN group name.
Description	ELIN group description.
ELIN Number Configuration	Specify the ELIN number in the format ELIN number : Partition, while adding an ELIN group.
Add ELIN Number Configuration	For editing the ELIN group specify the ELIN number to be added, in the format ELIN number : Partition.
Remove ELIN Number Configuration	For editing the ELIN group specify the ELIN number to be removed, in the format ELIN number : Partition.

Table 36: Batch Action File Columns for Adding, Changing, or Removing SMTP Notification Device

Column	Description
SMTP Display Name	Name of the SMTP device that an administrator creates for the user. Used for **Display Name** field in the SMTP notification device. **Note** • If SMTP display name is not available in the device, SMTP is created in Cisco Unity Connection. • If SMTP display name already exists, existing details are overridden with configured attributes.
New SMTP Display Name	Renames the SMTP display name.
SMTP Enabled	Allows the SMTP device to be enabled.
SMTP To Address	Email address of the user to whom email is sent. Used for **To** field in the SMTP device .
Remove Notification Devices	Removes multiple SMTP(s) for the user, using semicolon as a separator. Used only in change voice mail batch operation.

Batch Action File Columns for System Call Handler

The following table lists the additional columns that are used for adding System Call Handler through batch provisioning (Batch Action File Fields, on page 132 lists the required columns for all batch action files).

Table 37: Batch Action File Columns for Adding System Call Handler

Column	Description
Processor Name	Name of the Unity Connection server.
Display Name	Enter a descriptive name for the call handler.
Call Handler Template	Specify the call handler template on which to base the new call handler.
Search Scope	Specify the search scope that is applied to match extensions that callers dial from the call handler to objects in a particular search space.
Language	Specify the language in which Unity Connection plays the handler system prompts to the caller.

The following table lists the additional columns that are used for updating System Call Handler attributes through batch provisioning (Batch Action File Fields, on page 132 lists the required columns for all batch action files).

Table 38: Batch Action File Columns for Updating System Call Handler Attributes

Column	Description
Processor Name	Name of the Unity Connection server.
Display Name	Enter a descriptive name for the call handler.

Column	Description
Phone System	Specify the phone system that the call handler uses.
Active Schedule	Specify a schedule from the list to specify the days and times that the standard and closed greetings play, as well as the action that Unity Connection takes after the greeting.
Time Zone	Specify the desired time zone for the call handler.
Language	Specify the language in which Unity Connection plays the handler system prompts to the caller.
Extension	Enter the extension that the phone system uses to connect to the call handler.
Partition	Specify the partition to which the object belongs.
Search Scope	Specify the search scope that is applied to match extensions that callers dial from the call handler to objects in a particular search space.

The following table lists the additional columns that are used for canceling System Call Handler through batch provisioning (Batch Action File Fields, on page 132 lists the required columns for all batch action files).

Table 39: Batch Action File Columns for Canceling System Call Handler

Column	Description
Processor Name	Name of the Unity Connection server.
Display Name	Enter the Display Name of the call handler.

You can change the Greetings and Caller Input attributes through batch provisioning. Note the following points while creating the batch file for changing Greetings and Caller Input attributes:

- The following attributes have three headers (columns) in batch file, where the first column represents the call management element (for example, call handler, interview handler, directory handler, and so on), the second column represents the destination to which calls are sent, and the third column represents the value for Handler Conversation (Attempt Transfer or Go Directly to Greetings).
  - After Greeting
  - Action
- For the Greeting Status attribute, if you have selected "Enabled Until" option, you must provide the value for Time Expires attribute in the following format: mm-dd-yyyy hh:mm AM (or PM).

Batch Action File Columns for Directory Handler

The table below lists the additional columns that are used for adding and updating Directory Handler through batch provisioning (Batch Action File Fields, on page 132 lists the required columns for all batch action files).

Table 40: Batch Action File Columns for Adding and Updating Directory Handler Attributes

Column	Description
Processor Name	Name of the Unity Connection server.
Display Name	Enter a descriptive name for the directory handler.

Column	Description
Language	Specify the language in which Unity Connection plays the handler system prompts to the caller.
Extension	Enter the extension that the phone system uses to connect to the directory handler.
Partition	Specify the partition to which the object belongs.
Voice Enabled	For Unity Connection systems with the voice-recognition option, enable this option to create a voice directory handler.
Speech Confidence Threshold	Use this setting to adjust the likelihood that Unity Connection recognizes user utterances as voice commands and recipient names.
Play All Names	Use this setting to play the names of users in the directory for caller selection, rather than requiring the caller to search by spelled name.
Search Scope	Specify the scope for directory handler searches
Class of Service	Restricts directory handler searches to users who are assigned to the selected class of service on the local Unity Connection server.
System Distribution List	Restricts directory handler searches to members of the selected system distribution list.
Search Space	Restricts directory handler searches to users and contacts who are associated with a partition that is a member of the selected search space.
Search Criteria Order	Specify the method that callers use to spell a username

Column	Description
Search Results Behavior	Use this setting to specify the search results behavior. If Voice Enabled option is set to true, you have to specify the value for the following attributes: • Route Automatically on a Unique Match • Announce Extension with Each Name • Announce City with Each Name • Announce Department with Each Name If Voice Enabled option is set to false, you can specify the value for the following attributes in the Search Results Behavior column: • Route Automatically on a Unique Match • Always Request Caller Input If you want to provide the value for Announce Matched Names Using Extension Format or Announce Matched Names Using Menu Format attribute, you must use the Announce Matched Names Using column.
Route Automatically on a Unique Match	When this option is selected, Unity Connection routes a call to the extension assigned to the user without prompting the caller to verify the match.
Announce Extension with Each Name	If this option is enabled, Unity Connection provides a menu of users that includes user extensions.
Announce City with Each Name	Enable this option to have Unity Connection announce the city of each matching user when there are multiple matches.
Announce Department with Each Name	Enable this option to have Unity Connection announce the department of each matching user when there are multiple matches.
Always request caller input	When this option is selected, Unity Connection prompts a caller to verify the match before sending the caller to the specified user extension.

Column	Description
Announce Matched Names Using	If Announce Matched Names Using Extension Format option is enabled, Unity Connection announces to callers the names and extensions of matching users. If Announce Matched Names Using Menu Format option is enabled, Unity Connection provides a menu of users to callers. If this option is enabled, you can provide the value for the following attribute: • Announce Extension with Each Name
Maximum Number of Matches	Indicate the maximum number of matching names that are presented to a caller when more than one user matches the key presses entered by the caller.

The following table lists the additional columns that are used for canceling Directory Handler through batch provisioning (Table 27: Batch Action File Required Columns, on page 132 lists the required columns for all batch action files).

Table 41: Batch Action File Columns for Canceling Directory Handler

Column	Description
Processor Name	Name of the Unity Connection server.
Display Name	Enter the Display Name of the Directory Handler.

You can change the Caller Input attributes using the batch project. Note the following while creating the batch file for changing Caller Input attributes:

The following attributes have three headers (columns) in batch file, where the first column represents the call management element (for example, call handler, interview handler, directory handler, and so on), the second column represents the destination to which calls are sent, and the third column represents the value for Handler Conversation (Attempt Transfer or Go Directly to Greetings).

- If Caller Exits
- If no input
- If No Selection
- If Caller Presses Zero

For more detailed information on the attributes that are required in a batch action file based on different services, refer http://docwiki.cisco.com/wiki/Cisco_Prime_Collaboration_Provisioning_Batch_File_Attributes.

Guidelines for Creating Batch Action Files

Download sample batch files from Cisco.com. You can add additional columns to the sample batch files as required.

When creating batch action files, follow these guidelines:

- While creating batch action values, colon delimiter must be used to enter multiples values. For example, while creating a new CallingSearchSpace that contains multiple Route Partitions, use RP1:RP2:RP3.
- To add comments to a batch action file, insert # (pound symbol) followed by the comment. You can add any information regarding that batch. These comments are ignored at the time of importing the batch action file.

  For example:

  -
  - # This is to deploy a new site.
- To include multiple product types without adding multiple columns to a batch action file, insert >> (greater than symbol twice). You must insert >> at the beginning of the header row in a batch action file.

  For example:

```
>>OrderType  UserID    ProductName ServiceArea      Domain     ProcessorName Name

add          icadmin   Route       SampleServiceArea Alberta    cucm10.176   kpart-1
                       Partition

>>OrderType  UserID    ProductName ServiceArea      DeviceType DeviceName

deleteDevice UserID                MediaServer      cucm10.177 10.0.0

#Device Pool

>>OrderType   UserID   ProductName ServiceArea       Domain    ProcessorName Name

cancel       icadmin   Device Pool SampleSA         Alberta    cucm10.176   DP_Alberta
```

Note You must insert greater than symbol twice (>>). If there is a single greater than symbol (>) instead of two, then the batch action file gets imported, but the order fails.

- If you want the users that will be created to have self-care accounts, you must enable the CreateSelfCareAccounts rule for all applicable Domains.
- MAC Address is required when ProductName is Phone (or a bundle containing a Phone) and Phone Type is not a virtual phone (for example, CTI Port).
- New MAC Address is required when changing phones.
- Name is required when canceling Remote Destination Profile and Extension Mobility Access products.
- Mac Address is required when ProductName is Phone.
- Voicemail Alias is required when ProductName is Voicemail.
- When canceling a Line or an Extension Mobility Line product, the directory number and route partition are required.
- If you delete VG202,VG 204 and VG 224 products, all the phones in the Device and Provisioning will be deleted. You will get a warning message regarding this and only after the confirmation, the phones are deleted. Domain synchronization must be done to clean the customer records associated with the phones.

- Cisco Unity devices (Cisco Unity Connection, and Cisco Unity Express) do not support all products and services. If the batch action file is configured for a product which is not supported by the device in the specified Service Area, batch provisioning will fail.
- Product attributes that require user input during the manual order entry process are required to successfully complete the equivalent order in a batch project. Examples include:
  - Phone Type—Type of phone (for example, Cisco 7960, Cisco 7912) if ordered product is a Phone or a bundle that contains a Phone.
  - Line Type—Type of line (for example, Auto-Assigned Line or Chosen Line) if ordered product is a Line or a bundle that contains a Line.
  - Directory Number—Required when ProductName is *Line* and Type is *Chosen Line*. Additionally, ordering a product with a dependency that is not met by the order itself (for example, ordering a single Line) requires a column specifying the dependent object.
  - Route Partition—Required when ProductName is *Line* and Order Type is *Change*.
- If the product being ordered has a dependency that is not met by the order itself (for example, a single Line), a column specifying the dependent object is required. Examples include:
  - SelectedPhone—MAC address of the phone to add the line to.
  - SelectedLine—The SelectedLine value should be provided based on the product name:
    - If the Voicemail is added to Remote Destination Profile Line, you must provide the value in the following format: {RDP profile Name}Directory Number.
    - If the Voicemail is added to Line product, you must provide the value in the following format: {Phone Type : MAC Address}Directory Number.
    - If the Voicemail is added to EM Line product, you must provide the value in the following format: {Phone Type : profile name}Directory Number.
    - If the Voicemail is added to Line without endpoint, you must provide the Directory Number alone.

    Note If the Line product has route partition, you must provide the route partition along with the Directory Number (for example, for adding Voicemail to Remote Destination Profile Line, you must provide: {RDP profile Name}Directory Number/Route Partition).

  - SelectedVoicemail—Directory number of the voicemail to add unified messaging to.
  - SelectedEM_Access—Name of the EM_Access (device profile) to add the EM_Line to.

  Bundles that contain more than one instance of a base product require their attributes to be specified with a (1), (2), and so on, at the end of the column name. For example, Line Type(1), Directory Number(1).
- For bundled products, if the product attribute name is the same for different base products, append the product name in the attribute to differentiate them.

  For example, Calling Search Space is an attribute in both Phone and Line. For the product Phone Service, you can specify Phone Calling Search Space and Line Calling Search Space.

- Speed dial information can be provided in the following ways:
  - Directly—Used where there is one column. The column header is Speed Dial Info. The expected format is index:number:label, repeated for each speed dial, semicolon delimited, where index is the position of the speed dial (for example; 1, 4, 5, and so on), number is the phone number, and label is the speed dial name (for example, 1:8675306:Joe;4:888:Voicemail).

    If you use this format to add an additional line, you must reenter all the speed dial information previously entered in the column and add the new speed dial information.

    This format is recommend for initial setup of speed dials. To add speed dials to an existing list of speed dials, you must use the format described in the next sub-bullet.
  - As matching sets of columns—One set of columns can be called Speed Dial n (where *n* is the speed dial position), and the other can be called Speed Dial n Name. This format appends new speed dials to the existing speed dial list.

    For example:

Speed Dial 1	Speed Dial 1 Name	Speed Dial 4	Speed Dial 4 Name
8675306	Joe	888	Voicemail

    You can pause the speed dial number by introducing a comma. A comma introduces a delay of 2 seconds. You can introduce any number of commas in a speed dial directory number.
- Line Group information can be provided in the format LineGroupName:position. This is repeated for each Line Group, semicolon delimited. LineGroupName is the name of the line group. Position is the position of the directory number within the selected Line Group, and it can have values of last (or LAST), or numbers from 1 through 100; for example, LG1:1;LG2:5;LG3:last.

  To add an additional line, you must enter all of the Line Group information. The Line Group column headings must be listed as Line Groups(1) and Line Groups(2).
- If there are multiple instances of a column (for example, multiple directory numbers), each instance must be specified with a (1), (2), and so on, at the end of the column name; for example, Directory Number(1), Directory Number(2).
- In the provisioning attribute for the Cisco Unified Communications Manager Express Phone and Line configuration template, you must use a tilde (~) as a separator; for example, username AAAAA password BBBBBBBB~pin 676771. The column header for this attribute is CME Phone Configuration Template.
- To unset the value of a provisioning attribute that has a numeric value in Cisco Unified Communications Manager, you must enter a zero for the value. If you just enter an empty value, the provisioning attribute does not get unset in Cisco Unified Communications Manager.
- While placing an order for voicemail account, if you use the Chosen Line option and select E.164 format directory number, Provisioning will set the extension number by removing the + symbol from the directory number. But the Alternate Extension field will not be auto populated. You have to enter the directory number (along with the + symbol) in the Alternate Extension field in the batch file.
- You can provide the details in UTF-8 format, but the file encoding should be UTF-8 or UTF-8 Without BOM. UTF-8 Without BOM encoding will be available in advanced text editor like Notepad++. UTF-8 encoding will be available in Notepad editor. UTF-8 characters will be converted to junk characters if the file encoding is not specified as UTF-8 or UTF-8 Without BOM.

Keyword Usage in Batch Action Files

To perform specific functions, use the following keywords in batch action files:

- CUPM_BLANK—For the Add order type, no value will be provisioned for the attribute. For the Change order type, the current attribute value will be either cleared (if applicable), or set to the default value required by the processor.

  Note When using the Change order type for the set-only attributes that are an enumerated type that supports a static list of valid values (for example, Calling Search Space Activation Policy), CUPM_BLANK has no effect and the old values are retained.

- CUPM_SKIP—Skips the provisioning attribute when processing the action file. The attribute is not set during the order. The previous configured value is retained.

  When using CUPM_SKIP with the Add order type, not all attributes can be skipped. The following attributes are not skipped:

  - Mandatory attributes (for example, Device Pool and Location) are not skipped. They use the provisioning attribute settings configured at the Service Area level.
  - Device Description and Display (Internal Caller ID). These settings have rules, so they use the values based on their rules.

- VL7DL—Used to separate values of a set-only attribute (For example: On,VL7DL,Call Recording Enabled,VL7DL,None).

Keyword Support to Batch File

For Cisco Prime Collaboration Release 11.6 and later

This feature enables you to use keywords while editing a batch action, and uploading a batch file. You can define a keyword list to assign values for the attributes while creating the batch actions. You can also copy the list of keywords from an existing list of another batch project. The user interface suggests the keyword based on the input you provide. You can add, edit, copy, and delete the keywords. On the **Batch Provisioning** page, select a batch project and click **Keywords** button to view the list of keywords. The list includes the name of keyword, its value, and occurrence in the batch project. Keywords are replaced with the value in all the batch actions where it has occurred in a batch project. Occurrence is the count of the number of times a keyword has been used in the entire batch project (could be in multiple batch actions of the same project).

- You can add a maximum of 500 keywords per batch project. You cannot add system keywords such as FIRSTNAME, LASTNAME, USERID, MIDNAME, DEPT, EMAIL, MANAGER, TITLE, COMPANY, COUNTRY, CITY,STATE,ZIP, EMPID, CONTACTEMAIL, and CORPEMAIL.
- Keywords from one batch project can be copied to another batch project.
- In the Keywords dialog box, when you click **Copy from Project** button, a new dialog box lists all the batch projects, whose keyword list has been defined and contains at least one keyword.
- When you select any batch project from the list, all the keywords from that project are copied to the current batch project. However, if the selected batch project contains any keyword which exists in current keyword list, the current value is overwritten.

- Batch project quick view lists keywords and value details of the project. Replaced keywords are highlighted in blue color, while non-replaced keywords are highlighted in yellow color.

Auto-suggesting Keywords

While editing a batch action, you get an auto-suggestion for all the available keywords in the project. The auto-suggestion is filtered based on the input you provide. You can select the keyword by clicking over the auto-suggestion list. Any text enclosure within ${'text'} is considered as keyword. For example, ${SERVER_PORT}, SERVER_PORT is a keyword. You can also enter a keyword which does not exist in the keyword list (does not exist in the auto-suggestion box). When you save a batch action, all such keywords are automatically added to the keyword list of the batch project. These keywords are added with empty values. If a keyword does not have a value assigned, the keyword appears itself in the attribute value.

Note Nesting of keywords such as ${SERVER_PORT ${KEYNAME}} is not supported.

Managing Batch Projects

Batch Provisioning support is provided for all the devices of Unified Communications Manager, Unity Connection, Unity, Presence Processor, Unity Express, Call Manager Express, and Generic IOS Router. Users with the Administration role can provision devices using batch provisioning.

Sample batch files for all devices are available in the opt/cupm/sep/ipt/config/sample/batchProvisioning directory.

After you create a batch action file, you must create the batch project that it belongs to. When you upload a batch action file, its contents are converted to batch actions, and the columns that are common to all batch actions in the batch action file are displayed.

You must upload batch action files in the correct order according to any dependencies that exist between the batch actions. For more information about these dependencies, see Guidelines for Creating Batch Action Files, on page 146.

To create a batch project:

Procedure

Step 1 Choose **Advanced Provisioning** > **Batch Provisioning**.

Step 2 Click **Add** to create a new project.

Step 3 In the **New Batch Project** window, enter the name and description and click **Add**.

Step 4 In the **Configure a Batch Project** screen that appears after you choose the batch project, click **Add Batch Actions** to add batch action.

Step 5 In the Add Batch Actions page, select the appropriate File Name and Click **Add to Project**.

Step 6 You can do one or more of the following:

- Run the batch project immediately, or schedule it to run later. See the table below for editing, copying, deleting, canceling, exporting and other operations on Batch Projects.

- Schedule the batch project to be run later.

You can delete the batch projects or batch actions that you no longer require. To delete a batch project or a batch action, select the project or batch action and click **Delete**.

You can resume operation of a batch project which is in Paused state. Click the Resume icon to do so.

Click the **Batch Help** icon at the top right corner of the Batch Provisioning page. The Batch Action Help link opened in a new tab displays a table of all the batch actions along with the attributes and description for different services.

Table 42: Managing Batch Projects

Batch Operation	Procedure
To run a batch project immediately	**1.** Choose a batch project in **All Projects** pane. **2.** In the Configure a Batch Project page, click **Run Now**.
To schedule or reschedule a batch project	**1.** Choose a batch project in **All Projects** pane. **2.** In the Configure a Batch Project page, click the Calendar icon. Specify a date and time in the calender dialog box that appears and click **OK**. **3.** Click **Yes** in the confirmation message box to schedule or reschedule the batch project as appropriate. **Note** Batch projects created for infrastructure configuration cannot be restarted if there is a failure. **4.** Click **Run Now** to execute the batch project.
To cancel a scheduled batch project	**1.** Choose a batch project in **All Projects** pane. **2.** In the Configure a Batch Project page, click the **Clear** button next to the Calender icon. **3.** Click **Yes** to confirm. You can cancel a scheduled batch project provided that it has not started processing.
To stop a batch project	You can stop a batch project which is in Paused state and In Progress state. To do this: **1.** Choose the suitable batch project in **All Projects** pane and check its status. **2.** In the Configure a Batch Project page, click **Stop** to stop the batch project.

To view the batch action details	**1.** Choose a batch project in **All Projects** pane. **2.** In the Configure a Batch Project page, hover over **Quick View** of a batch action to view the details. The Batch Action Details pane displays all the configured information for the batch project action, including the status and log. In Batch Provisioning, during endpoint order, users with any user role can add a new endpoint. Even a pseudo user can add an endpoint.
To edit a batch project and a batch action file	To edit a batch project: **1.** Click **All Projects**. **2.** Select the batch project from the list displayed on the right side of the screen and click **Edit**. **3.** In the **Configure a Batch Project** window, click **Add Batch Actions**. Select a batch action file and click **Add to Project**. The new batch action file is added to the selected batch projects. To edit a batch action file: **1.** Select the suitable batch project in **All Projects** pane. **2.** In the **Configure a Batch Project** window, select the Action required and click **Edit**. **3.** In the **Edit Batch Action** window, click **Add New Attribute** to add a new attribute to the action file or click the **Edit** icon to edit the value of any existing attribute. Click **Save**. **Note** Only one batch action can be edited at a time.
To copy a batch project along with the batch actions	To copy a batch project: **1.** Select the batch project and click **Copy** to copy a batch project along with the batch action. **2.** In the **Copy Batch Project** window, enter the description and rename the auto-populated batch project name, if required, and click **Add**. A copy of an existing batch project along with the batch action files is created with the status showing "Not Scheduled" for batch project and "Not Started" for batch action. To copy a batch action: **1.** Select the batch actions and click the expand icon in the right pane . **2.** Click **Copy Action(s)**.
To export a batch project	**1.** Click **All Projects** and choose a batch project in the right pane. **2.** Click the expand icon in the right pane and click **Export**. All the batch actions of the selected project is copied to a text file. **Note** Only one project can be exported at a time.

To view the current status of a batch project	In the Configure a Batch Project page, the Batch Project Actions pane displays the status of each batch action project. To view the orders that are in a specific state (for example, In Progress or Completed state), choose the batch project and select the filter in the Batch Project Actions pane. After a batch project has completed, you can also check the user records of the users to verify that orders have been processed. To see details of a single running order within a batch project, administrators can also use My Activities (Choose **Activities** > **My Activities**) to view each order as it is executed in the workflow.

Troubleshooting

Issue: If all the buttons are disabled in the **Configure a Batch Project** page, the Batch Project might be in one of the following states:

- In Progress
- Stopped
- Paused

Recommended Action: If the Batch Project is

- In Progress: Wait till the project gets completed.
- Stopped: Create a new Batch Project or copy the stopped batch project to proceed.
- Paused: Either stop or resume the paused batch project.

Issue: You will not be able to edit a batch action if it is completed or failed.

Recommended Action: You can copy and then edit the batch action.

Migrating Prebuilt IOS Templates as Batch

For Cisco Prime Collaboration Release 11.6 and later

- Existing **Configuration Templates** are created as batch projects in **Batch Provisioning** on migration to batch. The configurations in each template is created as respective batch actions.
- Post migration, you have the privilege for **Batch Provisioning** if you had access to **Configuration Templates** privilege before migration.
- You must use the Batch Provisioning user interface (**Advanced Provisioning > Batch Provisioning**) to configure IOS Infra Objects.
- You can configure Unified Communications Manager, Unified Communications Manager Express, Unity Express, Unity, Unity Connection, and Generic IOS Router using the batch. You can add, edit, or delete the configuration settings of a device using the Infrastructure Configuration page.
- You can create generic Cisco IOS Prebuilt batch to auto-configure specific functionality on any device supported by the Provisioning that has the Cisco IOS generic router capability configured.

- Refer Prebuilt IOS Templates, on page 511 for more details.

Infrastructure Configuration Products for Devices

The following tables list the infrastructure configuration products that are available in Provisioning.

Infrastructure Configuration Products for Unified Communications Manager Release

Note From 11.0 release, support for 8.x devices is dropped.

Infrastructure Configuration Product	Cisco Unified Communications Manager	
	10.x and 11.x	12.0 and 12.5(1)
Analog Voice Gateway Reference	Y	NA
Cisco Fax Relay	Y	NA
Cisco Unified Communication Manager Group	Y	Y
CTI Route Point	Y	Y
Call Park	Y	Y
Call Pickup Group	Y	Y
Call Queuing	Y	NA
Call Search Space	Y	Y
Common Device Config	Y	Y
Common Phone Profile	N	Y
Client Matter Code	Y	Y
Date/Time Group	Y	Y
Description	Y	Y
Device Pool	Y	Y
Device Mobility Group	Supported for Cisco Unified Communications Manager 10.5 and above	N
Device Mobility Info	Y	Y
Enable Telnet	Y	NA
Forced Authorization Codes	Y	Y

Infrastructure Configuration Product	Cisco Unified Communications Manager	
	10.x and 11.x	12.0 and 12.5(1)
Geo Location Filter	Y	Y
Geo Location Configuration	Y	Y
H323 Gateway	Y	Y
Hunt List	Y	Y
Hunt Pilot	Y	Y
IOS Enhanced Conference Bridge	Supported for Cisco Unified IP Phone Services Communications Manager 10.5 and above	N
IP Phone Services	Supported for Cisco Unified IP Phone Services Communications Manager 10.5 and above	N
Line Group	Y	Y
Location	Y	Y
MAC Address (Last 10 Characters)	Y	N
Media Resource Group	Y	Y
Media Resource Group List	Y	Y
Meet-Me Conference	Y	NA
Meet-Me Number/Pattern	Y	Y
Modem Passthrough	Y	NA
MLPP Domain	Y	Y
Module in Slot 0	Y	NA
MT Package Capability	Y	NA
Partition	Y	Y
Physical Location	Y	Y
Resource Priority Namespace List	Y	Y
Resource Priority Namespace Network Domain	Y	Y
Remote Destination Profile	Y	Y

Infrastructure Configuration Product	Cisco Unified Communications Manager	
	10.x and 11.x	12.0 and 12.5(1)
Remote Destination Profile Line	Y	Y
RES Package Capability	Y	NA
RTP Package Capability	Y	NA
RTP Report Interval (secs)	Y	NA
RTP Unreachable OnOff	Y	NA
RTP Unreachable timeout (ms)	Y	NA
Route Group	Y	Y
Route List	Y	Y
Route Partition	Y	Y
Route Pattern	Y	Y
Service Parameter	Supported for Cisco Unified Service Parameter Communications Manager 10.5 and above	N
Service Profile	N	Y
Simple SDP	Y	NA
SIP Trunk	Y	Y
SIP Profile	Y	Y
SST Package Capability	Y	NA
T38 Fax Relay	Y	NA
Translation Pattern	Y	Y
UC Service	N	Y
Unified CM Group	Y	Y
VG202	Y	Y
VG204	Y	Y
VG224	Y	Y
VG350	N	N
Voice Region (Region)	Y	Y
Voiceport (Voicemail Port)	Y	Y

Infrastructure Configuration Product	Cisco Unified Communications Manager	
	10.x and 11.x	12.0 and 12.5(1)
Voicemail Pilot	Y	Y
Voicemail Profile	Y	Y

Infrastructure Configuration Products for Cisco Unified Communications Manager - Session Management Edition

Note From 11.0 release, support for 8.x devices is dropped.

Infrastructure Configuration Product	Cisco Session Management Edition	
	10.x and 11.x	12.0 and 12.5(1)
SIP Trunk	Y	Y
SIP Profile	Y	Y

Infrastructure Configuration Products for Cisco Unified Message Processor

Infrastructure Configuration Product	Cisco Unified Message Processor	
	10.x and 11.x	12.0 and 12.5(1)
Distribution List (Cisco Unity Connection)	Y	Y
Call Handlers	Y	Y
Class Of Service	Y	Y
Distribution List	Y	Y
Directory Handlers	Y	Y
Interview Handlers	Y	Y
Subscriber Template (User Template)	Y	Y

Note From 11.0 release, support for 8.x devices is dropped.

Table 43: Infrastructure Configuration Products (Cisco Unified Presence Processor)

Infrastructure Configuration Product	Cisco Unified Presence Processor	
	10.x and 11.x	12.0 and 12.5(1)
Audio Profile	Y	NA

Infrastructure Configuration Product	Cisco Unified Presence Processor	
	10.x and 11.x	12.0 and 12.5(1)
CIP Profile	Y	Y
Conferencing Profile	Y	NA
CTI Gateway Profile	Y	NA
LDAP Profile	Y	Y
Voicemail Profile	Y	Y

Customer Domain Template

If your implementation has more than one Domain, you can configure the Customer Domain Template according to the default business rules and user types that you require for your implementation.

When you create new Domains, they inherit the standard set of business rules and user types from the Customer Domain Template. You can then change the business rules and user types as required for each new Domain. Changes made to the Customer Domain Template affect only new Domains created after that point.

The Customer Domain Template is created by default when you install Provisioning. You configure it by specifying business rules and user roles for it the same way that business rules and user roles are specified for new Domains.

If you want to use these new Provisioning features, you must edit the Customer Domain templates.

Overview of Infrastructure Configuration

The Infrastructure Configuration page of Provisioning enables you to browse the infrastructure configuration settings of a Call Processor and Unified Message Processor. Through this page, you can add, edit, or delete the configuration settings of a Call Processor and Unified Message Processor. Also, you can view pending operations and schedule operations (see Scheduling an Infrastructure Configuration Task, on page 161).

To work with infrastructure configuration, you must be assigned the Infrastructure Configuration Management authorization role and be assigned permissions to the corresponding infrastructure products (see Managing Infrastructure Configuration Permissions).

The Infrastructure Configuration feature applies to Call Processors that are based on Cisco Unified Communications Manager devices and Unified Message Processors that are based on Cisco Unity Connection only.

Cross-launching Devices from Infrastructure Configuration

Cisco Prime Collaboration Provisioning allows an administrator to cross launch configured devices such as Unified Communications Manager, Unity Connection, and IM and Presence Services, from the Infrastructure Configuration page. When you cross-launch a specific device, you can access the device UI and perform any operation directly on the server of the specific device that you have cross launched.

Rest your mouse pointer over a device in the object selector widget, and click the Quick View icon to view the version and IP address of the device being used. Refer to Adding Devices to know the list of actions that can be performed through device Quick View.

Note

- Cross launch to Cisco TMS requires HTTPS to be enabled on the TMS server. If HTTPS is not enabled, you must change the URL to HTTP in the cross launch window.
- When you cross launch Unified Communications Manager, the Find and List page appears. To learn how to perform specific operations on Unified Communications Manager, refer the Cisco Unified Communications Manager Administration Guide, Release 12.0.

  To learn how to perform specific operations on Unity Connection, refer the System Administration Guide for Cisco Unity Connection, Release 12.x.

  To learn how to perform specific operations on IM and Presence Service, refer the Monitoring Cisco Unified Communications Manager IM and Presence, Release 12.0.

Adding an Infrastructure Configuration Instance

To add an Infrastructure Configuration Instance:

Procedure

Step 1 Choose **Infrastructure Setup** > **Infrastructure Configuration**. All available devices are listed in the left pane.

Step 2 Expand each device to view the infrastructure product of that device.

Step 3 Click the desired infrastructure product to cross launch (Cross-launching Devices from Infrastructure Configuration) or launch it natively:

- When you cross-launch, the Find and List page of the device appears. Click Add New, enter the necessary information, and click Save.
- Some of the infrastructure products (whose versions are earlier than 10.0) are launched natively, where you can add a product instance and configure it within Provisioning. Perform the following:

  a. Click **Add** and enter the necessary information in the Infrastructure Configuration - configure Product Instance page. An asterisk next to a field indicates a required field. For descriptions of the infrastructure configuration product fields, see Infrastructure Data Object Fields, on page 337.

  b. Click **Apply** or **Save as Draft**.

  Apply sends the configuration immediately to the device. **Save as Draft** saves the configuration locally only. At a later time, the service can be pushed to the device either by clicking Apply or by using infrastructure configuration scheduling (see Scheduling an Infrastructure Configuration Task, on page 161).

  Also, when you choose Save as Draft, the provisioning state of the object becomes Uncommitted Add (for details on provisioning states, see Infrastructure Provisioning States, on page 162). The operational status is inactive, meaning the object has not been pushed to the device.

Note Clicking Apply may cause the devices to restart, and end calls in progress unexpectedly.

To copy an Infrastructure Configuration instance for a native launch, click Copy. In the Infrastructure Configuration - Configure Product Instance page, click the Draft Configuration tab and enter the necessary information. An asterisk next to a field indicates a required field. Applied Configuration tab shows the already configured instance. Click **Apply** or **Save as Draft**. The infrastructure configuration instance is saved with a "copy of" prefix.

To delete an Infrastructure Configuration instance for a native launch, you can do one of the following:

- To immediately delete the configured instance from the device, click **Delete**.
- If you want to push the order at a later time, click **Schedule Delete**.
- If your configured instance is still saved locally, click **Delete Draft**.

The provisioning state of the object becomes Uncommitted Delete (for details on provisioning states, see Infrastructure Provisioning States, on page 162). The operational status is active.

Delete Draft does not make that instance unavailable for selection in other infrastructure products or user services. For example, if a route partition is marked for deletion, it is still available for selection in a Line or Phone product, as well as Calling Search Space.

To edit an Infrastructure Configuration Instance for a native launch, click the instance for which you want to make changes. In the Draft configuration tab, make the desired changes. An asterisk next to a field indicates a required field. Enter the required information.

You can click **Apply** or **Save as Draft** to save your changes.

Note To clear the value of a setting that has a numeric value in Cisco Unified Communications Manager, you must enter a zero for the value. If you just clear the value, the setting does not get unset in Cisco Unified Communications Manager.

Scheduling an Infrastructure Configuration Task

The infrastructure configuration scheduling feature enables you to group and schedule instances with pending operations to be provisioned.

Infrastructure configuration scheduling requires you to create tasks. In a task you can add pending configurations and they can be either add, modify or delete operations. You can have pending items from more than one Processor in the same task, and you can schedule this task to run at a fixed time or schedule it to run after successful completion of another task.

To view the infrastructure configuration scheduled tasks, click **Schedule Configuration** tab (Choose **Infrastructure Setup** > **Infrastructure Configuration**).

You can narrow your results by using the search function. To access the search function, in the results page, click **Show Filter**, and the search criteria appears.

The infrastructure configuration task is based on its initiation type.

If the task's initiation type is date/time, the execution of the task begins at the scheduled date/time. An order is created with all items in the task. The task status changes to in progress and it can no longer be modified or deleted. If all items in the task are completed successfully, the task's status changes to complete. If any one detail fails, then the entire task is aborted. An aborted or failed task cannot be rerun. You will need to create a new task.

If the initiation type is another task, then the task begins after the successful completion of the initiating task. If the initiating task fails, this task will never begin, which will be indicated in the List of Tasks page.

Note After a task is created, it cannot be updated if it is in progress, completed, or failed. Before the task begins, you can change the schedule date or time and add or remove pending items that should be pushed as part of the task.

Procedure

Step 1 Choose **Infrastructure Setup** > **Infrastructure Configuration**.

Step 2 In the Infrastructure Configuration page, click **Schedule Configuration** tab.

Step 3 Click **Add New**.

Step 4 In the Schedule Pending Configuration - Configure Task page, enter the necessary information such as name description and so on. For operation type, you can add, modify, or delete infrastructure configuration instances. A task cannot perform more than one operation. You can select only one operation type.

Step 5 Select the task details (click the triangle icon), desired values and click **Select**.

Step 6 In the Schedule Pending Configuration - Configure Task page, click **Save**.

To delete a scheduled infrastructure configuration task, in the Schedule Pending Configuration - Configure Task page, click **Delete**.

To purge an infrastructure configuration task you must put provisioning into maintenance mode. The infrastructure configuration scheduling tasks (Completed, Failed, and Aborted) are stored on your system. You may want to periodically purge them. All data purging activities are performed through the Data Maintenance Configuration page. For more information on data purging, see Enabling Data Purging for Provisioning, on page 328.

Infrastructure Provisioning States

An infrastructure configuration request goes through when you perform infrastructure configuration activities.

Following are the infrastructure configuration process states:

- Uncommitted Add—Configuration created locally but does not exist on the device.
- Add in Progress—A pending configuration is in progress and being configured through an order. No changes are allowed in this state.
- Add Failed—An operation on this object failed.
- Add Scheduled—A pending configured object is scheduled in one of the tasks waiting to be executed. No changes are allowed in this state.

- Uncommitted Update—An object that exists on the device has been modified locally but has not been submitted to the device.
- Update in progress—Modify operation is in progress as part of an order. No changes are allowed in this state.
- Updated Failed—Modify operation failed.
- Update Scheduled—A pending configuration to change an object on the device is scheduled as part of a task. No changes are allowed in this state.
- Uncommitted Delete—An object that exists on the device has been marked for deletion. The request to delete the object has not been made to the device.
- Delete in progress—Delete operation is in progress as part of an order. No changes are allowed in this state.
- Delete Failed—Delete operation failed.
- Delete Scheduled—A pending configuration to delete an object from the device is scheduled as part of a task. No changes are allowed in this state.

Overview of Business Rules

Cisco Prime Collaboration Provisioning contains a predefined set of business rules that determine how components within Cisco Prime Collaboration Provisioning are used. These business rules control the processing of orders, the behavior of the synchronization processes, and the default values for various objects in the system.

Business rules are applied at a Domain level. When you install Cisco Prime Collaboration Provisioning, you configure the business rules in the Customer Domain Template according to your business processes. When you create a new Domain, it inherits the standard set of business rules from the Customer Domain Template. You can then change the business rules as required for each new Domain. Changes made to the Customer Domain Template affect only new Domains created after that point. For information on Customer Domain Template, see Customer Domain Template, on page 159.

In addition to business rules, new Domains inherit the default User Role information, and folders are automatically created in the Inventory Manager Instance Browser for the users, Service Areas, and Voice Terminals that will be placed into that Domain.

Rules can be data driven (Cisco Prime Collaboration Provisioning uses the Data field), enabled or disabled driven, or both. The descriptions of the rules indicate which applies.

Note For some business rules, the Data or Enabled field is not applicable, which is indicated by *N/A*. All user input in fields marked as *N/A is* disregarded by the system.

Business Rule Descriptions

Table 44: Business Rule Descriptions describes all the standard business rules in alphabetical order, along with their default Data and Enabled settings.

Table 44: Business Rule Descriptions

Rule	Description

AssignSoftPhoneName	Assigns a unique name to a SoftPhone that workflow is provisioning. The Call Processor automatically generates the name using the value in the Data field as the prefix, then adds the CTI port counter number + 1. The Call Processor checks if the combination of prefix + CTI port counter number is in use, and if it is, it adds 1 to the CTI port counter number until a unique combination is found.
	`Data SoftPhone_`
	
	`Enabled  true (n/a)`

ChangeUnityPasswordOnNextLogin	If enabled, a Cisco Unity Connection user will be forced to change the password after the password is reset in Cisco Prime Collaboration Provisioning. The Data field is not applicable for this rule, and it is disregarded by the system.
	`Data <blank>`
	`Enabled false`

ChangeCCMPasswordOnNextLogin	If enabled, a Cisco Unified Communication Manager user will be forced to change the password after the password is reset from Cisco Prime Collaboration Provisioning. The 'Data' field is not applicable for this rule, and it is disregarded by the system.
	`Data <blank>`
	`Enabled false`
	ChangeCCMPasswordOnNextLogin rule is enabled by default in Cisco Unified Communications Manager while adding a user. Hence, while provisioning an order for a user in Cisco Prime Collaboration Provisioning, ensure ChangeCCMPasswordOnNextLogin rule is enabled for the user.

ChangeProvisioningPasswordOnNextLogin	If enabled, a Cisco Prime Collaboration Provisioning user will be forced to change the password after the password is reset from Cisco Prime Collaboration Provisioning. The 'Data' field is not applicable for this rule, and it is disregarded by the system.
	`Data <blank>`
	`Enabled true`

Rule	Description

CreateSelfCareAccounts	If enabled, the system automatically creates login accounts for new users so that they can submit their own orders. When the rule is disabled, the system still creates login accounts, but those accounts cannot place orders for themselves.
	
	`Data <blank>`
	
	`Enabled true`

DefaultCallManagerPassword	Sets the default password for new Cisco Unified Communications Manager and Cisco Unified Communications Manager Express accounts, which are created when a phone or line is ordered for a user for the first time. You can also use this password with a Cisco SoftPhone to gain access to the user-assigned lines. Minimum length is five characters.
	
	Note This rule has a password that is randomly generated during deployment of the application.
	
	`Data <Random Password>`
	
	`Enabled true (n/a)`

DefaultCallManagerPIN	Sets the default PIN to be used when a user is activated in Cisco Unified Communications Manager. A user is activated in Cisco Unified Communications Manager the first time a line or phone is ordered for the user. Beyond initially setting the PIN, this rule is not used in Provisioning. Minimum length is five characters.
	
	Note This rule has a password that is randomly generated during deployment of the application.
	
	`Data <Random Password>`
	`Enabled true`

Rule	Description

DefaultCallManagerMLPPPassword	Specifies the default credentials for Multilevel Precedence and Preemption Authorization. To specify a default password, you must enter it in the Data field and set Enabled to true.
	Note This rule has a password that is randomly generated during deployment of the application.
	`Data <Random Password>`
	`Enabled true`

DefaultCUPMPassword	Specifies the default password for self-care accounts. By default, the user password is empty and these users will not be able to log in until an administrator changes their password in the user wizard. If you want to specify a default password, you must specify a default password in the Data field and set Enabled to true.
	Note The new password value should match the password policy.
	`Data <blank>`
	`Data true`

DefaultDeviceProfile	Used for Extension Mobility-enabled phones. The default setting of NONE (or left empty) causes the rule not to be used.
	`Data NONE`
	`Enabled true (n/a)`

Rule	Description

DefaultUnitySubscriberPassword	Sets the default password for new voicemail accounts on the Cisco Unified Messaging Systems, such as Cisco Unity Connection. The workflow uses the Data value as the initial password. In Cisco Unity Connection, this value must be an integer. Cisco Unity Connection rejects trivial values (for example, 12345). The Enabled field is not applicable for this rule, and it is disregarded by the system.
	
	The DefaultUnitySubscriberPassword rule does not validate the length of the default password entered in the data field. Cisco Unity Connection may have different credential policies configured.
	
	Depending upon the policies set on the devices, the Provisioning administrator should enter the default password in these rules. If the default password entered for these rules is not accepted by the devices, the reset credentials to default operation will fail with an error message returned from the device.
	
	Note This rule has a password that is randomly generated during deployment of the application.
	
	`Data <Random Password>`
	
	`Enabled true (n/a)`

DefaultCallManagerDigestCredentials	Specifies the default password for digest credentials. To specify a default password, you must enter it in the Data field and set Enabled to true.
	
	Note The new password value should match the password policy.
	
	`Data <blank>`
	
	`Enabled true`

Rule	Description

DefaultUserType	Specifies the user type that new users are assigned by default. The value of the Data field must contain the name of a valid user type.
	Note This rule should be set to the user role that makes up most of the organization. This will ensure that during Domain synchronization most of the users are set up correctly.
	`Data Employee`
	`Enabled true (n/a)`

DefaultWebAccessPassword	Sets the default password for new voicemail accounts' web access on Cisco Unified Messaging Systems such as Cisco Unity Connection. The workflow uses the Data value as the initial password. The Enabled field is not applicable for this rule, and it is disregarded by the system.
	The DefaultWebAccessPassword rule does not validate the length of the default password entered in the data field. Cisco Unity Connection may be configured with different credential policies.
	Depending upon the policies set on the devices, the Provisioning administrator should enter the default password in these rules. If the default password entered for these rules is not accepted by the devices, the reset credentials to default operation will fail with an error message returned from the device.
	Note This rule has a password that is randomly generated during deployment of the application.
	`Data <Random Password>`
	`Enabled true (n/a)`

Rule	Description

DescriptionString	Default description string used on new phones, new user device profiles (EM_Access), and new users. FIRSTNAME, LASTNAME, USERID, and EXTENSION are keywords that are replaced with the user's first name, last name, user ID, and extension respectively. (This information is the first line added to the user's phone.)
	
	For change owner orders, the default value is automatically applied from this rule. The new phone owner's first name, last name, user ID, and extension are used.
	
	Note If you wish to keep your phone description as previously configured, you should disable this rule.
	
	`Data FIRSTNAME LASTNAME USERID EXTENSION`
	
	`Enabled true (n/a)`

DNAutoReservation	If enabled, when a line is canceled, the directory number associated with the line will be automatically reserved for the original owner.
	
	`Data <blank>`
	
	`Enabled false`

DNAutoReservationTimeout	Specifies the period of time (days:hours) that the directory number remains in the Reserved state.
	
	`Data 7:0`
	
	`Enabled true`

DirectoryNumberBlockValidation	If enabled, Ordering line will be blocked when the directory number is not within the range of the directory number block. The Data field is not applicable for this rule and it is disregarded by the system.
	
	`Data <blank>`
	
	`Enabled false`

Rule	Description

IsAuthorizationRequiredForAddOrder	If enabled, an Approver must approve Add orders before provisioning can occur. If disabled, the system automatically approves Add orders.
	Note This rule does not take effect when you place orders using Auto Provisioning, Quick Provisioning, Batch Provisioning or the Provisioning NBI.
	`Data <blank>`
	`Enabled false`

IsAuthorizationRequiredForOrder	If enabled, an Approver must approve orders before provisioning can occur. If disabled, the system automatically approves orders.
	Note This rule does not take effect when you place orders using Auto Provisioning, Quick Provisioning, Batch Provisioning or the Provisioning NBI.
	`Data <blank>`
	`Enabled false`

IsAuthorizationRequired ForChangeOrder	If enabled, an Approver must approve Change orders before provisioning can occur. If disabled, the system automatically approves Change orders.
	Note This rule does not take effect when you place orders using batch provisioning or the Provisioning NBI.
	`Data <blank>`
	`Enabled false`

Rule	Description

LineDisplayString	Template string used to construct the Internal Caller ID display format for the phone line. If disabled, the system defaults to FIRSTNAME LASTNAME. This rule does not apply if the Service Area has a Cisco Unified Communications Manager Express as a Call Processor.
	
	The default value for the Display (Internal Caller ID) provisioning attribute is applied from this rule. If you specify CUPM_BLANK or an empty value in batch provisioning or through the Cisco Prime Collaboration Provisioning user interface, the value for the Display (Internal Caller ID) provisioning attribute comes from this rule.
	
	Therefore, if you want to set an empty value for the Display (Internal Caller ID) provisioning attribute, you must enable this rule and make sure its value is empty.
	
	Note For Call Processors, the combination of characters for First Name and Last Name cannot exceed 30 characters. If this limit is exceeded, when you place an order, the Call Processor sends an error.
	
	`Data  FIRSTNAME LASTNAME`
	
	`Enabled  true`

Match Department	If enabled, Call Processor user accounts are associated to this Provisioning Domain based on their department code value matching one in the specified list of values. The list of department code values must be enclosed in double quotes (") and separated by a semicolon (;) delimiter. Department code values may contain wildcard characters (* or %). For example, if you specify the following in the Data field: `"Dept 1";"";"Dept 2"` The Call Processor user accounts that belong to Dept 1 or Dept 2, or have no department code set, are associated to the Domain.

Rule	Description

Match Device Pool	If enabled, Call Processor user accounts are associated to this Provisioning Domain only if they have a phone which has the device pool value specified in the data field. The device pool value can contain wildcard characters (* or %) and should be prefixed with the Cisco Unified Communications Manager name value (this is the Call Processor name in Cisco Prime Collaboration Provisioning). The value must be in double quotes (") and separated by a semicolon (;) delimiter.
	For example:
	`“CUCM1:DevicePool1”;”CUCM2:Device*2”`
	Users who have a phone or Remote Destination Profile in Call Processor CUCM1 with the device pool DevicePool1 and users who have a phone or Remote Destination Profile in Call Processor CUCM2 with the device pool DevicePool2 are associated to the Domain.
	`Data <blank>`
	`Enabled false`

Match Location	If enabled, Call Processor user accounts are associated to this Provisioning Domain only if they have a phone that has the location value specified in the data field. The location value can contain wildcard characters (* or %) and should be prefixed with the Cisco Unified Communications Manager name value (this is the Call Processor name in Cisco Prime Collaboration Provisioning). The value must be in double quotes and separated by a semicolon (;) delimiter.
	For example:
	`“CUCM1:Location1”;”CUCM2:Loc*2”`
	Users who have a phone in Call Processor CUCM1 with the location Location1 and users who have a phone in Call Processor CUCM2 with the location Location2 are associated to the Domain.
	`Data <blank>`
	`Enabled false`

Rule	Description

MonitorPhoneReturnEnabled	If enabled, tracks whether phones have been returned by implementing an additional workflow activity that is assigned to the user group specified in the Data field.
	
	`Data Shipping`
	
	`Enabled false`

NameDialingInfo	This string is used to construct the auto-attendant name dialing string. FIRSTNAME LASTNAME are replaced, but not the extension.
	
	Note This feature is available for Cisco Unified Communications Manager version 3.3.3 only.
	
	`Data FIRSTNAME LASTNAME`
	
	`Enabled true`

PhoneAssignmentDoneBy	**(For Cisco Prime Collaboration Release 11.5 and later)** If you check the **Enabled** check box, the Assignment step for a Phone order workflow is assigned to the users who have access to the Activities menu or belong to any Full Access group. Otherwise, the workflow automatically assigns the phone and MAC address. The Data field is not applicable for this rule, and it is disregarded by the system. **Note** This rule is available in Cisco Prime Collaboration Provisioning Advanced only. Cisco Prime Collaboration Provisioning Standard does not support PhoneAssignmentDoneBy rule.
PhoneReceiptDoneBy	**(For Cisco Prime Collaboration Release 11.5 and later)** If you check the **Enabled** check box, the Receiving step for a Phone order workflow is assigned to the users who have access to the Activities menu or belong to any Full Access group. The Data field is not applicable for this rule, and it is disregarded by the system. **Note** This rule is available in Cisco Prime Collaboration Provisioning Advanced only. Cisco Prime Collaboration Provisioning Standard does not support PhoneReceiptDoneBy rule.

Rule	Description

PhoneReservationTimeout	Specifies the period (in days) that a phone remains reserved in the system. If disabled, then the phone is reserved indefinitely.
	
	`Data  10`
	
	`Enabled true  (n/a)`

PhoneShippingDoneBy	**(For Cisco Prime Collaboration Release 11.5 and later)** If you check the **Enabled** check box, the Shipping step for a Phone order workflow is assigned to the users who have access to the Activities menu or belong to any Full Access group. The Data field is not applicable for this rule, and it is disregarded by the system. **Note** This rule is available in Cisco Prime Collaboration Provisioning Advanced only. Cisco Prime Collaboration Provisioning Standard does not support PhoneShippingDoneBy rule.

PseudoUserID	Used to construct the NewUserID field in the exported data file generated by the Export Phones without the Associated Users feature. The following keywords are supported:
	
	• DIRECTORYNUMBER—Replaced with the value of Directory Number-Route Partition for the first line of the phone.
	
	• MACADDRESS—Replaced with the MAC address or device name (for soft phone).
	
	• RANDOMNUMBER—Replaced with an automatically generated six-digit, random number.
	
	If this rule is disabled, you cannot use Export Phones without Associated Users feature.
	
	`Data pseudo-DIRECTORYNUMBER`
	
	`Enabled true (n/a)`

Rule	Description

PurgeUponUmRemoval	If enabled, a user's e-mail and voicemail are purged from the system when their Cisco Unity account is removed.
	Note You enable or disable this rule by specifying true or false in the Data field.
	`Data false`
	`Enabled true (n/a)`

DirectoryNumberBlockListing	The data can be **Single** or **All**. When **Single**, it displays directory number blocks assigned to the selected service area. When **All**, it displays directory number blocks assigned to all service areas within a domain.
	`Data <blank>`
	`Enabled false`

Sync All Users (Call Processor)	If enabled, during a Domain synchronization, all of the user accounts in all of the Call Processors in the Domain are assigned to the Domain being synchronized. If disabled, only users whose department is the same as the Domain are assigned to the Domain.
	`Data <blank>`
	`Enabled false`

Sync All Users (Unity Connection)	If this rule is enabled, all user accounts in a given Unified Message Processor are assigned to a Provisioning Domain. Otherwise, only user accounts in the given Unified Message Processor with a matching Call Processor user account are assigned.
	`Data  <blank>`
	`Enabled false`

Sync Only Existing Users	If enabled, then during a Domain synchronization, no new users are created. Only services of existing users in the Domain are synchronized.
	`Data <blank>`
	`Enabled false`

Rule	Description

Sync Primary User From Unity Connection	If enabled, user information is updated from the associated Unified Message Processor account; otherwise it is updated from the Call Processor. When the rule is enabled, you can also specify the Unified Message Processor ID, which takes precedence if a user has accounts on multiple Unified Message Processors. This value can also be left blank to indicate no preference.
	
	`Data <blank>`
	
	`Enabled false`

Configuring Business Rules

When you change business rules, you must first select the Domain. You can change the values for the rules and whether they are enabled. You cannot change the rule names or descriptions.

All business rules have the following properties. You can modify the Data and Enabled fields.

Property	Description
Rule Name	Name of the rule
Description	Detailed description of the rule
Data	Value to be specified for the rule
Enabled	Specifies if the rule is applied. Valid values are true or false.

Note You must carefully review the documentation for each business rule to ensure that you set the Data and Enabled properties appropriately.

Note Provisioning does not have a default reset capability for business rules. If you change a business rule's settings and later want to return to the default settings, you will have to manually change the settings.

The following procedure uses the AssignSoftPhoneName rule as an example of how to change rule properties.

Procedure

Step 1 Choose **Administration** > **Rules**.

Step 2 In the Rule Configuration page, select the Domain that you want to change the rule for.

Step 3 Select the rule under Configure Rule.

Step 4 Click the Edit icon. The Data and Enabled fields become active.

Step 5 Make the required changes and click **Save**. The changes are added to the AssignSoftPhoneName rule.

To configure the Domain Synchronization Rules, select **Configure Domain Sync Rules** and select the synchronization rules. See Configuring Business Rules for Domain Synchronization, on page 103 for details.

When you configure Provisioning, it is critical that you plan how you will use your business rules and how you want the Provisioning components to work. At a minimum, you must consider the following rules:

- AssociateAllUsersInCallProcessor
- CreateSelfCareAccounts
- EmailSender
- IsAuthorizationRequiredForAddOrder
- IsAuthorizationRequiredForOrder
- IsAuthorizationRequiredForChangeOrder
- MailHost
- OrderProvisionedEmailTemplate
- OrderRejectedEmailTemplate
- PhoneAssignmentDoneBy
- PhoneReceiptDoneBy
- PhoneShippingDoneBy
- DirectoryNumberBlockValidation
- DirectoryNumberBlockListing

Usage Scenarios for Configuring Business Rules

Some examples on how you could configure user access, configure products, and orders are listed in the following table:

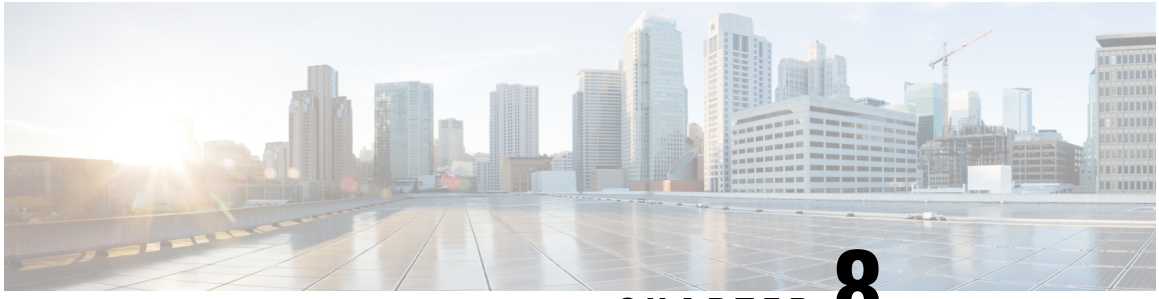
Table 45: Usage Scenarios for configuring Business Rules

Usage Scenario	Business Rule

To configure user access	You can set the following Business Rule:
	• If a user is using a line, to automatically reserve that number for the specific user
	  • DNAutoReservation—Toggles the reservation
	  • DNReservationTimeout—How long to reserve the numbers
	• To configure self-care accounts for users
	  • CreateSelfCareAccounts
	  • DefaultCUPMPassword
	• To assign the default user type for a new user
	  • DefaultUserType
	• To assign users of a specific Domain to manage phone inventory
	  • DomainPhoneManagement
	  • PhoneReservationTimeout
	• To assign users to manage user types
	  • DomainUserTypeConfiguration

To configure products	• To assign a name to CTI ports in Cisco Unified Communications Manager
	  • AssignSoftPhoneName—See rule for default value
	• To reserve directory numbers
	  • DNReservationTimeout
	• To track whether phones have been returned after having been canceled
	  • MonitorPhoneReturnEnabled

To configure services	• To use default passwords for Cisco Unified Communications Manager accounts
	  • DefaultCallManagerPassword
	  • DefaultCallManagerPIN
	  • DefaultUnitySubscriberPassword
	
	• To send e-mails when an order is rejected or completed (You have the option of not sending any e-mails)
	Note You must enable both EmailSender and MailHost for e-mail features to work in Provisioning.
	  • EmailSender
	  • MailHost
	  • OrderProvisionedEmailTemplate
	  • OrderRejectedEmailTemplate
	
	• To check if authorization is required for any type of order
	  • IsAuthorizationRequiredForAddOrder
	  • IsAuthorizationRequiredForOrder
	  • IsAuthorizationRequiredForChangeOrder
	
	• To validate manually entered DNs against the DN range for a service area or for all service areas within the same domain
	  • DirectoryNumberBlockValidation
	  • DirectoryNumberBlockListing
	
	• To handle phone assignment, shipping, and receiving
	  • PhoneAssignmentDoneBy
	  • PhoneReceiptDoneBy
	  • PhoneShippingDoneBy
	
	• When a voicemail and/or e-mail account is canceled, to remove messages in the canceled voicemail and/or e-mail accounts
	  • PurgeUponUmRemoval



CHAPTER 8

Managing Inventory

Managing Endpoint Inventory

You can add, update, or remove endpoints using the endpoint inventory. You can add and update directory numbers, reserve them for specific users, and clear directory numbers whose designated length of time in the Reserved state has been exceeded.

In addition to the above, you can also search for endpoints that are not associated to any users and those unused endpoints can be associated to a specific user.

Cisco Prime Collaboration Provisioning tracks the information about all services and users in an internal asset management inventory system. This information can be viewed by an administrator.

You can view the endpoint inventory report based on the Domain. The following details are displayed in the Endpoint Inventory page:

Table 46: Endpoint Inventory Management Page Field Descriptions

Field	Description
Call Processor	List of call processors.
Model	List of endpoint models.
Endpoint	You can add a new endpoint by specifying the domain, model, MAC address, and status. You can also click the Chooser icon to view the list of existing endpoints.
Domains	List of managed Domains.
Model	List of endpoint types.
MAC Address	Hexadecimal value that identifies the endpoint. The MAC address must be 12 characters in length. Valid values are alphanumeric characters (A-Z, a-z, 0-9), for example, 201B79989002.

Field	Description
Status	The status of the endpoint. Possible values are the following: • In-use—The endpoint is being used by a user. • Reserved—The endpoint is booked for a specific user. • Available—The endpoint is available, and can be manually or automatically assigned to a user. • Returned—The endpoint is returned to inventory, but its arrival is not confirmed. • Provisioning—The endpoint is currently being provisioned.
Reserved For (optional)	Specific user that the endpoint is reserved for.
Reserved On (optional)	Date that the endpoint was reserved on. It automatically appears after the endpoint information has been added or updated.
Reservation Timeout (optional)	Period of time, in days, that an endpoint will stay reserved in the system. Provisioning administrator sets the reservation timeout, therefore this field is non editable. The endpointReservationTimeout rule determines the endpoint reservation timeout for a Domain (see Overview of Business Rules, on page 163).

Note Self-Care option is available for users to set up lines, manage services, and configure endpoint options quickly and easily. For more information, see Customizing Your Personal Settings, on page 245.

If you are assigned the Ordering authorization role, you can perform the following tasks to manage the endpoint inventory:

Task	Description	Procedure
Search Endpoints Without Associated User	You can search for the endpoints that are not associated to any user and assign the endpoints to a specific user. **Note** Orphaned search results contain orphaned endpoints present in your domain along with global resource endpoints.	1. Choose **Advanced Provisioning** > **Manage Endpoints**. 2. Select the endpoints and click **Assign Selected Endpoints to User**. **Note** If you select more than one endpoint associated to different call processors, users associated to the respective call processor across the domain are listed. 3. Select a user and click **Save** to create an order.

Task	Description	Procedure
Add	You can add endpoints that are available to all users, or you can designate endpoints for specific users.	**1.** Choose **Advanced Provisioning** > **Manage Endpoints**. **2.** Enter the value in the Endpoint Inventory Management page and click **Add**. **Note** Third-party devices must be added as SIP devices in Cisco Prime Collaboration Provisioning. See Supported Devices for Prime Collaboration for more information.
Update endpoint information	You can change endpoint information.	**1.** Choose **Advanced Provisioning** > **Manage Endpoints**. **2.** In the Endpoint field, click the Chooser icon. **Note** You can search for the endpoint based on a complete or partial MAC address. You can use an asterisk (*) as a wildcard character at the beginning or end of the MAC address, but not in the middle. Do not specify SEP in the search criteria. **3.** In the Choose an Endpoint dialog box, select the endpoint that you require. **4.** Update the endpoint information as required and click **Update**. **Note** You cannot update an endpoint that is in In-use state).
Remove endpoints	You can delete endpoints from the inventory list.	In the Endpoint Inventory Management page, click the Chooser icon. In the Choose an Endpoint dialog box, select the desired endpoint, and click **Remove**. You cannot delete an endpoint that is In-use state. The endpoints that are not associated to any users are called as orphan endpoints. You can identify these endpoints and delete them if not required. To identify orphan endpoints, in the Endpoint Inventory Management page, click **Search Endpoints Without Associated User**. To delete orphan endpoints, select one or multiple endpoints from the list, and click **Delete Selected Endpoints**.

Task	Description	Procedure
Clear expired reservations	If required, you can clear all endpoints whose reservation time has expired, from the inventory. You can clear expired reservations for endpoints to change the status of the endpoints from Reserved to Available.	In the Endpoint Inventory Management page, select the appropriate domain and then click **Clear Expired Reservations**.

Managing Directory Number

In most cases, Service Area Directory Number Blocks (DNBs) are used to allocate directory numbers. However, you can explicitly track (store and manage) directory numbers that are associated with each Service Area in the Provisioning inventory.

You can add and update directory numbers, reserve them for specific users, and clear directory numbers whose designated length of time in the Reserved state has been exceeded.

Note To change the length of time that a directory number can remain in the Reserved state, you can modify the DNReservationTimeout rule. For more information, see Overview of Business Rules, on page 163.

Directory numbers can be in these states: In-use, Reserved, or Available.

When a line is added, Cisco Prime Collaboration Provisioning allocates directory numbers using the following process:

1. Checks if a directory has been reserved for the user.
2. Checks for a directory number in the Available state.
3. Checks the Service Area DNB for next available directory number.

In the Service Area component of the Domain, you can create DNBs, not individual directory numbers. After a directory number has been allocated to a user, Cisco Prime Collaboration Provisioning tracks the individual directory number.

The following details are displayed in the Directory Number Inventory page.

Table 47: Directory Number Inventory Management Page Fields

Field	Description
Directory Number	Specify the Directory Number that you want to add or update.
Call Processor/Route Partition	The Call Processor and route partition that the directory number is added to. **Note** The directory number is not added at this time. It is reserved for adding to the Call Processor once an order that requires one is received.

Field	Description
Status	The status of the number. Possible values are: • In-use—The directory number is currently being used by a user. • Reserved—The directory number is booked for a specific user for a specific period of time. • Available—The directory number is available, and can be assigned to any user.
Reserved For (Optional)	Specific user that the directory number is reserved for.
Reserved On (Optional)	Date that the directory number was reserved on. It appears automatically after the endpoint information has been added or updated.

You can perform the following tasks to manage the directory numbers in the inventory:

Task	Description	Procedure
Add	When you add a directory number, you can specify a status for it and/or reserve it for a particular user. The same directory number can exist in different Call Processors. When you add a directory number, you must specify both the Call Processor and route partition.	1. Choose **Advanced Provisioning > Manage Directory Numbers**. 2. In the Directory Number Inventory Management page, click Add New Directory Number. The fields in the right pane become editable. 3. Complete the fields as required (see Table 47: Directory Number Inventory Management Page Fields), and click **Save**.
Update directory number	You can search for and select a directory number to update. **Note** You cannot update the status of a directory number that is in In-use state.	1. Choose **Advanced Provisioning > Manage Directory Numbers**. 2. In the Directory Number field, do one of the following: • If you know the directory number, enter it and then click **Search**. • Search for the directory number, using an asterisk (*) as a wildcard. From the Choose a Directory Number dialog box, click the required directory number. 3. Click **Update Current Directory Number**. The fields in the right pane become editable. 4. Complete the fields as required (see Table 47: Directory Number Inventory Management Page Fields), and click **Save**.

Task	Description	Procedure
Clear expired reservations	You can clear expired reservations for directory numbers to place the directory numbers back into the available pool.	In the Directory Number Inventory Management page, click **Clear Expired Reservations** To set the number of days that the directory number is reserved for, see Overview of Business Rules, on page 163.
Delete directory number	You cannot delete a directory number that is in use.	In the Directory Number Inventory Management page, select the directory number and click **Delete**.

Managing Voicemail

You can search and delete voicemails that are not associated with any user.

To search and delete orphan voicemails:

Procedure

Step 1 Choose **Advanced Provisioning** > **Manage Voicemails**.

Step 2 In the **Unity Connection** field, select a Unity Processor.

Step 3 Click **Search**.

Step 4 To delete orphan voicemails, select one or multiple voicemails from the list, and click **Delete Voicemail**.

Attach Voicemail

If you delete a DN from Cisco Unified Communications Manager, the line is deleted and the voicemail associated with the line becomes an orphaned voicemail. You can associate an orphaned voicemail if you re-add the same DN or if you create a new DN for the user. An orphaned voicemail can only be associated to the user to which it belongs to and not any other user.

Note In **Action for stale LDAP users** field, when you set the option 'Deleteuser, but keep services in Provisioning and CUCM', Cisco Prime Collaboration Provisioning creates an orphaned voicemail. The Managed VoiceMail page lists the orphaned voicemail and you can delete it from the list.

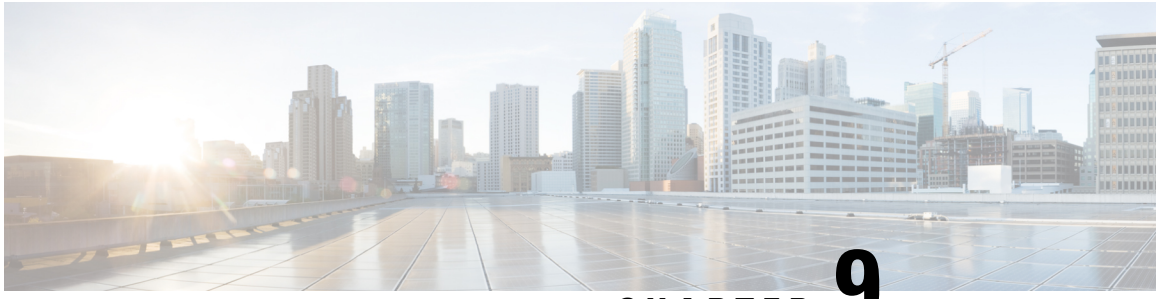
To associate the orphaned voicemail with a line:

Procedure

Step 1 Click on the **Attach Voicemail** link.

Step 2 Select the voicemail alias from the drop-down list.

Step 3 Click **Provision Services**.



CHAPTER 9

Provisioning Dashboards and Reports

Provisioning Dashboards and Reports Overview

On a day-to-day basis, operations personnel are likely to use the Dashboard displays to monitor the IP telephony environment. Cisco Prime Collaboration Provisioning has three dashboards. They are:

- Global Admin Dashboard—To manage the real-time information about the operational status of your processor, device, domain, and users.
- Domain Admin Dashboard—To manage the real-time information about the operational status of your domain related devices and users.
- User Dashboard—To manage the details of Running, Pending and Failed orders. The user dashboard is shown for users other than admin, ordering and self-care roles.

The benefits of Provisioning Dashboard are:

- Easy access to information —You can view the processor capacity, device synchronization status, pending orders, deployment details. You can also view the logged in and locked users.
- Easy customization—You can modify and personalize your dashboard and configuring your dashboard layout to display what you want to see.
- Lightweight GUI—Data is displayed in the Unified Dashboard and use of external pop-up windows are minimized.

Global Admin Dashboard

The Home dashboard allows you to view important statistics and details of the processors, pending orders, status of the device synchronization, domains and their deployment details, and users who are logged in as well as locked.

The dashboards are available under Home.

You can see all of this on a single page, instead of navigating through several pages. You can also click the links provided in the dashboard to view the relevant details.

A Pie Chart displays the details of the Licensed and Used Voice Terminal (Endpoints). To view the Pie Chart, you need to have Adobe Flash Player installed in your system. If it is not installed, you are prompted to install it.

The table below describes the dashlets available under Global Admin, Domain Admin and User dashboards.

Table 48: Provisioning Dashboard

Dashlet	Description	Global Admin	Domain Admin	User Admin
Capacity	Processor related details are listed in this pane. You can view the list of processors, available license count and also the count of used licenses. The graphical representation of the available and used licenses is shown in this pane.	X	—	—
Pending Order Status	You can view the list of the status of the Running, Pending and Failed orders. The Order number is available as a hyperlink and you can access the link to view the order details. The User can view the list of orders that are waiting for approval and also for assigning. For order related details, see Orders Overview, on page 251.	X	X	X

Dashlet	Description	Global Admin	Domain Admin	User Admin
Device Sync Status	You can view the list of devices and their synchronization details. The status and the completion date of the synchronization is displayed. A Search filter is available in this pane to search for devices, based on their name and type. Information available in Device Sync Status is in read only mode. For synchronization details, see Synchronizing Processors, Users, and Domains Overview, on page 93.	X	X	—

Dashlet	Description	Global Admin	Domain Admin	User Admin
Deployment Details	You can view the list of domain groups and their configuration details. Domain name can be accessed to launch the Domain Configuration screen. The count of the user and the service area associated with the domain are displayed along with the synchronization completion date. A Search filter is available in this pane to search for a particular domain, user, service area or based on the synchronization completion date. Information available in Deployment Details pane is in read only mode. For Domain and their configuration details, see Adding a Domain, on page 64.	X	X	—

Dashlet	Description	Global Admin	Domain Admin	User Admin
Logged In Users	You can view active sessions and log out single or multiple active sessions. The details of the active sessions can be viewed in this pane. For details on maximum number of concurrent logins, see System Capacity for Cisco Prime Collaboration Provisioning. Using the Logout button you can end single or multiple active sessions. This pane is available only when you have globaladmin privileges. See Viewing or Logging out Active Sessions, on page 240.	X	—	—
Locked Users	You can view the list of locked users in this pane. Unlock button is available to unlock the locked users. This pane is available only when you have globaladmin user privileges.	X	—	—

Provisioning Reports

Cisco Prime Collaboration Provisioning provides the following set of preconfigured reports:

Report	Description
Service Area	Provides the Call Processor, Message Processor, Route Partition, User Roles, Emergency Location (ELIN) Group, and Directory Number block details for all the Service Areas configured in Cisco Prime Collaboration Provisioning.

Report	Description
Resource Configuration	Displays the associated domain, device pool, and service area for each Call Processor. It also displays the user name, IP address, associated domain, and user template for each Message Processor.
Service Configuration	Displays the service catalog. It lists the available telephony products, infrastructure configuration products, and services. It also displays the services and endpoints that are associated to each user role for all the domains.
Endpoint Inventory	Displays the MAC address, device name, domain, service area, type, Call Processor, call search space, route partition, device pool, and user id for all the endpoints.
DN Inventory	Displays the Call Processor, route partition, call pickup group, usage status, and reservation status for all the directory numbers configured in Cisco Prime Collaboration Provisioning.
Directory Number Block	Displays the service area, first number, last number, block size, and minimum length for all the directory number blocks configured in Cisco Prime Collaboration Provisioning.
Audit Trail	Displays the following events: • User login • User logout • Password or PIN change • Password or PIN reset • Voicemail account unlocked • Account locked • Account unlocked • Timeout For more information about the Audit Trail report, see Audit Trail Report, on page 196.

Report	Description
Endpoint/Line Mismatch	You can use the following Endpoint/Line Mismatch Reports to identify the lines that are not associated to endpoints: • Users without Lines • Users with Lines but No Endpoints • Unassigned Lines • User Service Report: This report includes users with all provisioned services and products. Included fields are User Id, Domain, First Name, Last Name, Middle Name, Email, Phone Number, Product Id, Service Information, Description, Service Area, Phone Button Template, Type, Call Processor, Call Search Space, Route Partition, Device Pool, Company, Street, City, State, Country, Zip code, Auto-Provisioning Status Message, and Auto-Provisioning In-Process Message. **Note** This feature is not compatible with Cisco Prime Collaboration Provisioning10.x Cisco Prime Collaboration Provisioning servers.

To view provisioning reports, choose **Reports**.

Click the Communication Manager Reporting link under the Reports menu, to launch the Communications Manager Reporting page. This page will list all the Communication Manager devices that are configured in Cisco Prime Collaboration Provisioning. When you click on a particular Communication Manager link, Cisco Unified Reporting application will be cross launched for that Communication Manager.

Generating Endpoint Inventory Report

To generate Endpoint Inventory report:

Procedure

Step 1 Choose **Reports** > **Endpoint Inventory**.

Step 2 Select the domain and endpoint model.

Step 3 Do one of the following:

- To execute the search and display the search results, click **Search.**
- To execute the search and display the search results in .tsv format, click **Export**. The search results are exported in a tab separated value format.

Step 4 To change the settings to default, click **Reset.**

Step 5 Click **Select date and time to schedule report** link.

Step 6 Select a date and time from the calendar window.

Step 7 Select the UTC Offset or the location details.

Step 8 Click **Select** to set a date and time for scheduling the report.

You can also generate Endpoint Inventory report from the Manage Endpoints page:

1. Choose **Advanced Provisioning** > **Manage Endpoints**.
2. In the for domain field, select the Domain for which you want to view the report.
3. Click **Search Endpoint**.

   In the Endpoint Inventory Report, click **Edit** next to the endpoint to launch the Endpoint Inventory Management page. This field is populated with the endpoint information.

Note The Endpoint Inventory search is executed only if your login belongs to a Policy or Administrator group.

Audit Trail Report

The following table describes the fields displayed in the Audit Trail Report.

Field	Description
Date	Date and time of the event.
User ID	The user ID of the performer of the audit event.
Action	Lists all supported actions such as Add User, Update User, Delete User, User Login, User Logout, Lock User, Unlock User, and change in Digest Credential.
Status	Specifies whether the event is successful or failed.
Client IP	Specifies the IP address of the client during User Login, User Logout, Session Timeout, and Lock User.
Details	Lists the details of a specific audit trail based on the action. Details may include: User, Domain, Phone Number, Login, Logout, Lock, Unlock, User Role, User Type, Email, Selfcare, First Name, Middle Name, and Last Name.

The Audit Log Trail report can also be used to track the orders. It helps you to track the activities performed by a user and also to identify when the action took place. For example, based on user login or logout events, you can search for the orders created by a particular user during the login period. You can export audit data in .tsv format based on filtering provided in the user interface. To view the details of a specific audit trail, hover over **Quick View**.

The audit table has the entries of last 24 hours by default. The user can select a specific date range from the date filter, and the entries that are available gets populated in the table.

The user cannot view the entries which are purged. The purging period should be specified in the **Administration** > **Data Maintenance** page.

For Cisco Prime Collaboration Provisioning release 12.5 and later:

The following is the procedure to back up audit trails:

1. Navigate to **Report** > **Audit Trail** and click on the **Scheduled Export** button.
2. Select the **Enable Audit Backup** checkbox to enable audit back up.
3. Select the start time from the calendar in the **Start Time** field.
4. Schedule the recurrence of the audit backup from the following options:
   - None
   - Daily
   - Weekly
   - Monthly
5. Fill in the following SFTP location details in the **SFTP Backup Location** box:
   - Hostname/IP address
   - Path
   - Port
   - Username
   - Password
6. For encrypting the backup file, in the **Password Protection** box, type the password in the **Password** field and re-type the password in the **Confirm Password** field.

Note Ensure that 7z is installed on the SFTP server. The password that you insert in step 6 will be used to decrypt the backup file. You must remember this password. You will not be able to unzip the file without it.

7. Click **Save**.

Troubleshooting

Issue: Latest audit events are not displayed in the audit report after refreshing a page.

Recommended Action:

- Clear Date filter.
- Change Date filter for current timestamp.

CHAPTER 10

Managing Users

Managing Users

A user is a person who has active IP Telephony services. Cisco Prime Collaboration Provisioning allows you to add users, synchronize user information, reapply the services, update user information, and domain specific user roles.

The user role refers to the role that a user will have within an organization. This role dictates the services to which the user is entitled. User roles are predefined in the system.

Note

- Any out-of-band configurations (configurations that are performed directly on the processor but not synchronized with Cisco Prime Collaboration Provisioning) can result in failed orders. You must always synchronize Cisco Prime Collaboration Provisioning with the processors that it is provisioning.
- For Cisco Prime Collaboration Provisioning 12.3 and later, the admin and globaladmin users cannot be created using the User Provisioning page of Cisco Prime Collaboration Provisioning User Interface.
- User ID must contain more than one character.

Adding Users

Note To create a new user retaining the user information during system reboot, refer the following steps.

To add users:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 In the **User Provisioning** page, click **Add.**

Step 3 In the Add User window, if you want to add user click **User** radio button, else click **Open Space** radio button, and enter the User ID, Domain, and Name. Also, enter values for other fields if required.

Expand the **Additional Settings** pane to enter location and contact details.

To launch quick view for a particular domain or user role, while selecting the domain and user role, click the drop-down menu and rest the mouse on quick view icon.

Note While adding or editing a user, you can select multiple user roles. In the Mulitple User Role box, if the popup quickly opens and disappears, then you need to long-press on the arrow icon for a few seconds and the popup reappears.

Step 4 In the **Save and Begin Provisioning** drop-down:

- To save the details and launch the Service Provisioning page for the user, click **Save and Begin Provisioning**.
- To save the details and add another user, click **Save and Add Another**.
- To save the details and close the Add User window, click **Save and Close**.
- To save the details and view services if you choose to Auto-Provision Parameters based on the user role, click **Save and View Services**.

Note

- If you are removing a user who has services associated, you are notified to disassociate the services before removing the user.
- To add a user, the **LDAP integration** field in **Device Setup**page must be **None**.
- The user ID must be unique and case sensitive. Valid values are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), apostrophe (‘), space ( ), and at sign (@).
- A user created locally in a Cisco Prime Collaboration Provisioning domain that is LDAP-integrated, will be added to Cisco Unified Communications Manager as a local user. If the Unified Communications Manager processor has a synchronization schedule that sets its LDAP directory settings, the user will be updated to LDAP-integrated after this synchronization occurs.
- For LDAP users, all fields, except Manager User ID, Directory URI, Voicemail email ID, in the **Additional Settings** pane are updated with the values in LDAP only if you perform an LDAP synchronization.
- To create a username for Cisco Unified Communications Manager Express and Cisco Unity Express, enter only alphabetical characters in the First Name and Last Name fields. If you use other types of characters, orders for the user will fail.
- To create a username for Call Processors, the combination of characters for First Name and Last Name cannot exceed 30 characters. If this limit is exceeded when you provision, the Call Processor sends an error message.
- Room role allows you to provision endpoints without an associated user in the Call Processor.
- While selecting roles for user, the default or Employee user role should be configured to match the typical setup of employees in your organization. If you do not configure the default or Employee user role to meet your needs, you may not see all the desired options in the employee user record.
- The DefaultUserType rule controls which user role is set as the default. Cisco Prime Collaboration Provisioning comes with the Employee user role configured as the default user role. If you update the default user role name for a domain in Cisco Prime Collaboration Provisioning, ensure that you update the DefaultUserType rule with the new default role name for that domain.
- Changing the username does not also change the endpoint or line description field for the user (if an endpoint or line was ordered for the previous username).
- For Cisco Unified Communications Manager Express and Cisco Unity Express, enter only alphabetical characters in the First Name and Last Name fields. If you use other types of characters, orders for the user will fail.
- For Cisco Unified Communications Manager, the combination of characters for First Name and Last Name cannot exceed 30 characters.
- If a user does not have any associated services, you are prompted to confirm removal of the user.
- When a service is disassociated from a user, the service is not deleted or disassociated on the device (processor); it is only disassociated within Provisioning.
- When a subsequent Domain synchronization occurs, depending on the synchronization rules, the user could be created again, and the services could be associated with the user.

Cross-launching Related Links in Unified Communications Manager and Unity Connection from User Provisioning

Cisco Prime Collaboration Provisioning allows an administrator to cross launch Manager configuration and Assistant configuration for a selected user. As an administrator, you can cross-launch Related Links Pages for Users, Endpoints and Lines from Cisco Prime Collaboration Provisioning. When you cross-launch the Manager configuration and Assistant configuration, you can access the UI and perform any operation directly on the server. Using Single Sign-On, you can cross launch to a few of the applications.

If the Voicemail service is provisioned for the user, the cross-launch links from the Voicemail service: Notification Devices, Alternate Extensions, Greetings, Private Lists.

Rest your mouse pointer over **User Services** in the **Service Details** page (**User Provisioning** select a user), and click the quick view icon to view the Manager configuration and Assistant configuration cross launch link.

Related Topics

Overview of Authorization Roles, on page 210
Single Sign-On for Cisco Prime Collaboration Provisioning, on page 25

Moving a Single User

Before you begin

Ensure the following before performing a single user move:

- You must have administration privileges to perform this task.
- User can be moved from one domain to another irrespective of the service area, provided they belong to the same call processor.
- User can be moved from one service area to another provided they belong to the same domain and call processor.
- Users cannot be moved unless they are on the same cluster. Users cannot be moved between clusters.

To move a single user from one domain to another:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 In the **User Provisioning** page, select a user and click **Move**.

Move User window appears with options for single user move.

Step 3 Select a new domain from the **New Domain** drop-down list, where the user will be moved.

Step 4 Select the service area from the **New Service Area** drop-down list. This drop-down will list the service areas in a domain based on the services that are configured for a user. For example, if a user has voice mail service

enabled, service areas that are not associated with the Cisco Unified Communications Manager will not be listed in this drop-down.

Step 5 Click **Apply to All Services** to apply all services to the new service area.

If you want to update the services with new settings, you can still select a service and choose a new service area and service template for a particular service.

Check the **Keep Service Area and Template Settings** check box to apply the service area attribute settings alone to the selected service.

Note You cannot apply Service Template settings when you select this check box.

Step 6 Save the settings and click **Move User** to initiate the single user move.

Once the move is successful, a new order is created for that user.

Note To view the move status, hover over **Quick View**.

You cannot move a single user when user synchronization/domain synchronization/Cisco Unified CM synchronization is in progress.

Note **For Cisco Prime Collaboration Provisioning Release 12.5 and later**

Similar to normal users, you can move the Pseudo user IDs across domains and service areas.

Moving Bulk Users

Before you begin

Ensure the following before performing bulk user move:

- You must have administration privileges to perform this task.
- All users selected for bulk move must be from the same domain and cluster.
- Bulk move cannot be performed for multiclustered users.

To move a bulk of users from one domain to another:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 In the **User Provisioning** page, select users and click **Move**.

Bulk Move window appears.

Step 3 Select a new domain from the **New Domain** drop-down list, where the user will be moved.

Step 4 Select the service area from the **New Service Area** drop-down list.

Step 5 Select the **Endpoint Settings** and **Line Settings** if you want to configure new service area settings along with the move.

This is an optional step. Skipping this step will move the users to a new service area with the existing service area settings.

Step 6 Click **Move User** to initiate the bulk move.

Once the move is successful, a new order is created for that user.

Note To view the bulk move status, you can either hover over **Quick View** or click **Bulk Move Status** to view the detailed information on the move.

You cannot move bulk users when user synchronization/domain synchronization/Cisco Unified CM synchronization is in progress.

Note **For Cisco Prime Collaboration Provisioning Release 12.5 and later**

Similar to normal users, you can move the Pseudo user IDs across domains and service areas. You can also move combinations of normal and pseudo users.

Importing Users Using a Text File

Cisco Prime Collaboration Provisioning enables you to import multiple users in a single operation in the following ways:

- Using a file in text (TXT) format
- Using an LDAP server

For information on adding individual users, see Adding Users, on page 199.

To import users using a text file:

Procedure

Step 1 Click **User Provisioning** > **Import Users**.

Step 2 In the Import User dialog box, click the **From File** radio button.

Step 3 Click **Browse** and select the user import file.

You can also download the sample import file available in the Import Users dialog box for your reference. You can edit the sample file (.txt) using Excel, save the updated spreadsheet as tab-delimited text file, and import the file. OrderType, UserID, LastName, and Domain are mandatory fields (rest of the fields are not mandatory; you can leave them blank).

If you want to enable auto-provisioning for a user, you must set the DoNotAutoProvisionServices field to "False". Also, you must provide the values for Auto-Provisioning ServiceArea and Auto-Provisioning Line Type fields. If you have selected the Line Type as Chosen Line, you must provide the value for Auto-Provisioning Directory Number field.

Note Valid values for user ID field are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), apostrophe ('), space ( ), and at sign (@).

Step 4 Click **Import**.

The Import button remains disabled, till you select a file for import. After you click the Import button, the import status of the file will be displayed in the Import Users page. To see the import status of the previously imported file, click **View Last File Import Status**.

Cisco Prime Collaboration Provisioning creates the users based on the details provided in the file. If Auto-provisioning is enabled (set to True), Cisco Prime Collaboration Provisioning will automatically provision the default services for the users based on the Auto-provisioning parameters provided in the uploaded file.

Importing Users From an LDAP Server

To import users from an LDAP server:

Procedure

Step 1 Click **User Provisioning** > **Import Users**.

Step 2 In the Import User dialog box, click the **From LDAP** radio button.

Step 3 Select the domain.

Ensure that Directory Number blocks are available in the selected domain for the users that are synchronized without DN numbers.

Step 4 Click **Import**.

To view the latest LDAP synchronization report, click **View Last LDAP Sync Report**

Note If a user is mapped to a user role for which auto-provisioning is enabled, the configured services will be automatically provisioned for that user.

See Configuring LDAP Server Synchronization, on page 113 for more information.

Exporting Users

Cisco Prime Collaboration Provisioning enables you to export users along with their user information. However, you cannot export the services provisioned for the user.

Note The **Export Users** button is enabled when you select one or more users.

To export users:

Procedure

Step 1 On the **User Provisioning** page, select the number of users that you want to export.

Step 2 Click **Export Users**. A tab-separated data text file is generated. This file contains details of the exported users. You can import the exported users using the **Import Users** button.

Managing User Passwords

You can change the password, reset to default, or prompt users to change their password after their initial login to the application. You must have the correct privileges to manage passwords.

You can update the following:

- Provisioning login password
- Cisco Unified Communications Manager password

  Note The Cisco Unified Communications Manager password cannot be modified when the Cisco Unified Communications Manager is configured to use external authentication. Cisco Prime Collaboration Provisioning indicates that the password is updated, although it is not.

- Cisco Unified Communications Manager PIN
- Cisco Unified Communications Manager Express password
- Cisco Unity Subscriber password
- Cisco Unity Connection PIN
- Cisco Unity Connection Web password

  When resetting the Cisco Unity Connection Web password, if the new password is not of required length, the following error occurs: `Unity Connection Password: Failed to reset credential: The credential minimum length check failed. Minimum length = 8`

- Unified CM MLPP Password

  This password can be changed using the Manage PIN/Password option only when you set the MLPP User Identification Number and MLPP Precedence Authorization Level for User Service (on the Service Provisioning page).

The Cisco Prime Collaboration Provisioning login password must be a combination of at least three of the following:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

You can either change or reset the password to the Provisioning system default, or prompt the user to change their password when they log in to the application next time. You can obtain the default values for the user passwords from your Provisioning administrator, Managed Service Provider, or corporate IT department.

The following rules control the default passwords:

- DefaultCUPMPassword
- DefaultCallManagerPassword
- DefaultCallManagerPIN
- DefaultCallManagerDigestCredentials
- DefaultUnitySubscriberPassword
- DefaultWebAccessPassword

For more information about rules, see Overview of Business Rules, on page 163.

Note After you reset the password of a user, you must inform the user of the default value that is required to change their password.

To change, reset password, or prompt users to change their password the next time they log in to the application:

Procedure

Step 1 Open the Manage User page for the desired user (see Adding Users, on page 199).

Step 2 Click **Manage Passwords**.

Step 3 On the Password Management page, you can select Password, PIN, or Digest Credentials to modify. Select the password to be changed from the drop-down list.

Step 4 Do one of the following:

- To change the password, specify a new password (and confirm), and then click Apply.
- To set the password to default, click **Reset Password**.
- To prompt users to change their password when they log in to the application the next time, click **Prompt User**.

Step 5 Click **Done** to confirm.

The following rules are applicable while creating a password:

- Password cannot be the same as, or reverse of, the username.
- Password cannot have a character repeated consecutively more than three times.
- Password cannot be:
  - Cisco or the reverse.
  - Cisc0 (with zero substituted for o).
  - C!sco (with exclamation mark substituted for i).
  - Ci$co (with dollar sign substituted for s).

    - Any variation of the previous that uses variations in case (uppercase or lowercase).

- Password must have lowercase, uppercase, special characters, and digits.
- The minimum number of characters required is eight (by default, but can be changed).
- The maximum number of characters allowed is 127 (default is 80 characters).

(For Cisco Prime Collaboration Release 11.6 and later) The following enhancements have been made to the existing password policy:

- The password must contain characters from three of the following four character sets: lowercase, uppercase, number, and special character. The number of character sets is configurable (Default is three).
- The minimum number of characters required is six (Default is eight, but can be changed).
- **Allows re-use of password after <number of> changes** (minimum is 0, maximum is 24, and default is 0). This setting enables the user to reuse an existing password after the specified number of password change instances. For example, If the value is set as 0, the user can reuse the same password immediately. If the value is set as 10, the user can reuse the current password after the next ten instances of password changes, that is, if the current password is xyxy, this password can be reused after the next ten password changes.
- **Password can only be changed after <number of> hours** (minimum is 0, maximum is 48, and default is 0). If the value is set as 0, the user can change the password immediately. If the value is set as 24, the user can change the password after 24 hours since change of the last password.
- **Password expires after <number of> days** (minimum is 0, maximum is 365, and default is 0). This setting notifies the user that the password is expiring in "x" number of days and the account is disabled if the password is not changed within the specified timeframe. For example, if the value is set as 0, the password never expires.
- **Show warning message <number of> days before expiration** (minimum is 0, maximum is 31, and default is 0). This setting indicates when the user is notified about password expiration. For example, if the value is set as 0, this setting is disabled, and no warning message is displayed about expiration of the password. If the value is set as 5, a warning message is displayed five days before the expiration of the password.
- **Prompt for confirmation <number of> days before expiration** (minimum is 0, maximum is 30, and default is 0). This setting indicates when the user has to be prompted about expiration and changing of the password. When prompted, the user has to either acknowledge the password expiry or proceed to change the password. For example, if the value is set as 0, this setting is disabled, and no confirmation prompt is displayed about expiration or change of the password. If the value is set as 3, the user is prompted to change the password three days before the expiration of the password.

Cisco Prime Collaboration Provisioning stores the password policy properties in a file named passwordpolicy.properties under opt/cupm/sep. You can modify the properties file to change the password policies as required. Restart Cisco Prime Collaboration Provisioning whenever you modify the password policies.

Although Cisco Unified Communications Manager Express allows a user to have only one associated endpoint, Cisco Prime Collaboration Provisioning overcomes this limitation, allowing more than one endpoint to be associated to the user.

In Cisco Unified Communications Manager Express, new users are created with the same username appended with a tilde (~) and sequence index (starting with 1) from the second and subsequent endpoints (for example,

TestUser and TestUser~1). Use the exact username to view the corresponding endpoint details in the Cisco Unified Communications Manager Express web interface.

When you change the password in Cisco Prime Collaboration Provisioning, the password is changed for all the corresponding user names in Cisco Unified Communications Manager Express.

Resetting User Password Using Forgot Password Link

For Cisco Prime Collaboration Release 11.6 and later

To reset your password using **Forgot password?** link in the login page:

Procedure

Step 1 Click **Forgot password?** link in the login page.

Step 2 Enter your **User ID** and click **Send Email**.

Password reset email will be sent your email account.

Note If you have set security questions for password recovery, then you will be prompted to answer password reset questions. Enter the answers and click **Submit**. Go to Step 4.

Step 3 Click the link in the password reset email to initiate the password reset request.
Change password page of Cisco Prime Collaboration Provisioning appears.

Step 4 Enter your new password and click **Change Password**.
You will be redirected to login page.

Recovering User Password

For Cisco Prime Collaboration Release 11.6 and later

When you log in, you are prompted to configure the password recovery. Click **Yes** to set the recovery email ID, otherwise click **No** to return to the Home page.

To configure the password recovery:

Procedure

Step 1 Choose **Administration** > **Settings** and click **Password** tab.

Step 2 Do one of the following:

- To recover the password using email, click **Send Email** radio button. Click **email server configuration** to configure the email notification settings. For more details, see Configuring System Notifications.
- To recover the password using security questions, click **Security Questions** radio button.

  In the next login, you are prompted to set up security questions and answers after enabling the password recovery using security questions.

Step 3 Click **Update**.

Synchronizing a User

The data of a user in Cisco Prime Collaboration Provisioning is synchronized with the user data in the Call Processor and Unity Connection. For more information about synchronizing, Overview of Domain Synchronization.

When synchronizing users, remember the following:

- The username and phone number fields may display Unknown for users who were initially created on Cisco Unified Communications Manager Express and then later synchronized to Cisco Prime Collaboration Provisioning.

  You can update the user information through Cisco Prime Collaboration Provisioning, but be aware that this information will be pushed to the Cisco Unified Communications Manager Express system, and will overwrite any existing information for the user in the ephone description field.

- If a Cisco Unified Communications Manager Express is the only device present in a Domain and Service Area, during Domain synchronization users are not created in Cisco Prime Collaboration Provisioning if the ephone username command is not configured in Cisco Unified Communications Manager Express.

  Ensure that the ephone username command is configured in Cisco Unified Communications Manager Express for all users.

- For Cisco Unified Communications Manager Express, when using the button command in ephone configuration mode, ensure that you only use a colon (:) as the separator. Cisco Prime Collaboration Provisioning only supports a colon as a separator in the button command. If any other separator is used, Cisco Prime Collaboration Provisioning does not display the line in the User Record Details page. Only the endpoint is displayed.

Procedure

Step 1 Choose **User Provisioning**.

Step 2 From the list of users, mouse over QuickView, and click **Synchronize User**.

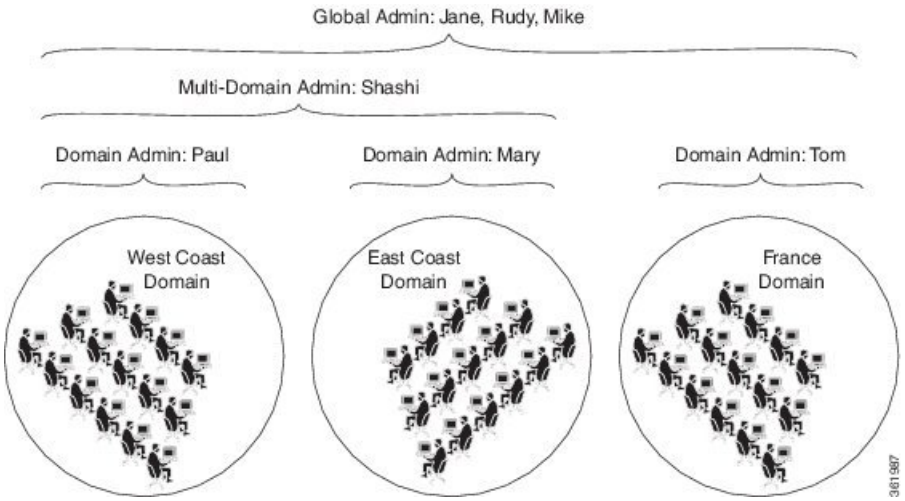
Note If the Domain contains a large number of users, the synchronization may take several minutes.

Overview of Authorization Roles

For Cisco Prime Collaboration Release 11.2 and earlier

Two types of Provisioning user roles are available: global and domain specific. Based on their roles, Provisioning users are authorized to perform various tasks in Provisioning. In the example below, the Domain administrators have administrative privileges for a specific domain. They can set polices and rules for the domain assigned to them. The multi-domain administrators have privileges for more than one domain. The global administrators have access to all Provisioning functionality.

Figure 5: Global and Domain Specific Roles in Provisioning



When you attach a Provisioning server with existing user data, then the globaladmin and domain-admin roles are synchronized automatically in the User Management page.

Note the following:

- Activity roles are available in Cisco Prime Collaboration Provisioning Advanced only. This menu is not available in Cisco Prime Collaboration Provisioning Standard.
- While creating an order for an endpoint in Cisco Prime Collaboration Provisioning Standard, MAC or dummy MAC address is mandatory.

Apart from global and domain administrator roles, a Provisioning user can also have ordering and activity roles. A provisioning user with an ordering role can place orders for users in a particular domain.

Table 49: Authorization Roles Description

Authorization Role	Description
Global Roles	
Administration	Has access to all Provisioning functionality.
Maintenance	Authorized to configure system cleanup activities. See Maintenance Mode.
Roles for Domain In the drop-down list, select the Domain for which you are setting the authorization roles. The selected roles only apply to the selected Domain. To apply the same authorization role to all available domains, select **Apply to all domains**. **Note** If the administrator selects Apply to all domains, existing roles of the user in all the domains will be overridden with the current selection.	
Policy	Authorized to modify user roles, and add or update endpoint inventory.

Authorization Role	Description
Infrastructure Configuration Management	Authorized to provision infrastructure configuration objects. When you select this role, you must also select a profile from the Permission Profile box.
Permission Profiles	Sets the permissions for which infrastructure configuration object users assigned this authorization role can configure. (For information on setting permissions, see Managing Infrastructure Configuration Permissions).
SelfCare User	Authorized to manage his own services; set up lines, manage services, and configure endpoint options quickly and easily. **Note** The SelfCareUser check box is available only if the CreateSelfCareAccounts rule is enabled for the domain.
Ordering Roles Users assigned these roles are allowed to place orders for other users and themselves.	
Ordering	Authorized to: • Add, delete, or update a user within a Domain. • Add, delete, or update a user role within a Domain (if the rule for that Domain permits it). • Add, delete, or update endpoints in the inventory within a Domain (if the rule for that Domain permits it). • Search and view detailed user information within a Domain. • Place an order for a user within a Domain.
Advanced Ordering	Authorized to access all the functionality specified by the Ordering role; can also access Advanced Order Options in the Order Entry page.
Advanced Assignment	Authorized to access all the functionality specified by the Ordering role, and to assign the MAC address for an endpoint at the time of order entry. Available in Cisco Prime Collaboration Provisioning Advanced only.
Activity Roles Users assigned one of these roles can perform activities assigned to the group during order processing.	

Authorization Role	Description
Approval	Authorized to accept and complete the approval for orders.
Assignment	Authorized to accept the user activity for assigning the MAC address.
Shipping	Authorized to accept and complete shipping of orders.
Receiving	Authorized to accept and complete receiving of orders.

Access Control Groups

For Cisco Prime Collaboration Release 11.5 and later

This feature (choose **Administration > Access Control**) enables you, as an administrator, to create access control groups for granting privileges to users to access specific pages and perform specific operations on them. You can assign and restrict system access to the user by providing granular access. You can grant access rights to the users through the Access Control Group, with which the user can access the features and functions based on the granular control. All authorization roles including ordering, shipping, and maintenance are converted to access control groups if you are upgrading to Cisco Prime Collaboration Provisioning 11.5 and later. In addition, the feature enables you to export and import access control groups in different systems having same versions of Cisco Prime Collaboration Provisioning. The following table lists the default access control groups:

For Cisco Prime Collaboration Release 12.1 and later

Read-Only Access for the following administrative UIs has been implemented.

- Logging and ShowTech
- Data Maintenance
- Backup Management
- Updates
- Schedule Synchronization
- License Management
- Single Sign-On
- Rules
- Settings

Table 50: Default Access Control Groups

Name	Description
View Only	Users who only view domains, service areas, service templates, and user roles
Administrators	System Administrator with full access

Name	Description
Help Desk	User can place an order without access to advanced setting

Before you perform operations on the Access Control Group, note the following:

- Cisco Prime Collaboration Provisioning Standard does not support the creation of a new access control group. However, you can modify existing groups and assign users to groups.
- You must upload an advanced license (with delegation feature enabled) to create a new access control group. In standard license, delegation feature is disabled by default.
- You can create up to 1000 groups only.
- “globaladmin” users have full access and are not assigned to any access control groups.
- A user can be assigned more than one Access Control Group.
- A user can be given access to a particular privilege with limited or full access.
- Some privileges have domain-based restrictions.
- Each domain can be controlled with different granular access as suitable.
- Administrator users cannot change or delete the group which they belong, but can change or delete other administrators group.
- Full access groups can be created only either globaladmin or users with full access privilege. The default administrator group can be edited and deleted too.
- For the users other than administrator and full access users, Access Control Group table lists the groups which are created with access items other than full access.
- Buttons and quick view in the respective pages and operations are displayed or hidden based on the granular control.
- Access Control link in quickview of user provisioning is displayed only if the logged in user is a member of Full Access group or having Access Control privilege (either **All** or **Assign users to groups** granular access).

When the users who have access to the **Access Control** page login, they:

- Can create access control groups.
- Can assign users to groups, when the user is assigned a group that has access to access control page with All granular access or Assign users to groups or add group, edit group, delete group, or if the user has full access.
- Cannot assign or edit or delete himself to any group.
- Cannot modify the full access privileged users or globaladmin.

Creating Access Control Group

The following example details the procedure to create an Access Control Group which enable the users to perform:

- Add/Edit/Delete/Import/Move users in User Provisioning page—The user who is assigned with Add/Edit/Delete/Import/Move access can view the relevant buttons.

  For Cisco Prime Collaboration Provisioning release 12.5 and later: The available options are Add/Edit/Delete/Import/Export/Move

- View the configuration information of devices—The user who is assigned with read-only access can only view the relevant information.

To assign the members with Write (Add/Edit/Delete/Import/Move) access to the selected domains for the User Provisioning page, perform the following steps:

1. Create a group with a unique name and add members to the group.
2. Under **Privileges** section, click **Add**.
3. From the **Name** drop down in the dialog box, select **User Provisioning**.
4. Select the domains from the **Accessible Domains** check box as suitable.
5. Select the **Access** check box and the relevant details as suitable.
6. Click **Save**.

For Cisco Prime Collaboration Provisioning release 12.5 and later: The available options are Add/Edit/Delete/Import/Export/Move

To view the configuration information of devices, perform the following steps:

1. Select the group you have already created.
2. Under **Privileges** section, click **Add**.
3. From the **Name** drop down in the dialog box, select **Device Setup**.
4. Select **Read-Only**from the **Access** check box.
5. Click **Save**.

Operations of Access Control Group

You can perform the following operations using access control groups (choose **Administration > Access Control**):

Operation	Description
Add	To add a new Access Control Group • Mandatory field: Group Name. Optional fields are: Description and Members. • Save button is disabled if you do not enter a Group Name and add a Privilege. • Valid values for the Group Name field are alphanumeric characters (A-Z, a-z, 0-9), space and the following special characters: _-./:;=?@^{}[]|`~ _. • A user can be assigned to more than one Access Control Group.
Edit	To modify an existing Access Control Group • Group Name is editable. • **Members** multi-select box does not display the user who has logged in. • In the selected users box, if the logged in user is part of the group, the user is displayed.
Delete	To remove an existing Access Control Group • After deleting a group, users assigned to that group no longer have access to the system.
Copy	Creating a new group by copying Privilege from an existing group • While copying Access Control Group, user is not copied. • Group Name is a mandatory field and is prefixed with "Copy of". • Save button is disabled if Group Name or Privilege is empty.
Export	To export the groups to a tsv file • Access Control Group details are exported to a tsv file. • You can export the users only if the user is assigned to full access groups or the group is created with granular control **All** or **Assign user to groups** for Access Control access item.

Operation	Description
Import	To import the exported groups into a different Cisco Prime Collaboration Provisioning Server • While importing, if the users(which are exported in tsv file) are not available in the new system, an access control group is created and displays the message about the users which are not present in the new system. • If the user is already available in the new system and a part of other access control group, the user is also a part of new group as well during import. • If at least one valid domain is there, an access control group is created with that domain.
Quick View	Hovering over **Quick View** displays the details of the group, including the members and the access list items.

Note Changes to your access control group(s) or privilege(s) invalidates your session and you are logged out. This happens if you perform the following operations:

- Adding a new group
- Editing an existing group(changes to members and privileges)
- Deleting an existing group
- Copy an existing group
- Importing the groups
- Updating group through the user provisioning (user quick view > Access Control).

Privileges with Granular Control

Privilege Name	Description	Granular Access	Domain Control
Full Access	Relates to users who have all the access permissions in Cisco Prime Collaboration Provisioning.	All	NA

Privilege Name	Description	Granular Access	Domain Control
Access Control	Enables you, as an administrator, to configure roles, access control groups, and access privileges for roles.	• All, Read-Only • Write > Add/Edit/Delete Groups • Write > Assign users to groups	NA
Device Setup	Enables you to add or edit or delete UC devices to Cisco Prime Collaboration Provisioning.	All, Read-Only	NA

User Provisioning	Enables you to add or edit or delete or import users, and provision services.	• All, Read-Only
		• Write >
		  • Add/Edit/Delete/ Import/Move
		  • Provision Services
		  • Provision Services with Advanced
		  • Provision Services with Assignment
		  • Password Management
			Yes

Provisioning Setup	Enables you to set up all your user provisioning tasks such as adding and configuring Domains, Service Areas, User Roles, and, Service Templates.	All, Read-Only	No
Infrastructure Configuration	Enables you to view, add, edit, or delete the configuration settings of a Call Processor and Unified Message Processor.	All, Read-Only	Yes
Provisioning History	Enables you to search and view the status of an order.	All, Read-Only	Yes
Dashboard	Enables you to manage the real-time information about the operational status of your processor, device, domain, and users.	All, Logged In Users, Locked Users	NA

Privilege Name	Description	Granular Access	Domain Control
Manage Endpoints	Enables you to upload new and existing endpoints through the user interface.	All	Yes
Manage Directory Numbers	Enables you to store and manage directory numbers that are associated with each Service Area in the Provisioning inventory.	All	NA
Inventory Search	Enables you to browse and search the Provisioning inventory.	All	NA
Unified Communication Services	Lists the Unified Communication services.	All	NA
Getting Started Wizard	Ability to run the Getting Started Wizard.	All	NA
Activities	Enables you to view all the order-related activities, including System Activities.	All	Yes
Reports	Enables you to view details on Service Area, Endpoint Inventory, DNB, Audit Trial, and so on.	All	NA
Audit Trail	Enables you to view details about the user login or logout, password, account, and timeout.	All	NA
License Management and Single Sign-On	Enables you to add or import or delete licenses, and enable SSO in Cisco Prime Collaboration Provisioning to cross-launch the UC applications.	All	NA
Rules and Settings	Supports predefined business rules and allows you to manage Analog Endpoints, Password Policy, self-care feature access, FIPS and custom settings.	All	NA

Privilege Name	Description	Granular Access	Domain Control
Logging and ShowTech	Enables you to view and download application log files.	All	NA
Maintenance and Backup	Enables you to put Cisco Prime Collaboration Provisioning into maintenance mode as well as backup your data, and restore it.	All	NA
Updates and Support	Enables you to view and add endpoint bundles, localization languages, and SSL certificates.	All	NA
Schedule Synchronization	Enables you to synchronize Call Processors, Message Processors, Presence Processors, Active Directories, and Domains.	All	NA

Authorization Roles After Upgrade

For Cisco Prime Collaboration Release 11.5 and later

The following table maps the existing authorization roles with the granular access that the users have after upgrading to Cisco Prime Collaboration 11.5 and later.

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Administration	Has access to all Provisioning functionality.	All Pages	All	All Pages	All
Maintenance	Authorized to configure system cleanup activities. See Maintenance Mode.	Dashboard	Pending Order Status	Dashboard	Welcome page
				Maintenance	All
		Data Maintenance	All	Backup Management	All
				Data Maintenance	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Policy	Authorized to modify user roles, and add or update endpoint inventory.	Manage Endpoints	All	Manage Endpoints	All
		Dashboard	Pending Order Status	Dashboard	Welcome page
		Provisioning Setup	Access only to user roles of assigned domains	Provisioning Setup	Access to domains, service areas, service templates, and user role of all the domains
Infrastructure Configuration Management	Authorized to provision infrastructure configuration objects. When you select this role, you must also select a profile from the Permission Profile box.	Dashboard	Pending Order Status	Dashboard	Welcome page
		Infrastructure Configuration	All	Infrastructure Configuration	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Ordering	Authorized to: • Add, delete, or update a user within a Domain. • Add, delete, or update a user role within a Domain (if the rule for that Domain permits it). • Add, delete, or update endpoints in the inventory within a Domain (if the rule for that Domain permits it). • Search and view detailed user information within a Domain. • Place an order for a user within a Domain.	Dashboard	• Pending Order Status • Device Sync Status • Deployment Details	Dashboard	Pending Order Status
		User Provisioning	• All buttons in User Provisioning • All actions in quick view without advanced and assignment provisioning	User Provisioning	• All buttons in User Provisioning • All actions in quick view with granular access without advanced and assignment provisioning
		Provisioning History	All	Provisioning History	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Advanced Ordering	Authorized to access all the functionality specified by the Ordering role; can also access Advanced Order Options in the Order Entry page.	Dashboard	• Pending Order Status • Device Sync Status • Deployment Details	Dashboard	Pending Order Status
		User Provisioning	• All buttons in User Provisioning • All actions in quick view with advanced ordering	User Provisioning	• All buttons in User Provisioning • All actions in quick view with advanced ordering
		Provisioning History	All	Provisioning History	All
Advanced Assignment	Authorized to access all the functionality specified by the Ordering role, and to assign the MAC address for an endpoint at the time of order entry. Available in Cisco Prime Collaboration Provisioning Advanced only.	Dashboard	• Pending Order Status • Device Sync Status • Deployment Details	Dashboard	Pending Order Status
		User Provisioning	All buttons and all actions in quick view with assignment	User Provisioning	All buttons in User Provisioning and all actions in quick view with assignment
		Provisioning History	All	Provisioning History	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Approval	Authorized to accept and complete the approval for orders.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains
Assignment	Authorized to accept the user activity for assigning the MAC address.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains
Shipping	Authorized to accept and complete shipping of orders.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains
Receiving	Authorized to accept and complete receiving of orders.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains

Configuring Privileges

For Cisco Prime Collaboration Release 11.5 and later

This section details steps to be followed to add or edit or delete the privileges.

Procedure

Step 1 Choose **Administration** > **Access Control** and enter or select the necessary details such as Group Name, Description, and Members.

In the Members drop-down, select the users as suitable.

Step 2 Click **Add** or **Edit** or **Delete** in the Privileges pane as suitable.

Step 3 Click **Selected** from **Accessible Domains** drop-down in the Privilege dialog box and choose the domains you want to access or click **All** to choose all the domains.

Note
- **Accessible Domains** drop-down is enabled only if you choose Provisioning Setup or User Provisioning in **Name** drop-down. For more information on domain control, see Privileges with Granular Control.
- If you select Infrastructure Setup access item, click **Selected** from **Accessible Infrastructure Objects** drop-down and choose the objects you want to access or click **All** to choose all the objects.

Step 4 Select **Access** as suitable.

Step 5 Click **Save**.

Granular Control Support for Access Control Items

The following tables describe the supported granular controls for access control items.

Table 51: Granular Control Support for Access Control Items

Access Control Item	Supported Granular Control	Description
Full Access	Not Applicable	Other than administrators and the users who are part of the full-access privileged group, **Full Access** access items are not listed in Name drop-down in the Add Access or Edit Access dialog box.

Access Control Item	Supported Granular Control	Description
Access Control	• All • Read-Only • Write > Assign Users to Groups • Write > Add/Edit/Delete Groups	Other than administrator and full access users, **Access Control** access items are not listed in Name drop-down in the Add Access or Edit Access dialog box. • With **Write > Add/Edit/Delete Groups** granular control, the user can perform all operations on Access Control page, but cannot assign users to any group. The user cannot assign groups to any user through the user provisioning quick view. While editing or copying a group, Assigned User list box is disabled or hidden. While exporting, users are not exported to the .tsv file. While importing, groups are created but users are not assigned to any group. • With **Assign Users to Groups** granular control, the user can edit the access control groups, but cannot update any items in the access list table. Apart from the Edit button, all other buttons are hidden in the Access Control Group table. In the user quick view, **Access Control** action is displayed through which the user can be assigned to any group. While editing the groups, user (other than administrator user) cannot edit or delete the **Access Control** access item for any of the groups. In addition, the Edit and Delete buttons are disabled in the Access List table.

Access Control Item	Supported Granular Control	Description
Device Setup	• All • Read-Only	• Enabled: **Dashboard**, **Device Setup** menu items, and Links for Device Name under **Device Sync Status**. • **All** and **Selected** radio buttons are disabled for the **Accessible Domains** field. • With **Read-Only** granular control, the user can view all devices in the list page of the device setup. Only **View the Detailed Log** action item is displayed in the device quick view. • The user can add, edit, delete devices, and change the services under UC Services.

Access Control Item	Supported Granular Control	Description
User Provisioning	All, Read-Only Write > • Add/Edit/Delete/Import/Move • Provision Services • Provision Services with Advanced • Provision Services with Assignment • Password Management	

Access Control Item	Supported Granular Control	Description

		• Only the **Dashboard**, and **User Provisioning** menu items are displayed. **Pending Orders** dashlet is displayed if the user has Provision Services granular control or All granular control.
		• **Accessible Domains** is a mandatory field while adding access list, with two radio buttons:
		  • **All**—All domains are accessible.
		  • **Selected**—To select specific domains.
		• With **All** granular control, all buttons are displayed in the User Provisioning table. The user can provision services through auto provisioning, quick service provisioning, add-on services, and legacy ordering flow. The User Provisioning table lists only those users which are associated with the selected domains for access items. The user can set advanced attributes while provisioning services.
		• With **Read-Only** granular control, User Provisioning table lists only those users which are associated with the selected domains in **Accessible Domains**. The user cannot provision services.
		• With **Write > Add/Edit/Delete/Import/Move** granular control, the user can add, edit, delete, import, and move users. While importing users, autoprovisioning does not happen. Only Move and Bulk Move Status buttons are displayed in the User Provisioning table. The user can navigate to the customer record page, but cannot provision services. The user can be moved with services to other domains. Only View action is visible in the service quick view.
		• With **Write > Provision Services** granular control, Provision Services

Access Control Item	Supported Granular Control	Description
		button is enabled in the User Provisioning table. Provision Services, Add User to Unified CM only, Unlock Voicemail actions are displayed in the quick view of User Provisioning. The Custom Services Wizard and Provision Services button are enabled in the customer record page and the user can provision services through quick provisioning and legacy ordering flow and add-on services. While provisioning services through Custom Service Wizard, Advanced Attribute pane is hidden. The user cannot assign the MAC address for the Endpoint service. The user can provision any services through quick service provisioning. • With **Write > Provision Services with Advanced** granular control, Provision Services button is enabled in the User Provisioning table. The Provision Services, Add User to Unified CM only, Unlock Voicemail actions are displayed in the quick view of User Provisioning. The Custom Services Wizard and Provision Services button are enabled in the customer record page. T the user can provision services through quick provisioning and legacy ordering flow and add-on services. While provisioning services through Custom Service Wizard, Advanced Attribute pane is available to perform advanced settings. The user cannot assign the MAC address for the Endpoint service.

Access Control Item	Supported Granular Control	Description
		• With **Write** > **Provision Services with Assignment** granular control, Provision Services button is enabled in the User Provisioning table. The Provision Services, Add User to Unified CM only, Unlock Voicemail actions are displayed in the quick view of User Provisioning. The Custom Services Wizard and Provision Services button are enabled in the customer record page. The user can provision services through quick provisioning and legacy ordering flow and add-on services. While provisioning services through Custom Service Wizard, Advanced Attribute pane is hidden. The user can assign the MAC address for the Endpoint service. • With **Password Management** granular control, only Manage Password/PIN action are displayed in the quick view of the user. All buttons in the User Provisioning table are hidden. User can navigate to the customer record page. All links for add-on services and all actions are hidden in the service quick view.

Access Control Item	Supported Granular Control	Description

Provisioning Setup	• All
	• Read-Only
		• Only the **Dashboard** and **Provisioning Setup** menu items are displayed. Only the **Deployment Details** dashlet is displayed in the dashboard.
		• Users can add Provisioning Setup access item multiple times in the access list with different domains and granular controls.
		• With **Read-Only** granular control, the user can view Domains, Service Areas, Service Templates, and User Roles in the list page of Domain, Service Area, Service Template, and User Role.
		• With **All** granular control, the user can add, edit, delete, and extract domains, service areas, service templates, and user roles.
		• You can select the domains and have write access to:
		  • Add/Edit/Delete/Export Domains
		  • Add/Edit/Delete/Copy Service Areas
		  • Add/Edit/Delete User Roles
		  • Add/Edit/Delete/Copy Service Templates
		  • With All Attributes
		  • Without Security Attributes

Access Control Item	Supported Granular Control	Description
Infrastructure Configuration	• All • Read-Only	• Only the **Dashboard** and **Infrastructure Setup** menu items are displayed. Under **Infrastructure Setup**, only the **Infrastructure Configuration** menu item is available. • Infrastructure Configuration Permission Profile is merged with Infrastructure Configuration and displayed in the Accessible Infrastructure Objects multiselect box. • With **Read-Only** granular control, the user can view all objects on the Infrastructure Configuration page. • With **All** granular control, the **Add New** button is enabled on the Schedule Configuration page. In addition, the add, edit, and copy buttons are enabled for the objects if a profile is attached, else the buttons are displayed for all the objects. If any permission profile is attached, the user can provision only those objects that are included in the profile.
Provisioning History	• All • Read-Only	• Only the **Dashboard** and **Activities** menu items are displayed. Under the **Activities** menu, only **Provisioning History** is available. • With **Read-Only** granular control, only Search and Clear buttons are enabled on the Provisioning History page. • With **All** granular control, all the buttons are enabled on the Provisioning History page and the user can perform all the operations.

Access Control Item	Supported Granular Control	Description
Dashboard	• Logged In Users • Locked Users • All	• Only the **Dashboard** menu is available with this access item. **Logged In Users** and **Locked User** dashlets are displayed along with other dashlets based on the selected granular control for this item. • **Prime Collaboration Provisioning Capacity** dashlet is displayed only for the administrator users. **Pending Order Status** dashlet is displayed if the group to which user belongs is created with User Provisioning with granular control. **Deployment Details** dashlet is displayed only if the user has access to Provisioning Setup. This dashlet lists only the domains that are selected in the **Accessible Domains** list box. **Device Sync Status** dashlet is displayed if the user has access to Device Setup. • With **Write** > **Logged In Users** and **Write** > **Locked Users** granular controls, the relevant dashlet is displayed in the dashboard along with other default dashlets. In addition, the users which are logged in to the system and the locked users are listed as suitable. • With **All** granular control, all the six dashlets are displayed in the dashboard and links for domain name, order, and device name are enabled only if the logged in user has access.

Table 52: Granular Control Support for Access Control Items (Continued)

Access Control Items	Supported Granular Control	Description
Manage Endpoints	• All	• Only **Dashboard** and **Manage Endpoints** under the **Advanced Provisioning** menu items are available. • All the buttons are enabled. The user can perform all the operations on the Manage Endpoints page. The user can assign endpoints to any users available in the system.
Manage Directory Numbers	• All	• Only **Dashboard** and **Manage Directory Numbers** are available under the **Advanced Provisioning** menu. • All the buttons are enabled. The user can perform all the operations on the Manage Directory Numbers page.
Inventory Search	• All	• Only **Dashboard** and **Inventory Search** are available under the **Advanced Provisioning** menu. • All the links for the Sample Reports are enabled. The user can create a new search and edit an existing search.
Unified Communication Services	• All	• Only **Dashboard** and **Unified Communication Services** are available under the **Advanced Provisioning** menu. • Apply button is visible and the user can perform all operations on this page.

Access Control Items	Supported Granular Control	Description
Getting Started Wizard	• All	• Only **Dashboard**, and **Getting Started Wizard** are available under the **Infrastructure Setup** menu. • The user can proceed to all the steps of GSW, and also has access to import LDAP users, and perform auto provisioning. • If only Getting Started Wizard access item is added in the access group and the user clicks **Getting Started Wizard** after logging in, the user is redirected to the dashboard. • If the access control group contains the access lists for both Getting Started Wizard and User Provisioning and the user clicks Getting Started Wizard, the user is redirected to the User Provisioning page.
Infrastructure Configuration Permissions	• All	• Only the **Dashboard**, and **Infrastructure Setup** menu items are available. Under Infrastructure Setup, only the **Infrastructure Configuration** menu is available. • The Add New button in Infrastructure Configuration Permission Profiles is visible for adding new profiles. The user can also update or delete the profiles.
Activities	• All	• Only the **Dashboard** and **Activities** menu items are available. • The user can perform all the operations.

Access Control Items	Supported Granular Control	Description
Reports	• All	• Only the **Dashboard**, and **Reports** menu items are available. • The users can generate reports for **Communication Manager Reporting**, **Service Area**, **Resource Configuration**, **Service Configuration**, **Endpoint Inventory**, **Directory Number Inventory**, **Directory Number Block**, and **Endpoint /Line Mismatch**.
Audit Trail	• All	• Only the **Dashboard**, and **Reports** menu items are available. **Audit Trail** submenu item is displayed under **Reports**. • The users can generate the Audit Trail report that contains events about every PIN or Password change, PIN or Password reset, PIN or Password change on next login, unlock voice mail of a user in a Unity or Unity Connection device, login management, user management, pin or password management, changes in access control group, user roles, self-care, system settings, and synchronization.
License Management and Single Sign-On	• All	• Only **Dashboard**, **License Management**, and **Single Sign-On** are available under the **Administrator**menu. **Audit Trail** submenu item is displayed under **Reports**. • The user can add and delete license, and have access to perform all operations on the Single Sign-On page.

Access Control Items	Supported Granular Control	Description
Rules and Settings	• All	• Only the **Dashboard**, and **Administrator** menu items are available. **Rules**, **Settings**, **System Notification Settings**, and **Domain Notification Settings** submenu items are visible under **Administrator**. • **Configure Rules in Domain** drop-down lists all the domains available in the system on the Configure Rule page. The user has access to perform all the operations on **Settings** page. The **Update** button is visible to the user. The **Test Settings** and **Save** buttons are visible on the **System Notification Settings** page. The user can perform the system configuration notification settings. The **Test Settings**, **Apply to domain template only** and **Apply to all domains**buttons are visible to the user. The user can access the notification configuration domain settings.
Maintenance and Backup	• All	• Only the **Device Setup**, and **Administrator** menu items are available. The **Data Maintenance**, **Maintenance Mode**, and **Backup Management** submenu items are visible under **Administrator**. • The user can update the configure data to be purged and **Update** button is visible on the Data Maintenance page. The user can perform all the operations. **Enter Maintenance Mode** button is visible on the **Maintenance Mode** page.

Access Control Items	Supported Granular Control	Description
Updates and Support	• All	• Only the **Dashboard**, and **Administrator** menu items are available. • The user can perform all the operations. All the buttons are visible in the **Logging and ShowTech**, **Updates**, and **Process Management** pages.
Schedule Synchronization	• All	• Only the **Dashboard**, and **Administrator** menu items are available. • All the buttons are visible and the user can schedule synchronization (**Administrator** > **Schedule Synchronization**).

Accessing User Records for a User

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click a specific user.

Step 3 Hover over the quick view icon next to the user in the user record page to view the user information and to perform the actions for the selected user.

In the Service Details pane, the quick view of a service displays an Add-on Service (if applicable) for quick provisioning. For example, if an existing service (called as Anchor service) is an endpoint, you can add Line service (called Add-on Service) by hovering over the quick view icon and clicking the plus symbol or the link beside the symbol. The following table lists the Add-on Service available for Anchor Service.

Anchor Service	Add-on Service
User Services	Enable Mobility, Enable SoftPhone, IM & Presence
Endpoint	Line
EM Access	EM Line
Line, EM Line, and Shared Line	Voicemail, SNR
RDP	RDP Line

Anchor Service	Add-on Service
RDP Line	Voicemail

Viewing or Logging out Active Sessions

You can view active sessions and log out single or multiple active sessions.

Procedure

Step 1 Choose **Home** > **Dashboard** > **Logged In Users**.

The Logged In Users page appears, showing the list of active sessions.

Step 2 To cancel single or multiple sessions, select the session that you want to end.

Step 3 Click **Log Out**.

The selected session and the user are logged out of the server.

Note The Logged In Users and Locked Users can be accessed only by the globaladmin.

Using Global Search

You can use the global search field to locate any of the following:

- User ID
- Name
- MAC Address
- Directory Number
- DN Description
- Phone Description
- VM Alias Name
- EM Name

To search using the global search field at the top of the view pane:

Procedure

Step 1 Go to the search field in the top right corner of the Home page.

Step 2 Select the required option form the Search drop-down list:

- User ID

- Name
- MAC Address
- Directory Number
- DN Description
- Phone Description
- VM Alias Name
- EM Name

Step 3 Enter valid information.

Step 4 Press **Enter** to begin the search. You will be taken to the corresponding User Provisioning page if an exact match exists. If more than one match occurs, the system displays all records that matches the search criteria. When you click on a result, you will be redirected to that specific User Provisioning page.

CHAPTER 11

Using Prime Collaboration Self-Care

Prime Collaboration Self-Care Overview

Prime Collaboration provides a Self-Care portal, which allows you to control preference settings such as user name, password, and so on. You can update your own account and services by using the Self-Care portal. The Self-Care feature enables you to modify line settings, manage services, add reset Voicemail Box, Voicemail PIN, and configure phone options. The Self-Care portal covers user services across multiple Cisco Unified CM clusters, Unity Connection clusters and IM&P clusters.

Note When Cisco Unified Communications Manager is shared between two or more users, and if one or more users are using LDAP, Prime Self-Care will be used regardless of the version of Cisco Unified Communications Manager.

To enable Prime Collaboration Self-Care, see Creating a Self-Care Account, on page 243.

Creating a Self-Care Account

You can create a Self-Care account in Cisco Prime Collaboration Provisioning. You can choose to enable or disable Self-Care for each user you create.

Note

- To assign Self-Care roles, you must enable the CreateSelfCareAccounts rule while creating a new domain. The CreateSelfCareAccounts rule is disabled by default.
- You can also assign Self-Care roles in an already existing domain by running the Self-Care Migration Utility. This will enable Self-Care role for already existing users. See Self-Care User Migration Script for details.
- The SelfCareUser check box is available only if the CreateSelfCareAccounts rule is enabled.
- After creating users, the users can login to Self-Care only after the globaladmin or domain-admin changes their account password. By default, the user password is empty. You must specify a default password in the DefaultCUPMPassword Data field and set Enabled to true to set the default password.
- If the users domain is authenticated with Active Directory, the self-care login will use the AD server defined for the users domain.

To create a Self-Care account for a user:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click **Add User** and check the **Enable Prime Collaboration Self-Care** check box.

Step 3 Enter the necessary user information and save.

Enabling or Disabling Self-Care Using Batch Provisioning

You can enable Self-Care while creating new users using Batch Provisioning. To enable Self-Care for a user, provide the authorization role as SelfCareUser in the batch action file.

Batch Provisioning can also be used to enable or disable Self-Care role for an existing user. To enable provide the authorization role as SelfCareUser, and to disable provide none in the batch action file.

Note The CreateSelfCareAccounts rule must be enabled for the domain to create a Self-Care account.

For information on Batch Provisioning see Managing Batch Projects, on page 151.

Launching Prime Collaboration Self-care

Based on your user role, you can launch Self-Care.

Note If you are using IE 10, you must select the Standards mode for the Self-Care portal to work properly.

Note **For Cisco Prime Collaboration Provisioning release 12.5 and later**

When you log in to the Self-care/Non-Selfcare User login page for the second time, it displays the successful date and time of the previous login.

A user with only Self-Care role will be directed to the self-care portal after login:

Procedure

Step 1 In a browser enter, http://<provisioning-ip>/cupm/selfcareuser/Login.

Step 2 Use Self-Care credentials to log in.

Since the user has only Self-Care role, he will be able to access only the Self-Care menu. Provisioning menus will not be available for such a user.

Customizing Your Personal Settings

Self-Care enables you to set individual attributes and personal preferences for the following aspects of phone use:

- Phone options include configuring speed dial numbers, do not disturb options, and music when a call is placed on hold.
- Profile options allow you to configure options for extension mobility and single number reach.
- Line options for a specific line on the phone, such as call forwarding, caller identification, and notifications.
- User options for the phone user, such as passwords and personal identification numbers (PINs).

You can update the /opt/cupm/sep/ipt.properties file to hide or display the features displayed in the Phone Settings, Line Settings, and User Settings page of Self-Care portal. For example, if you want to configure the features in the Phone settings, your entries would be:

In Cisco Prime Collaboration Provisioning UI, choose **Administration** > **Settings** to view the following Endpoint Features.

```
enabled features for Phone Settings should be provided as follows:
General,SpeedDials,DoNotDisturb,Locale,MusicOnHold,Others
dfc.ipt.selfcare.phone.features=General,SpeedDials,DoNotDisturb,Locale,MusicOnHold,Others#
```

Note You must log in as root user to update the ipt.properties file. You must restart the cupm services for the changes to take effect.

To configure Self-Care options:

Procedure

Step 1 In a browser, enter http://<provisioning-ip>/cupm/ipt/selfcare/home.html.

Step 2 Enter your username and password.

The Self-Care portal screen appears. The Self-Care portal screen contains the following elements:

- Phone carousel—The phone carousel (positioned in the lower left side of the screen) contains icons for the phones and service profiles that you can configure. Click the icons at either side of the visible icons to view the additional phones or profiles.
- Main menu—The main menu options (to the right of the phone carousel) are Phone Settings, Line Settings, and User Settings. Depending on your selection in the phone carousel, the Phone Settings option might be replaced by Extension Mobility Settings or Single Number Reach Settings.
- Configuration area—The configurable categories for the selected main menu option appear next. When you click a category, such as Speed Dials, the right side of the screen displays the configurable options.

Step 3 In the phone carousel, select the phone or profile you want to configure.

Step 4 In the Line Settings menu, ensure that you select the correct line for the options you are configuring.

The following options are available for you to configure in the Self-Care portal:

- Configuring Phone or Extension Mobility Settings
- Configuring Single Number Reach Settings
- Configuring Line Settings
- Configuring User Settings

Configuring Phone and Extension Mobility Setting

The following table lists the Phone and Extension Mobility settings you can perform using Self-Care.

Table 53: Configuring Phone and Extension Mobility Setting

Settings	Description	Procedure
General	Update your phone MAC address and unlock Voicemail Box.	Choose Phone Settings > MAC Address, enter a valid MAC address for your phone, then click Save.
Speed Dials	Add phone numbers for speed dialing. Add a comma between the numbers to pause speed dialing. You can add any number of commas. Default delay for a comma is two seconds.	Choose Phone Settings > Speed Dials , then click Add. Enter the necessary information and click Save.

Settings	Description	Procedure
Do Not Disturb	Enable or disable the Do Not Disturb feature. Select the action to be taken if an incoming call arrives while the Do No Disturb feature is enabled.	Choose Phone Settings > Do Not Disturb, then check the Enable Do Not Disturb check box.
Locale	Select your work and network locales for time and language support.	Choose Phone Settings > Locale, then choose your location from the User Locale drop-down list, and click Save.
Music On Hold	Select the source of the music to be played when you place a user on hold.	Choose Phone Settings > Music On Hold, then choose the audio source to play when you place a call on hold from the User Hold Audio Source drop-down list, and click Save.
Others	Enable or disable the following options: • Speakerphone • Speakerphone and headset • Video • PC Port use • Extension Mobility	Choose Phone Settings > Others, then check or uncheck the check box as required for each option, then click Save .

Line Settings

The following table lists the available line settings for each line of the selected phone or profile:

Table 54: Line Settings

Settings	Description	Procedure
Call Forward	Set default call-forwarding options. Customize call-forwarding for external or internal incoming calls.	Choose Line Settings then select Call Forward, Caller ID, Notification, or Music On Hold to update and click Save.
Caller ID	Configure caller ID options.	
Notification	Set audio and visual options for incoming calls and notification of messages.	
Music On Hold	Select the source of the music to be played when a call is placed on hold.	

User Settings

The following table lists the available User Settings:

Table 55: User Settings

Settings	Description	Procedure
Information	Update your name. Enter your email address.	Choose **User Settings**, then select **Information, Password, PIN,** or **Conference** to update and click **Save**.
Password	Update your password.	
PIN	Update your personal identification number.	
Conference	Update attendees access code. **Note** You can update attendees code, only if Conference Now service is enabled for the user.	

Common Self-Care Tasks

The following table lists all the common self-care tasks a user can perform:

Table 56: Common self-care Tasks

Task	Procedure
Change a password	Choose User Settings > Passwords.
Change a PIN	Choose User Settings > PIN. **Note** You can change your phone and voice mail PINs. Phone PIN is to reset the Cisco Unified Communications Manager (or Extension Mobility) PIN, and voice mail is to reset the Unity Connection PIN.
Disable use of a speakerphone	Choose Phone Settings > Others, then check the Disable Speakerphone check box.
Enable extension mobility	Choose Phone Settings > Others, then check the Cisco Extension Mobility check box.
Enable video calls	Choose Phone Settings > Others, then check the Enable Video check box.
Forward calls	Choose Line Settings > Call Forward, then set the options for forwarding incoming calls.

Task	Procedure
Provide e-mail information	Choose User Settings > Information, and enter your email address.
Select a different phone as your primary device.	Choose User Settings > Information, and choose the preferred device from the Primary Device drop-down list.
Select call and message notifications	Choose Line Settings > Notification, then choose the notification options for incoming calls and messages.
Select the source for music for calls on hold	Choose Phone Settings > Music On Hold, then choose the audio source to use when you or the network places a call on hold.

Configuring Single Number Reach

The Single Number Reach feature enables you to associate a another phone number with your business IP phone number. When a call is received on the business phone number, Cisco Prime Collaboration Provisioning automatically directs the call to ring on the phone you specify as well as the business phone. In this way, the Single Number Reach feature enables callers to reach you by dialing a single number, regardless of your location.

To configure an alternate number for Single Number Reach:

Procedure

Step 1 In the phone carousel, select the icon associated with the remote destination profile.

Step 2 Choose **Single Number Reach Settings** > **Alternate Numbers**.

Step 3 Provide the information as described in the Table 57: Field Description for Single Number Reach table, then click **Save.**

Step 4 If needed, click **Add New** to add an additional alternate number.

Table 57: Field Description for Single Number Reach

Field	Description
Alternate Number	Enter the alternate number that Cisco Prime Collaboration Provisioning is to direct calls to when calls are received on your primary phone.
Description	(Optional) Enter a description of the alternate number.
Enable Reach Me Anywhere	Check the check box to enable incoming calls to ring on multiple phones at the same time.
This is a mobile device	Check the check box if the alternate number is for a mobile device.

Field	Description
Allow me … seconds to answer	Enter the length of time (in tenths of seconds) that Cisco Prime Collaboration Provisioning should wait for you to answer the call on the primary phone before directing the call to the alternate number.
Continue ringing the alternate number for … seconds	Enter the length of time (in tenths of seconds) that Cisco Prime Collaboration Provisioning should ring at the alternate number.
If the alternate number answers within … seconds	Enter the length of time (in tenths of seconds) that Cisco Prime Collaboration Provisioning should wait after directing a call to the alternate device before connecting a call on the device. This delay prevents calls from being picked up by automated greetings, such as voice mail, on the device.
Line Association Information	Check the check box for the line to associate with this alternate number.

Self-Care User Migration Script

The SelfCareMigrationUtility can be invoked during the migration, or from the CLI, after migration. The tool processes all the users in the domains that have CreateSelfCareAccounts rule and DefaultCUPMPassword rule set.

This tool can be run through CLI from /opt/cupm/sep/ipt/bin. It can be run either globally (means for all domains) or for a single domain.

To run script:

Procedure

Step 1 Go to /opt/cupm/sep/ipt/bin.

Step 2 Run:`./SelfCareMigrationUtility.sh ALL ENABLE`

- ALL—Indicates all domains.
- ENABLE—Enables selfcare for all users in the domain specified.

  Tto disable selfcare option, run:

  ```
  ./SelfCareMigraionUtility.sh ALL DISABLE
  ```

  The script can be run at the domain level also. To do this, run:

  ./SelfCareMigrationUtility.sh *DOMAIN NAME* [ENABLE | DISABLE]

For more information on migration, see the Cisco Prime Collaboration Upgrade and Migration Guide.

CHAPTER 12

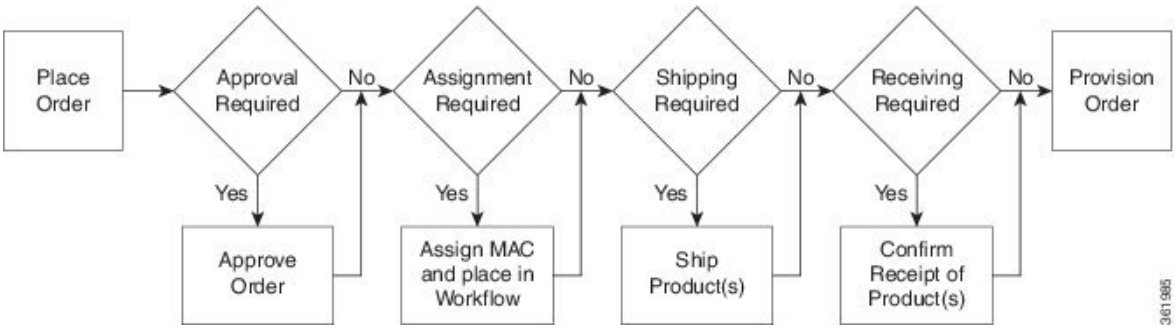
Managing Orders

Orders Overview

You can provision individual or bundled services. Users with Ordering authorization role (see Table 49: Authorization Roles Description, on page 211) can add, change, or cancel their own orders or those of other users.

Cisco Prime Collaboration Provisioning contains an automation engine which performs the order processing, including service activation and business flow based on how Cisco Prime Collaboration Provisioning is configured. The ordering process involves several workflow activities such as approval assignment, shipping and receiving (See Figure 6: Processing an Order, on page 252 for details. These individual workflow activities can be enabled or disabled, and assigned to different provisioning user roles per domain (see Table 49: Authorization Roles Description, on page 211 for Ordering Roles). If any of the activities are enabled, the order processing stops until the assigned provisioning user takes appropriate action. After the action is acknowledged, the processing continues and any disabled activity is automatically acknowledged by Cisco Prime Collaboration Provisioning.

Figure 6: Processing an Order



The length of time it takes to provision an order can vary. To verify if the order has successfully completed, go to the user record of the user (choose **User Provisioning**). Hover over **Orders** at the top right corner of the user record page to view the order details. The View Orders section shows the services with the status as Complete. Also, you can perform an order search for the order number.

Note After the system has been idle for a long period of time, the first order placed may take longer than usual.

While placing orders, remember the following:

- While ordering services on a Message Processor (Cisco Unity Connection, and Cisco Unity Express), not all the services are available. This is because the processors do not support all services. Supported Cisco Unity Services, on page 252 lists the orderable and nonorderable voice services for Cisco Unity processors.
- While ordering services on either Cisco Unified Communications Manager Express or Cisco Unity Express, be careful when entering Cisco IOS CLI commands (when configuring provisioning attributes through the Advanced Order Configuration pane). Your authorization role does not restrict what you can configure.
- Some attributes may not be supported by a particular endpoint type on a given protocol, so when placing endpoint orders, you should only set values for attributes that are supported by the chosen endpoint type and protocol. Else, you cannot provision services successfully.
- Cisco Prime Collaboration Provisioning synchronizes unsupported infrastructure objects like Intercom Calling Search Space and Intercom Route Partition from Cisco Unified Communications Manager. If these unsupported objects are used in provisioning services, it will result in error.
- If the Enable Voice Gateway feature property is set to N, the Order Entry screen will display analog endpoints. If the property is set to Y, then the analog endpoints are not shown in the screen.
- To order Analog endpoints, you must add Voice Gateway References to the service area in the Service Area Configuration screen.

Supported Cisco Unity Services

The following table lists the products and services supported by Cisco Unity.

Table 58: Supported Cisco Unity Products and Services

Message Processor	Services
Cisco Unity Connection	Orderable: • Voicemail • Enhanced Endpoint Service
Cisco Unity Express	Orderable: • Enhanced Endpoint Service • Voicemail

Ordering Service for a User

Creating orders for all the services follow the same basic procedure.

A user may not have access to all services. Cisco Prime Collaboration Provisioning implements a form of policy enforcement to allow users to get endpoints and services appropriate for the role assigned. The list of services that appear at order time depends on the following:

- User role that is assigned to the user, and the Domains and Service Areas available to the user.
- Availability of resources to support delivery within the Service Areas (for example, a Cisco Unity Connection system must be available to provide Unified Messaging).
- Provisioning system configuration.

  Service dependencies:

  - Line requires an existing endpoint.
  - Voicemail and Email require an existing Line.
  - Extension Mobility Line requires Extension Mobility Access.

To order a service for a user:

Procedure

Step 1 From the Cisco Prime Collaboration Provisioning navigation pane, choose **User Provisioning**.

Step 2 On the User Provisioning page, click a specific user.

Step 3 On the Service Details page, click **Custom Services Wizard**.

Step 4 Select a Service Area from the drop-down list. Rest your mouse pointer over the quick view icon for information on a Service Area in the drop-down list.

Step 5 Click **Continue**.

All available services which you can provision are displayed. Refer to Table 59: Provisioning Services, on page 255.

Step 6 Select the service that you want to provision and click **Continue**.

Note If endpoints are not displayed in the list for a user, you must associate the user role of a specific user to endpoints. If you are trying to add an endpoint and endpoints are not displayed, it is because the user role does not allow endpoints or endpoints cannot be provisioned for the user within that service area.

Step 7 On the Service Provisioning page, follow the Order Entry wizard, entering the required information for the service. For details of required fields, see Table 60: Order Entry Fields, on page 263.

When placing orders, note the following:

- The <Service Type> Information and Advanced Order Configuration panes provide specifications for the selected service.
- Users with Advanced Order or Administrator authorization role can access the Advanced Order Configuration pane. However, an order can be completed or an endpoint can be provisioned without using the Advanced Order configuration.

  Note To clear the value of a provisioning attribute that has a numeric value in the Cisco Unified Communications Manager, you must enter zero as the value. If you do not specify any value and leave the field blank, you cannot clear the value of the provisioning attribute.

- When selecting the service template, Base Line Information attributes with keywords are replaced with the user information automatically. You can also enter keywords while in the process of ordering a service.

  Note If the selected service template is mapped to a non-configured Service Area during User Provisioning, the Cisco Prime Collaboration Provisioning maps that Service Area to the selected Service Template.

  Select the **Show All Templates** checkbox to display all the service templates that are associated with the selected service and the product model irrespective of the Service Area and the User Role within the domain.

Step 8 Click **Continue** to create the order.

Step 9 Click **Confirm**, and then click **OK**. You can view the order number on the Service Details page. Verify the order status by reviewing the Provisioning History pane.

You can use the global search field at the top of the view pane to search User ID, Name, MAC address, Directory Number, DN Description, Phone Description, VM Alias Name, and EM Name.

- For User ID and Name search, alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), dots (.), at signs (@), space, and apostrophe are allowed (for example, AASJKUser006, AAS*, AA*, *SJKUser006, 3242#@!#########&@!*@(3), AANewRDUser00*).
- For MAC Address search, alphanumeric characters (A-Z, a-z, 0-9), dash (-), period (.), and underscore (_) are allowed (for example, 0024C444C3C6, 0024*, *24).
- For Directory Number search, alphanumeric characters, period, and underscore are not allowed. Special characters such as +, ?, (), and - are allowed in the directory number (for example, \+0000057, \+0000*, \+*, *0000*, *57).

- For DN Description, Phone Description, VM Alias Name, and EM Name search, all characters except non-printing characters such as tabs, quotes ("), close angle bracket (>), open angle bracket (<), ampersand (&), percent (%) are allowed.

Note
- When you search for phones using the MAC address in the global search option, use the format xxxxxxxxxxxx.
- A minimum of three characters in the search string is recommended to enable faster retrieval of search results.

To view the provisioning attributes for an ordered service, on the Service Details page, hover over the desired service, and then click View in the Actions list.

To add user notes to an ordered service, on the Service Details page, hover over quick view, and then click User Notes.

To create a template from an existing service, click **Create Template** from Quick View. Enter the necessary details and click **Create Template**. A template is created for the service with all its values.

If you are deploying many services, you may want to combine these activities into a single activity. The batch provisioning functionality of Cisco Prime Collaboration Provisioning enables you to create a single batch that contains multiple types of orders. You can also combine multiple types of services into a single batch operation.

To configure a batch project, choose **Advanced Provisioning > Batch Provisioning**.

Note While provisioning a service, if selecting the Security Profile Provisioning Attribute results in an error, uncheck the Protected Device option for the order to complete successfully. Ensure that the Cluster and Device Security Modes are configured appropriately for the Cisco Unified Communications Manager cluster. For information on the security parameters in Cisco Unified Communications Manager, see Cluster and Security Modes, in the Cisco Unified Communications Manager Security Guide.

Note The following services are not displayed for ordering until you associate the service to a user role.

Table 59: Provisioning Services

Service	Description

Enable Mobility Support	Enables Mobility for the selected user on the selected Call Processor. When ordering using default parameters, the following provisioning attributes are used: • Enable Mobility: True • Enable Mobile Voice Access: True • Max Desk Pickup Wait Time: 1000 ms • Remote Destination Limit: 4 This service is available only for Cisco Unified Communications Manager 10.x and later.
Enable Presence	Enables presence messaging updates by enabling the Presence Server license on a Call Processor for the user. This option is available only for Cisco Unified Communications Manager 10.x and later. You cannot see this service for ordering until you associate the service to a user role.
Enable Presence Client	Enables the use of Cisco Unified Personal Communicator by enabling the Unified Personal Communicator license on a Call Processor for the user. This is a bundle of Enable Presence Client and Client User Settings. Enable Presence Client is available only for Cisco Unified Communications Manager 10.x and later. This service is available only when you order Enable Presence. You cannot see this service for ordering until it is associated with the user role.
Enhanced Mobility Service	Includes an Extension Mobility device profile, line, and voicemail for the selected user on the selected Call Processor. This bundle enables you to create standard provisioning services such as Extension Mobility, line, and voicemail in a single order. You cannot see this service for ordering until it is associated with the user role.
Client User Settings	Enables Unified Personal Communicator User Settings on a Unified Presence Processor. Client User Settings can be ordered only through bundle services such as Enable Client Service or Presence Service. You cannot see this service for ordering until it is associated with the user role.

Enable SoftPhone Support	• Enables use of a personal computer along with a physical endpoint (both ring at the same time), or a CTI port (a virtual phone defined on Cisco Unified Communications Manager). • Not supported on Cisco Unified Communications Manager Express, or when ordering from a Call Processor based on Cisco Unified Communications Manager Express. • Does not appear in the service list if all available Call Processors already support SoftPhone. A list of valid Service Areas appears for specific Call Processors that are available to you. Though you enable this service based on the Service Area, you can do so only once per Unified CM, even if more Service Areas are associated with it. • When ordering, specify the server name or IP address of the user's computer in the Associated PC field. • Applies only to a Cisco SoftPhone that uses a CTI port. Cisco IP Communicator does not use CTI ports to communicate with Cisco Unified Communications Manager, but acts as a physical endpoint with a MAC address. To order Cisco IP Communicator, you must order a physical endpoint and select Cisco IP Communicator as the endpoint type. • Required for Cisco Jabber to control the desk phone.
Enhanced Endpoint Service	Includes an endpoint, line, and voicemail. The line is automatically associated with the endpoint that you ordered, and the voicemail is automatically associated with the line. When placing an order for Enhanced Endpoint Service on a Cisco Unified Communications Manager Express, you must enter the call-forward provisioning attributes. When entering an order, click Advanced Order Configuration and in the Voicemail Configuration Template provisioning attribute, enter the following commands: `call-forward busy <voice mail port/dn>` `call-forward noan <voice mail port/dn> timeout <seconds>` For a Cisco Unity Express Service Area, enter only alphabetical characters in the Voice Mail Display Name field. If you use other types of characters, orders for the user fail. For Cisco Unity Express Service Area, you cannot add, modify, or cancel orders when the infrastructure or user synchronization is in progress.

Extension Mobility Access or Access with Line	Enables users to log into a specific endpoint type and have their endpoint device profile applied to it. This service is available either by itself, or bundled with a line. Extension Mobility is available for ordering only if the optional Extension Mobility details are entered for a Call Processor when it is added to Cisco Prime Collaboration Provisioning. While ordering Extension Mobility Access for iPhones, order may fail if you use the default values for the following attributes: • DND Option • DND Incoming Call Alert (Set-only Attribute) • MLPP Indication For ordering Extension Mobility Access for iPhones, we recommend that you create a service template with the following values for these attributes and apply the template while creating an order: • DND Option—Call Reject • DND Incoming Call Alert—Disable • MLPP Indication—Off
Extension Mobility Line	The directory number or the line ordered for a device profile on a Cisco Unified Communications Manager. It can be ordered as an upgrade when the user already has Extension Mobility Access.
Cisco Jabber Service	Allows you to order Jabber service. Cisco Jabber service is orderable for Cisco Jabber for Tablet, Cisco Jabber for Desktop, Cisco Jabber for Android, Cisco Jabber for BlackBerry, and Cisco Jabber for iPhone. You must have a user role to view the Cisco Jabber Service in the order page. If you are upgrading from Prime Collaboration 9.0 to Prime Collaboration 9.5 and later versions, you cannot see this service for ordering until you associate the service to a user role. **Note** Check the **Provision Line for Selected Services** check box to provision a shared line for the selected Cisco Jabber Services.

Line	Line service can be provisioned for a user with or without an endpoint. No shipping, assignment, receipt, or tracking (for returns) steps are required for provisioning a new Line service. The Upgrade designation next to the Line service indicates that a line is being ordered for an existing endpoint. For Call Processors, the display for a line cannot exceed 30 characters. Ensure that the combination of characters for First Name and Last Name does not exceed 30 characters. If this limit is exceeded, when you place an order, the Call Processor sends an error. Using service templates, you can create keyword-based automatic settings, with automatic truncation, that prevents the character count from exceeding 30 characters. End User Association is automatically provisioned for Line services.
Line on a Shared Endpoint	Order a line on a shared endpoint when users require their own separate lines on the same physical endpoint. When this service is provisioned, the endpoint and all lines on it are displayed in each of the user record. The Shared icon appears next to the endpoint that is shared in the user record.

Endpoint	Order an endpoint that does not have a line or a directory number associated with it. Must not be associated with a line or a directory number.
	
	Extension Mobility functionality extends to most Cisco Unified IP Phones. Check the Cisco Unified IP Phone documentation to verify that Cisco Extension Mobility is supported. See the following URLs:
	
	• http://www.cisco.com/en/US/partner/products/ps10326/products_user_guide_list.html
	• http://www.cisco.com/en/US/partner/products/hw/phones/ps379/products_user_guide_list.html
	• http://www.cisco.com/en/US/partner/products/ps10451/products_user_guide_list.html
	• http://www.cisco.com/en/US/partner/products/ps10453/products_user_guide_list.html
	
	Guidelines for endpoint names:
	
	• Unified Personal Communicator:
	  • Must match the username. UPC is automatically added to the endpoint name after the order is provisioned.
	  • Must contain uppercase letters (A-Z) or numbers (0-9). Other characters are ignored.
	  • May contain 12 additional characters after UPC.
	  For example, if the username is john_jackson, enter JOHNJACKSON.
	
	• Cisco Jabber for iPhone:
	  • Must contain the prefix TCT. If you do not enter it, Cisco Prime Collaboration Provisioning automatically adds it.
	  • Must contain no more than 15 characters, including the prefix.
	  • Must consist only of alphanumeric characters (A-Z, a-z, 0-9). Cisco Prime Collaboration Provisioning converts lowercase letters to uppercase before pushing the information to the endpoint.
	
	• CTI port-Must contain 1-15 characters: alphanumeric (A-Z, a-z, 0-9), underscore (_), hyphen (-), or period (.).
	• IP Communicator-Must contain 1-15 characters: alphanumeric (A-Z, a-z, 0-9), underscore (_), hyphen (-), or period (.).
	
	Client Services Framework-Must contain 1-15 alphanumeric characters (A-Z, a-z, 0-9).
	
	Note Endpoint attributes are displayed based on the supported features for the selected endpoint type.

Endpoint Service	Adds a new endpoint and a line. While ordering Endpoint service, the maximum number of lines depends on the phone button template for the phone type (if a phone button template is available). For Cisco Unified Communications Manager Express, because no phone button templates are available, the maximum number of lines is defined in the product catalog for each endpoint type. When placing endpoint service orders for Cisco Unified Communications Manager Express, note the following: Cisco Prime Collaboration Provisioning always provisions the ephone-dn with a dual-line. • Cisco Prime Collaboration Provisioning always provisions the ephone-dn with a dual-line. • During user synchronization, Cisco Prime Collaboration Provisioning synchronizes all the ephone-dns with single-line, dual-line, and octo-line. • The endpoint must not have orphan ephone-dns (those that are not used by, or associated to, an ephone). **Note** Endpoint attributes are displayed based on the supported features for the selected endpoint type.
Remote Destination Profile	Order Remote Destination Profile for users, configure their attributes, and allow selection or configuration of a Remote Destination Profile Line, which supports Single Number Reach (SNR). Remote Destination Profile does not support Change Owner and Replace operations. You cannot see this service for ordering until you associate the service to a user role.
Remote Destination Profile Line	Order unlimited Remote Destination Profile Lines in a single Remote Destination Profile. Remote Destination Profile Line supports Autoassign or Chosen types of Lines. Remote Destination Profile Line can be shared among users and the same destination can be shared between Remote Destination Profile, Line, and Enable Mobility Access Line. In this scenario, all types of lines are displayed as shared lines. In Remote Destination Profile, you can order Voice Mail or Extension Mobility as they are ordered in the Line services. You can order Remote Destination Profile with any user role but not as a pseudo user. You cannot see this service for ordering until you associate the service to a user role.

Remote Destination Profile Service	Enable the Remote Destination Profile service for all Service Areas to share this Call Processor and also add a Remote Destination Profile Line. You can order Remote Destination Profile with any user role but not as a pseudo user. You cannot see this service for ordering until you associate the service to a user role.
Single Number Reach Service	Configure an Enable Mobility, Remote Destination Profile, and Remote Destination Profile Line. For mobility to work on a desk phone, you must do the following: • Configure the Line on the phone and Remote Destination Profile to be shared. • Configure the User ID that is used for the Remote Destination as an Owner. • Create a softkey template in Cisco Unified Communications Manager and assign it to a desk phone. Cisco Prime Collaboration Provisioning does not support softkey customization. Create a customized template in Cisco Unified Communications Manager. You cannot see this service for ordering until you associate the service to a user role. **Note** If you have ordered Enable Mobility Support service for a user, you cannot order Single Number Reach service for that user. Single Number Reach service option is not be displayed for that user on the User Provisioning page.
User Services	Enables presence messaging by enabling the user presence service settings on a Call Processor. To configure User Services, do the following: **1.** Add the Presence Server to Provisioning and perform the Infrastructure synchronization. **2.** Add the Presence Server to the Service Area that is used for ordering. **Note** User Services is available for Cisco Unified Communications Manager 10.x and above versions. **Note** User Services is available as an orderable service and it is also added by default when you create an order for a service.

Voicemail (individually)	Create orders for additional Voicemail services if the user already has a line. The Upgrade designation next to the voicemail service indicates that the Line service is being upgraded to include voicemail. When placing an order for voicemail on a Cisco Unified Communications Manager Express, you must enter the call-forward provisioning attributes. When entering an order, click Advanced Order Configuration and in the Voicemail Configuration Template provisioning attribute, enter the following commands: `call-forward busy <voice mail port/dn>call-forward noan <voice mail port/dn> timeout <seconds>`

Table 60: Order Entry Fields

GUI Element	Description
Associated PC	The name (DNS resolvable) or IP address of the computer to be used with the SoftPhone support.
Email ID	Enter the email ID. It cannot contain spaces.
Display Name (Email)	Enter the name to be used in the From field of the email.
Enable Extension Mobility	You must enable this check box through **Advanced Order Configuration** > **Extension Information** when you want to retain the EM Services that are added under subscribed services. Otherwise, EM Services are not provisioned to the endpoint and the same configuration is updated in Cisco Unified CM. You can add or edit subscribed services (EM Service or Subscribed services) through **Advanced Order Configuration** > **Subscribe/Unsubscribe services and assign SURL**, while provisioning endpoint services.
Extension Mobility Line	Select one of the following: Auto-assigned-System automatically assigns a directory number. Chosen Line-User specifies a directory number. The directory number cannot include dashes or spaces.
Line Type	Select one of the following: • Auto-assigned-System automatically assigns a directory number. Auto-assigned numbers come from the service area you selected at the beginning of the order process. • Chosen Line-You specify a directory number. The directory number cannot include dashes or spaces. An administrator can choose a specific unused number or a number that the user already has, for a shared line. In the Advanced Order Configuration option, you can then configure the provisioning attributes for the line. You can copy the provisioning attributes of a configured line on the same endpoint by selecting the line from the Copy Line field and clicking **Done**.

Directory Number	You can either enter a directory number directly into the field, or you can choose a directory number by clicking **Select a Number**. In the **Choose Number** window, you can either: **1.** Select a directory number that are already associated from the **Select an Existing Directory Number** pane. This pane displays: • Reserved directory numbers that are associated to a user. • Directory numbers that are associated to the user line service. Or **2.** In the **Search for an Available Directory Number** drop-down, choose your search criteria from the following: • Individual Numbers (not assigned to any block) — Enter a specific number to search for. • DN Blocks — The directory number blocks that are configured for a single service area on which the order is being placed are displayed. Choose a number to enter into the **Directory Number** field.
Line Position	During the order process, a page appears that lists the available line positions on the endpoint. Next to the line position, it indicates whether the line position is available. In the line position page, you can do the following: • Configure the line type - Click **Not Assigned** next to the line, and on the next page, configure the line type. After the line is configured, you must click the save icon on the right side of the page, to save your settings. • Change line position-Click the up or down arrow beside the line position. • If you want to configure more than one line, after configuring the first, backup and configure the next. Line position is not supported on Cisco Unified Communications Manager Express or Extension Mobility Access Lines.
Selected Endpoint	Select an endpoint from the list.
MAC Address	(Optional) In Cisco Prime Collaboration Provisioning Standard, it is mandatory to enter MAC or dummy MAC address. In case of Analog endpoints, MAC address is automatically generated based on the selected voice port.
Endpoint Type	Select an endpoint type from the list.
Protocol	Select the protocol. Endpoints may support both SCCP and SIP, or any one. Provision with the default protocol set in the Provisioning Attribute. If you do not select a protocol, the default setting is chosen. If you apply a service template with the setting, the template settings are used.
Target Endpoint	Select a target endpoint from the list.

Service Template	List of available Service Templates.
Analog Voice Gateway Reference	Select an analog voice gateway reference. Before executing the user synchronization, execute the infrastructure synchronization. During user synchronization, if the synced back analog endpoint is associated to a voice gateway reference that does not exist in IM, the voice port instance creation and its association is skipped. As a result, the analog endpoint is not manageable through Cisco Prime Collaboration Provisioning. Synchronization of analog endpoints and IM instance creation is done only for the Call Processor versions 10.xand above. The Analog Voice Gateway Reference field is enhanced to include the description of the gateway along with the alphanumeric reference number. While configuring the Voice Gateway infrastructure service, if the gateway description is provided, the description appears in the Analog Voice Gateway Reference field.
Name	Name of the Remote Destination Profile.
Description	Description of the Remote Destination Profile.
Selected Remote Destination Profile	Name of the selected Remote Destination Profile.
Service Area	List of available Service Areas. If a Service Area has a Unity Connection that is configured as a Unified Messaging Processor, and the Unity Connection does not have an external email server, Provisioning does not list the Service Area as an option when ordering Email.
Use Dummy MAC Address	Used for Tool for Auto-Registered Phones Support (TAPS) phones. If you check this check box, Provisioning creates a phone with a dummy MAC address, which is unique in the system. After a TAPS phone is provisioned on the Cisco Unified Communications Manager and updated with a real MAC address, you must run a user and Domain synchronization in Provisioning. This updates the dummy MAC address in Provisioning with the real MAC address. After a dummy endpoint is ordered, change and cancel orders do not require a user or Domain synchronization.
Voicemail Alias	Enter an alias for the voicemail. Alias identifies the voicemail in Cisco Unity Connection. The alias can be same as the user ID for whom voicemail is ordered.
Voicemail Display Name	Enter a display name for the voicemail.
Voiceport	Based on the Analog Voice Gateway Reference field, the relevant Voiceport is populated. You can view the list of occupied and available ports. Only the available port is selected for ordering.

Advanced Order Configuration	Lists the available provisioning attributes for the ordered service. This allows you to set provisioning attributes when placing an order . Click the plus sign (+) next to the Advanced Order Configuration option to expand this pane. To unset the value of a provisioning attribute that has a numeric value in Cisco Unified Communications Manager, you must enter a zero for the value. If you only clear the value, the provisioning attribute is not unset in Cisco Unified Communications Manager. Advanced Order Configuration is available only to users who are assigned the Advanced Ordering authorization role.
Choose a reserved endpoint	Opens a search page that lists reserved endpoints. A reserved endpoint is booked for a specific user. **Note** Enter MAC Address or Dummy MAC Address of the endpoint while provisioning.

Copy endpoint	Opens a search page that lists all the endpoints in the system that are supported by the user role. Copy endpoint allows you to provision a new endpoint with the same settings of an existing endpoint. To copy settings, on the search page, select an endpoint and click **OK** to confirm. This feature is available only to users with the Advanced Ordering role. When you have Global access, you can copy all the endpoints that are orderable for the user, including managed and unmanaged endpoints, as long as the endpoint belongs to the same Call Processor. When you have Domain access, you can only copy managed endpoints that are orderable for the user and are in the user's manageable Domains, as long as the endpoint belongs to the same Call Processor. Because some settings are unique to each endpoint, not all settings are copied to the new endpoint. The following settings are not copied to the new endpoint: • Directory Number • MAC Address • Endpoint Description When an endpoint is copied, services are not copied to the new endpoint. For example, if lines, voicemails, or emails exist on the endpoint, they are not copied to the new endpoint. In addition to this, the set only attributes associated with the endpoint are not copied. Through Copy endpoint, you can only copy the provisioning attributes that are set while creating an order. If the Cisco Unified Communications Manager version for the copied endpoint does not support an attribute, or if the copied endpoint type does not support an attribute, the attribute is cleared on the new endpoint. You are allowed to copy only an analog phone to another analog phone. Copying an IP phone to analog phone is not allowed. When an endpoint is copied, the provisioning attributes that are set during the add order are only copied. Once the Order is completed, in Cisco Unified Communications Manager, the Overriding Common settings check box is enabled. It means that the default attributes of the new endpoint have been modified.

Orderable Cisco Jabber Services	You can order Cisco Jabber services only if you have enabled Jabber on a Cisco Unified Communications Manager. To enable Jabber for a Cisco Unified Communications Manager, choose **Device Setup**. Hover over Quick View of the device and click **UC Services** tab. Select a Jabber service from the list: • Cisco Jabber for Tablet • Cisco Jabber for iPhone • Cisco Jabber for Desktop • Cisco Jabber for Blackberry • Cisco Jabber for Android

Related Topics

Creating Service Templates, on page 79
Provisioning Attribute Description in Batch Help, on page 335
Searching for an Order, on page 296
Batch Provisioning, on page 127

Line to End-user Association for Call Processors

Line to end-user association is automatically created in the Call Processors when ordering any of the following Line services for Provisioning:

- Line
- Line on a Shared Endpoint
- Extension Mobility Line
- Remote Destination Profile Line

Association will be created based on the following rules:

- For Add order of any Line service, end-user association is automatically provisioned in the Call Processor for all the Line services.
- For Change order on any Line service, association is created as follows:
  - If user association does not exist, association is provisioned between ordering User ID and Line services.
  - If user association exists and if ordering User ID is already associated, association is preserved.
  - If user association exists and if it is not ordering User ID, a new association is provisioned for the ordering user along with already existing users.
- For Cancel orders of any Line services, as the service itself is deprovisioned, end-user associations are also removed from Cisco Unified Communications Manager.

- While you modify or replace endpoint orders, you should provide supported values based on the endpoint type. If valid values are not provided, the order will move to an unrecoverable state. For example, Iphone and Nokia has specific set of supported values.
- For Replace orders of endpoint, user association is preserved from the old endpoint.
- For Change Owner cases (applicable only for IP Phone):
  - Users associated with lines of previous owner should be replaced with new owner association.
  - When changing owner of a endpoint from a registered user to a pseudo user, association is de-provisioned.
  - When changing owner from a pseudo user to a normal user, association is added.

If a line is not provisioned through Cisco Prime Collaboration Provisioning, the user association for the line may not get created in Cisco Unified Communications Manager after it is synchronized to Provisioning.

If this occurs you should run the Line to End-user Association utility. If you do not run the utility, the presence status for any lines other than the primary extensions will not be reported and the Single Number Reach Service will not work correctly.

For information on running the Line to End-user Association utility, see http://www.cisco.com/en/US/products/ps12363/prod_installation_guides_list.html.

During user synchronization, Cisco Prime Collaboration Provisioning synchronizes all user associations of Line objects from the Call Processor.

- Only Cisco Unified Communications Managers versions greater than 6.0.x are provisioned with this association.
- This association is not applicable for pseudo users .

Note You cannot unset a particular user from a list of associated users. To work around this limitation, remove the user association manually from the Cisco Unified Communications Manager and synchronize Cisco Unified Communications Manager with Cisco Prime Collaboration Provisioning.

Ordering Shared Endpoints and Lines

You can configure both shared endpoints and lines within Cisco Prime Collaboration Provisioning. The following scenarios are possible:

- Common shared line—Multiple users share the same line from different endpoints.
- Primary shared line—Multiple users share the same line from different endpoints, but one user's line display is used for all users (for example, a help desk). Users can also have their own lines separate from the shared line.
- Shared endpoint—Multiple users share the same endpoint, but have separate lines from that endpoint.

When ordering shared lines and endpoints, remember the following:

- If the second user orders a line on a shared endpoint that already has a line with voicemail, email, and unified messaging, he will not see these products for the first line in his user record. This also occurs when a shared line is ordered.
- If the second user deletes a shared endpoint, it is still displayed in the user record for the first user, and it is still present in Cisco Unified Communications Manager. But if the second user deletes any lines on the shared endpoint, those lines are deleted from the user record for the first user and from Cisco Unified Communications Manager.
- If the second user deletes a shared line, it is deleted from the second user's endpoint on Cisco Unified Communications Manager. But it is still displayed in the user record for the first user, and is still present in the first user's endpoint on Cisco Unified Communications Manager.
- The first user should not order a new voicemail for the second user's line (which displays a voicemail in its own user record). This second voicemail will fail on Cisco Unity because a voicemail already exists with the same directory number.
- Any changes made to the directory number provisioning attributes that are set on a shared line are also applied to all the lines that share the same directory number. The directory number attributes for the existing line are applied to the new shared line.
- By default, the DN block assignment algorithm will not take into account the Partition and will try to assign unique DN patterns from the block. To avoid assigning an existing DN that is in a different partition, add the following property:

```
dfc.ipt.servicearea.dnblock.uniquedn: Y
```

Note To modify the property, you need root CLI access. For CLI access, contact Cisco TAC.

- If the first user deletes a shared line or a endpoint, the associates of the shared line or a endpoint will move to the second user.

Setting Up a Common Shared Line

You can configure a scenario where multiple users share the same directory number by using lines on their own endpoints:

- Each user’s name is displayed on the shared line on their own endpoint.
- Caller ID displays the user’s name when they call other people.
- Each user’s own endpoint and the shared line are displayed in their own user record.

To set up a Common Shared Line:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Check the check box next to the user that you want to provision the services.

Step 3 Click **Provision Services**.

Step 4 In the Service Details page, click **Custom Services Wizard**.

Step 5 Select a **Service Area** and click **Continue**.

Step 6 Select **Line on a Shared Endpoint** and click **Continue** to start the order process.

Step 7 Do the following:

- Select **Chosen Line for the line on a shared endpoint type**.
- Select the Line Position for the line.
- Specify the Target endpoint.
- Specify the directory number for the shared line.

Step 8 Expand the Advanced Order Configuration pane.

Step 9 In the Directory Number Information pane, select the **Route Partition** for the directory.

Step 10 Enter the required information in the other panes available under Advanced Configuration, and click **Confirm**.

Step 11 Repeat these steps for each of the remaining users.

Setting Up Primary Shared Lines

You can configure a scenario where multiple users share the same line from their own endpoints, but the primary user's line display takes precedence over the others:

- One primary user, and one or more secondary users, can all share the same line.
- The primary user's line display appears on the shared line on all the user's endpoints.
- When a secondary user makes calls using the shared line, the caller ID displays the primary user's line display.
- User records for secondary users display the shared line as well as their own individual lines.
- User records for the primary user display all three shared endpoints and all three lines as well as the lines of the individual users.

Example Procedure for Setting Up a Primary Shared Line

In this scenario, the Help Desk is the primary user that shares a line with secondary users 1 and 2.

User	Line Display	Destination Number
Primary User	Help Desk	123
User 1	User 1	321
User 2	User 2	345

Note For all endpoints, ensure that you choose an endpoint model that has capacity for the shared line.

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click User 1, and then click **Custom Services Wizard**.

Step 3 Select a **Service Area** and then click **Continue**.

Step 4 Select **Endpoint Service** and click **Continue**

Step 5 Click **Not Assigned link** to assign the line type.

Step 6 Specify the directory number as 321. You can create orders for endpoints and services. You can create orders for individual services, or you can order bundled services.

Step 7 Repeat Step 1 through Step 6 for User 2, but specify the directory number as 345.

Step 8 Repeat Step 1 through Step 6 for Primary User (Help Desk), but specify the destination number as 123.

Step 9 Repeat Step 1.

Step 10 Click **Primary User**.

Step 11 Select a new Line on Shared Endpoint, making sure to do the following:

- Select **Chosen Line**.
- Specify 123 for the directory number.
- Select the MAC address for User 1's endpoint.

Step 12 Select the MAC address for User 2's endpoint.

Repeat Step Step 10, making sure to do the following:

Select **Chosen Line**.

Specify 123 for the directory number.

Step 13 Click **Confirm**.

You can configure a scenario where two or more users share the same endpoint, but have their own lines and line display information:

- Each user's line display shows up on their line on the shared endpoint.
- Caller ID displays the appropriate user's line display when they call other people.
- Each user record lists the shared endpoint, their own line, and the other user's line.

Ordering Lines without Endpoints

Cisco Prime Collaboration Provisioning allows you to order lines or shared lines without any associated endpoints. The users can add the desired endpoints to these lines through the User Provisioning page (User Provisioning) or Self-Care. You can add lines without endpoints through user interface or in bulk through batch provisioning.

Note This feature is supported for Cisco Unified Communications Manager 10.0 and above. This feature is supported for all deployment models such as small, medium, and large.

Though the following attributes are present in Cisco Prime Collaboration Provisioning while ordering lines without endpoints, they do not have the associated mapping field in Cisco Unified CM:

- Line Position
- Line Groups
- Redirected Number
- Dialed Number
- Caller Number
- Caller Name
- Maximum Number of Calls
- Busy Trigger
- Log Missed Calls
- Monitoring Calling Search Space
- Recording Media Source
- Visual Message Waiting Indicator Policy
- Line Text Label
- External Phone Number Mask
- Ring Setting (Phone Idle)
- Ring Setting (Phone Active)
- Call Pickup Group Audio Alert (Phone Idle)
- Call Pickup Group Audio Alert (Phone Active)
- Use Service Parameter
- No Retrieve Destination Internal-Calling Search Space
- Display (Internal Caller ID)
- ASCII Display (Internal Caller ID)
- Advertise via Intercluster Lookup Service

To add an endpoint to the line, rest your cursor on the line service listed in the Service Details pane and click the Attach Endpoint option. You can detach the associated endpoint from a line using the Detach Endpoint option in the quick view.

You have to re-synchronize after the endpoints are associated through Self-Care to manage the endpoints registered through Self-Care.

You can retain the line services of an endpoint while cancelling the endpoint. Once the endpoint service is cancelled, the retained lines will be considered as lines without endpoint. Cisco Prime Collaboration Provisioning allows you to add voicemail and email services to the lines without endpoints.

You can use the following Endpoint/Line Mismatch Reports to identify the lines that are not associated to endpoints:

- Users with No Line
- Users with Lines and No Endpoint
- Unassigned Lines

To generate this report, Choose Reports > Endpoint/Line Mismatch Reports, and click Export next to the desired report.

Related Topics

Prime Collaboration Self-Care Overview, on page 243
Creating a Self-Care Account, on page 243
Enabling or Disabling Self-Care Using Batch Provisioning, on page 244
Launching Prime Collaboration Self-care, on page 244
Customizing Your Personal Settings, on page 245
Configuring Phone and Extension Mobility Setting, on page 246
Line Settings, on page 247
User Settings, on page 248
Common Self-Care Tasks, on page 248
Configuring Single Number Reach, on page 249
Self-Care User Migration Script, on page 250

Attach Extension Mobility Access to a Line

For Cisco Prime Collaboration Provisioning 12.2 and later

This functionality allows the user to attach an Extension Mobility Access to an unassigned line using Cisco Prime Collaboration Provisioning User Interface.

Procedure

Step 1 Choose **User Provisioning** .

Step 2 Select the User to whom you need to attach the EM Access.

Step 3 In the Service Details page, hover over the information (i) icon next to the selected unassigned line, and click **Attach EM Access** in the Actions list.

Step 4 In Configure Service page, enter the necessary information such as Selected EM Access, Line Position, Line Description, and so on.

Step 5 Click **Continue**.

Step 6 In Order Confirmation Details page, click **Confirm** to attach the EM Access for the selected line.

Detach Extension Mobility Access from an Extension Mobility line

For Cisco Prime Collaboration Provisioning 12.2 and later

This functionality allows the user to detach the Extension Mobility Access from an Extension Mobility line using Cisco Prime Collaboration Provisioning User Interface.

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Select the User for whom you need to detach the EM Access from the Extension Mobility Line.

Step 3 In the Service Details page, hover over the information (i) icon next to the selected EM Access line, and click **Detach EM Access** in the Actions list.

Step 4 In Order Confirmation Details page, click **Confirm** to detach the EM Access to the selected EM line.

Ordering Voicemail Service

To order Voicemail service:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click the desired user.

Step 3 In the Service Details page, click **Custom Services Wizard**.

Step 4 Select a Service Area from the drop down list. Rest your mouse pointer over the quick view icon for information on a Service Area in the drop-down list.

Step 5 Click **Continue**.

Step 6 Select Voicemail service and click **Continue**.

Step 7 In the Service Provisioning page, do the following:

- Enter the required information in the Basic Voicemail Information pane.

  Note Text to Speech (TTS)-enabled and TTS-disabled service templates are displayed in the Service Template drop-down list, only if an Exchange Server is configured for that Service Area. If Exchange Server is not configured in that Service Area, only the TTS-disabled service templates are displayed in the Service Template drop-down list.

- In the Advanced Order Configuration pane, enter the required information in the following tabs:
  - General (see Table 61: Advanced Order Configuration - General , on page 276 for field description).
  - Received Messages (see Table 62: Advanced Order Configuration - Received Messages, on page 278 for field description).
  - Call Behavior (see Table 63: Advanced Order Configuration - Call Behavior, on page 280 for field description).

- Phone Menu (see Table 64: Advanced Order Configuration - Phone Menu, on page 282 for field description).
- Sent Messages (see Table 65: Advanced Order Configuration - Sent Messages , on page 283 for field description).
- Alternate Identities

Note General, Received Messages, Call Behavior, Phone Menu, Sent Messages, and Alternate Identities tabs are displayed for Unity Connection 10.x and above.

Step 8 Click **Continue.**

Step 9 Click **Confirm** and then click **OK.**

Note
- All Voicemail users provisioned in Unity Connection will be created as users integrated with Cisco Unified Communication Manager.
- When Cisco Prime Collaboration Provisioning imports an user from Unity Connection LDAP Import list , the user will be shown as Active LDAP Imported User.
- User fields such as Alias, First Name and Last Name will be greyed out.

Table 61: Advanced Order Configuration - General

Field	Description
Cross-Server Transfer Extension	Enter the extension to release transfer calls to, if a user attempts to transfer a call to another user but the cross-server transfer attempt is unsuccessful.
Outgoing Fax Server	Select the applicable fax server for the user.
Partition	Select the partition to which the object belongs. Partitions are grouped together into search spaces, which are used to define the scope of objects (for example, users and distribution lists) that a user or outside caller can reach while interacting with Unity Connection.
Search Scope	Select a search space to apply to the user account.
Phone System	Select the phone system on which the user extension was created.

Class of Service	Lists the class of services (COS) that are configured in the Unity Connection device. If you select one of the TTS-enabled COS, Unified Messaging service is enabled for that Voicemail account. If you select the TTS-disabled COS, Unified Messaging service is disabled for that Voicemail account. TTS-enabled COS and TTS-disabled COS options are displayed in the Class of Service drop-down list, only if an Exchange Server is configured for that Service Area. If Exchange Server is not configured in that Service Area, only the TTS-disabled COS options are displayed. While ordering Voicemail, if you are not selecting any value from the Class of Service drop-down list, class of service is configured based on the subscriber template assigned for that service area. In the service listing page, Text-to-Speech icon will be displayed against the Voicemail service if Unified Messaging service is enabled for that Voicemail account. The Voicemail quick view will also display the class of service assigned for that Voicemail account and whether Unified Messaging service is enabled for that Voicemail account. **Note** This option is available for Unity Connection 9.0 and above versions. **Note** This is an optional field while adding the Voicemail account. But, this is a mandatory field while changing the Voicemail order.
Exchange Server	This field will appear only if you are changing the Voicemail order. If Unified Messaging service is enabled for that Voicemail account, this field will display the name of the Exchange server on which the mailbox is created for that Voicemail account. If Unified Messaging service is disabled for that Voicemail account, all the Exchange Servers that are configured in that Service Area will be displayed in this drop-down list.
Active Schedule	Select a schedule from the list to specify the days and times that the standard and closed greetings play, as well as the action that Unity Connection takes after the greeting.
List in Directory	Check this check box to list the user in the corporate directory, which outside callers can use to reach users.
Send Non-Delivery Receipts on Failed Message Delivery	Check this check box to route non-delivery receipt (NDR) messages to the sender when message delivery fails.
Skip PIN When Calling From a Known Extension	Check this check box if you do not want this user to be asked for a PIN when calling from this extension.
Use Short Calendar Caching Poll Interval	Check this check box so that the Outlook calendar information for the user is updated according to the frequency that is configured in the Calendars: Short Calendar Caching Poll Interval (In Minutes) field.

Set for Self-Enrollment at Next Sign-In	Check this check box so that the user is asked at the next sign-in to record a name and a standard greeting, to set a PIN, and to choose whether to be listed in the corporate directory.
Location	
Address	Enter the user address.
Building	Enter the building the user is located in.
City	Enter the city.
State	Enter the state.
Postal Code	Enter the postal code.
Country	Enter the country.
Time Zone	Select the desired time zone for the user.
Language	Select the desired language for the user.
Manager	Enter the name of the manager.
Department	Enter the user department.
Billing ID	Billing ID can be used for organization-specific information, such as accounting information, department names, or project codes.

Table 62: Advanced Order Configuration - Received Messages

Field	Description
Maximum Message Length	Set the recording length (in seconds) allowed for messages left by unidentified callers.
Callers Can Edit Messages	Check this check box to allow callers to be prompted to listen to, add to, rerecord, or delete their messages.
Message Urgency	Indicate the action that Unity Connection allows when a message has been left by an unidentified caller or by a user who has not explicitly signed in: • Mark Normal—Messages left by unidentified callers are never marked urgent. • Mark Urgent—All messages left by unidentified callers are marked urgent. • Ask Callers—Connection asks unidentified callers whether to mark their messages urgent.

Message Sensitivity	Indicate the action that Unity Connection allows when a message has been left by an unidentified caller or by a user who has not explicitly signed in: • Mark Normal—Messages left by unidentified callers are never marked private. • Mark Private—All messages left by unidentified callers are marked private. • Ask Callers—Connection asks unidentified callers whether to mark their messages private.
Mark Secure	Check this check box to have Unity Connection mark messages as secure that are left for this user by unidentified callers or by users who have not explicitly signed in.
Play After Message Recording	Indicate the action that Unity Connection performs after a message has been sent by an unidentified caller or by a user who has not explicitly signed in: • Do Not Play Recording—No recording will be played after the message has been sent. • System Default Recording—Play the default system recording after the message has been sent. • Play Recording—Play the customized recording after the message has been sent.
Recording Selection	This field will be enabled only if you select the Play Recording option in the Play After Message Recording field.
Language That Callers Hear	Select the language in which system prompts are played to callers.
After Message Action	This field will be enabled only if you select the Play Recording option in the Play After Message Recording field.
Respond to Requests for Read Receipts	Select the language in which system prompts are played to callers.

Message Aging Policy	Indicate the action that Unity Connection performs after a caller leaves a message: • Call Action—Select the applicable action from the list. • Call Handler—Sends the call to the system call handler that you specify. • Interview Handler—Sends the call to the interview handler that you specify. • Directory Handler—Sends the call to the directory handler that you specify. • Conversation—Sends the call to the conversation that you specify. • User with Mailbox—Sends the call to the user extension that you specify.
Use System Settings for Mailbox Quotas	Check this check box to use the system settings for mailbox quotas.
Warning Quota	When the mailbox for a user reaches this size, the user is warned that the mailbox is near the maximum size allowed.
Send Quota	When the mailbox for a user reaches this size, the user is prevented from sending any more voice messages.
Send/Receive Quota	When the mailbox for a user reaches this size, the user is prevented from sending or receiving any more voice messages.
Message Actions	
Voicemail	Select the action that Unity Connection takes when the user receives a voice message.
Email	Select the action that Unity Connection takes when the user receives an e-mail message.
Fax	Select the action that Unity Connection takes when the user receives a fax message.
Receipt	Select the action that Unity Connection takes when the user receives a delivery receipt.

Table 63: Advanced Order Configuration - Call Behavior

Field	Description
Caller Input Keys	To edit caller input settings, select the applicable key.
Wait for Additional Digits	Indicate the amount of time that Unity Connection waits for additional input after callers press a single key that is not locked.
Enable Prepend Digits	Check this check box to simulate abbreviated extensions by using prepended digits for call handlers and user mailboxes.
Prepend Digits	Enter the digits that are prepended to any extension that a caller dials while listening to the greeting of the user.

Alternate Rule, Closed Rule, and Standard Rule	
Rule Status	Specifies whether the rule is enabled or disabled.
Date/Time	Indicates the date and time at which the rule is disabled, if it has been enabled until a specific end date.
Transfer Calls To	Select one of the following settings: • Greeting—When this option is selected, the call is transferred as follows: For user settings—to the user greeting, without ringing the user phone. For call handler settings—to the call handler greeting. • Extension—Enter an extension to which the call is forwarded.
Extension	The extension that the phone system uses to connect to the object.
Transfer Type	Select how Unity Connection transfers calls. • Release to Switch—Unity Connection puts the caller on hold, dials the extension, and releases the call to the phone system. When the line is busy or is not answered, the phone system—not Unity Connection—forwards the call to the user or handler greeting. This transfer type allows Unity Connection to process incoming calls more quickly. Use Release to Switch only when call forwarding is enabled on the phone system. • Supervise Transfer—Unity Connection acts as a receptionist, handling the transfer. If the line is busy or the call is not answered, Unity Connection—not the phone system—forwards the call to the user or handler greeting. You can use supervised transfer whether or not the phone system forwards calls. Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly.
Rings to Wait For	Select the number of times the extension rings before playing the user or handler greeting.
Play the “Wait While I Transfer Your Call” Prompt	Check this check box to have Unity Connection play “Wait while I transfer your call” to callers while performing the transfer.
If Extension Is Busy	Indicate how Unity Connection handles calls when the phone is busy. You may want to use holding options sparingly, because having calls on hold can tie up ports.
Tell Me When the Call Is Connected	Check this check box to have Unity Connection say “transferring call” when the user answers the phone. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option.

Tell Me Who the Call Is For	Check this check box to have Unity Connection say “call for <recorded name of user or call handler>” or “call for <dialed extension number>” when the user answers the phone. Use this setting when users share a phone or a user takes calls from more than one dialed extension. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option.
Ask Me If I Want to Take the Call	Check this check box to have Unity Connection ask users whether they want to take a call before transferring the call. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option.
Ask for the Caller's Name	Check this check box to have Unity Connection prompt callers to say their names. When answering the phone, the user hears “Call from...” before Connection transfers the call. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option.

Table 64: Advanced Order Configuration - Phone Menu

Field	**Description**
Touchtone Conversation Menu Style	Select the menu style to be used for touchtone conversation.
Touchtone Conversation	Select the Touchtone Conversation style that users hear when they listen to and manage their messages by phone.
Conversation Volume	Select the volume level at which users hear the conversation.
Conversation Speed	Select the speed at which prompts are played to users.
Enable Finding Messages with Message Locator	Check this check box to allow users to find voice messages from other users and from unidentified callers when they check messages by phone.
Message Locator Sort Order	Select one of the following options: • Last In, First Out • First In, Last Out Use in conjunction with the Finding Messages with Message Locator-Enabled check box, to allow users to find specific messages by phone.
Time Format	Indicates the time format that Unity Connection uses to play time stamps when users listen to their messages by phone.
When Responding to Menus	
Times to Repeat Menu	Specify how many times Unity Connection repeats a menu when a user has not responded to it. The range of valid entries is 0 to 10.

Wait for First Touchtone (Milliseconds)	Specify how long Unity Connection waits for a user to press a first key or say a voice command after playing a menu. The range of valid entries is 500 to 10,000 milliseconds. Default setting: 5,000 milliseconds.
Wait for Names, Extensions, and PINs (Milliseconds)	Specify how long Unity Connection waits for additional key presses after the user has pressed a key when entering usernames or extensions to address a message, update passwords or PINs, change call transfer or message notification numbers, and so on. The range of valid entries is 1,000 to 10,000 milliseconds. Default setting: 3,000 milliseconds.
Wait for Multiple Digit Menu Options (Milliseconds)	Specify how long Unity Connection waits for additional key presses after the user has pressed a key that represents the first digit of more than one possible key combination in a particular phone menu. The range of valid entries is 250 to 5,000 milliseconds. Default setting: 1,500 milliseconds.
After Sign-In, Play	Check the appropriate check boxes to indicate what Unity Connection plays after a user signs in.
When Exiting the Conversation	Select from the following actions, to indicate the destination to which Unity Connection sends users when they exit the conversation: • Call Action—Select the applicable action from the list. • Call Handler—Sends the call to the system call handler that you specify. • Interview Handler—Sends the call to the interview handler that you specify. • Directory Handler—Sends the call to the directory handler that you specify. • Conversation—Sends the call to the conversation that you specify. • User with Mailbox—Sends the call to the user extension that you specify.

Table 65: Advanced Order Configuration - Sent Messages

Field	Description
Message Volume	Select the volume level at which Unity Connection plays the body of user messages and recorded introductions for fax messages when users play their messages by phone.
Message Speed	Select the speed at which Unity Connection plays the body of user messages and recorded introductions for fax messages when users play their messages by phone.
Fast Forward Message by (milliseconds)	Specify the amount of time that Unity Connection skips ahead when users fast-forward while listening to messages.

Rewind Message by (milliseconds)	Specify the amount of time that Unity Connection skips back when users rewind while listening to messages.
For Saved Messages Play Count	Check this check box to have Unity Connection announce the total number of messages that have been saved.
For Draft Messages Play Count	Check this check box to have Unity Connection announce the number of messages that have been saved as drafts.
Play Message Type Menu Before Messages	Check this check box so that Unity Connection plays the message type menu when users sign in to Unity Connection by phone:
After the Menu Automatically Advance to the Next Message	Check this check box to set Unity Connection to automatically move to the next message in the message stack without requiring user to perform any action in the After Message Menu options, such as Save or Delete.
Confirm When Deleting New and Saved Messages	Check this check box to have Unity Connection ask users to confirm their choice when they delete new and saved messages by phone. Consider checking this check box if users do not have access to deleted messages.
For New Messages, Play	Check the check boxes, as applicable, to have Unity Connection announce message count totals for messages that are marked new.
When Disconnected During Message Playback	
Create a Message Bookmark	Check this check box if you want Unity Connection to create a message bookmark when the call is disconnected or the user hangs up while listening to a message.
Mark a New Message	Indicate whether you want Unity Connection to leave messages marked as new or mark them as saved (read) if users access the message body and then hang up or are disconnected before indicating how to manage the message.
For Each Message, Play	
Sender’s Information	Check this check box so that Unity Connection plays caller information about a message sender after playing the message.
Include Extension	Use in conjunction with the Sender’s Information check box. Check this check box to have Unity Connection include the extension of the user who left the message, in addition to the recorded name, after playing the message.
Sender’s ANI	Use in conjunction with Sender’s Information check box. For messages left by an unidentified caller, check this check box to have Unity Connection provide the phone number (ANI or caller ID) information after playing the message.

New Message Play Order	Indicate the order in which Unity Connection plays new messages to the user: • Sort by Message Type—Select a message type, and then select the Up and Down arrows to reorder the list of message types. • Then By—Select Newest First or Oldest First to specify the order in which Unity Connection plays new or saved messages. Note that except for receipts, urgent messages are always played before regular messages for each message type (receipts are sorted by the time that they were sent).
Saved Message Play Order	Indicate the order in which Unity Connection plays saved messages to the user.
Deleted Message Play Order	Select Newest First or Oldest First to specify the message order for deleted messages. **Note** Except for receipts, urgent messages are always played before regular messages for each message type (receipts are sorted by the time that they were sent).
Send Message Settings	
User Can Send Broadcast Messages to Users on This Server	Check this check box to allow users to send broadcast messages to all users on the local Unity Connection server.
User Can Update Broadcast Messages Stored on This Server	Check this check box to allow users to edit broadcast messages. By checking this check box, you also enable users to send broadcast messages to all users on the local Unity Connection server.
Message Addressing and Sending	
Enter a Recipient By	Select how the conversation prompts users to address messages to other users: • Spelling the Last Name Then First Name • Entering the Extension • Spelling the First Name Then Last Name
Confirm Recipient by Name	Enable this option if you want users to hear a confirmation of a selected name when addressing users.
Continue Adding Names After Each Recipient	Enable this option so that Unity Connection asks users to continue adding names after each recipient when sending and forwarding messages to multiple recipients.
When a Call Is Disconnected or the User Hangs Up	Indicate whether you want Unity Connection to send or discard messages when calls are disconnected while users are in the process of sending, replying to, or forwarding a message. Calls can be intentionally or unintentionally disconnected when a user hangs up or a mobile phone loses its charge or signal, and so on.

Allow Users to Save Draft Messages	Check this check box to allow the user to choose whether to save a message as a draft during message composition.
Retain Urgency Flag When Forwarding or Replying to Messages	Check this check box to have Unity Connection retain the urgency flag when users forward or reply to urgent messages by using the phone interface.

Changing the Voicemail Password or PIN

To change the voicemail password or PIN for a user:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Place your cursor over the quick view icon to launch the quick view for the user.

Step 3 Click **Manage Passwords/PINs**.

Step 4 In the Manage User page, select **Unity Connection PIN** from the Select Password drop-down list to change the voicemail PIN of the user. Select Unity Connection Web Password to change the web application password for Unity Connection.

Step 5 Click Done.

The Unity Connection Password or PIN that you add in the Manage User page will be applied to all the voicemail accounts created for the user.

To change the Password or PIN for an individual voicemail account, place your cursor over the quick view icon displayed next to the Voicemail service in the Service details page, and click Password/PIN. You can also change the password or PIN settings in the Manage Voicemail page. The following table explains the fields displayed in the Password/PIN settings area of the Manage Voicemail page.

Field	Description
Locked by Administrator	Check this check box to prevent a user from accessing Cisco Unity Connection. To prevent a user from accessing voicemail, check this check box for the Voicemail PIN.
User Cannot Change	Select this option to prevent the user from changing the password or PIN. Use of this setting is most applicable for accounts that can be accessed by more than one person. When you select this option, also check the Does Not Expire check box.
User Must Change at Next Sign-In	Select this option when you have set a temporary password or PIN, and want the user to set a new password or PIN the next time that the user signs in to Cisco Unity Connection.
Does Not Expire	Check this check box to block the system from prompting the user to change this credential. Use of this check box is most applicable for low-security users or for accounts that can be accessed by more than one person. If this check box is checked, the user can still change this credential at any time.

Field	Description
Authentication Rule	Select the authentication policy to apply to the selected user password or PIN settings.

Configuring and Provisioning Notification Devices

For Cisco Prime Collaboration Release 11.2 and later

You can provision SMTP Notification devices for a Cisco Unity Connection user from Cisco Prime Collaboration Provisioning itself through batch and the user interface. Cisco Unity Connection allows the user to be notified of the incoming voice messages and emails when the message arrives in the user mailbox. SMTP Notification Devices can be provisioned to new voicemail users or existing users. Through batch and the user interface, you can:

- Add or Change or Cancel SMTP Notification template.
- Add or Change or Cancel SMTP Notification device.
- Add or Change voicemail template for SMTP Notification template.
- Add or Change voicemail order for SMTP Notification template.

In addition, you can apply keywords in service template, user interface, and batch for notification settings to provide a consistent text message format. You need not change each voicemail notification setting with its user-related information.

Keywords are supported for the following attributes:

- Display Name
- To
- From
- Message Header
- Message Body
- Message Footer

To add an SMTP template with keywords through the user interface, choose **Provisioning Setup**. In the All Domains pane, expand a Domain and click **Service Templates**. Click **Add** and select **Voicemail - SMTP Notification** service from Template Settings for Cisco Unity Connection Processors to proceed with the process. You can also edit or copy or delete the service template as suitable.

Management of Notification Devices from Ordering Wizard

Hover the voicemail quick view on the **Service Details** page (**User Provisioning** select a user) to launch the notification devices. The page displays the notification devices that are already created for the user. You can add or edit or delete the SMTP Notification device from the user interface.

Click **Save** to provision the notification device to Cisco Unity Connection. Order is created for the SMTP Notification device and the order status is shown with the order ID.

In addition, you can cross-launch the following notification devices:

- Phone

- Pager
- HTML

Note

- Each user can have multiple Notification device settings of same type or different type.
- Notification settings configured in user templates are applied to user by default when a voicemail is created. Default notification settings can only be modified and cannot be deleted.
- You can select both voicemail service template and notification device template to order voicemail.
- You are recommended to perform Cisco Unity Connection user synchronization if you are not able to provision SMTP for a voicemail user or SMTP is not getting listed when you click **Notification Devices**.

Reapplying SMTP Template through Change Voicemail Flow

To reapply an SMTP template through change voicemail flow:

1. Add an SMTP template with a display name. For example: SMTP-X.
2. Create a voicemail template by selecting the newly added SMTP template and place voice mail order using the voicemail template. SMTP device namely SMTP-X is provisioned to the user.
3. Change the SMTP template for display name. For example: SMTP-Y.
4. Reapply the SMTP template through change voicemail to the user.
5. One more SMTP device namely SMTP-Y is provisioned to the user.

Ordering Presence Services

To order a Presence service:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Check the check box next to the user that you want to provision the services.

Step 3 Click **Provision Services**.

Step 4 In the Service Details page, click **Custom Services Wizard**.

Step 5 Select a Service Area and click **Continue**.

Step 6 Select User Services and then click **Continue** to configure the User Services product.

Note User Services can also be ordered through batch, auto provisioning, manual provisioning and Getting Started Wizard.

User Services can also be ordered by clicking **Add User to Unified CM only** link from the quick view icon in the user record page.

User Services is available for Cisco Unified Communications Manager 10.x and above versions. After you upgrade to Provisioning 9.0 and above, User Services will not be available for ordering. You should manually associate this service to the corresponding user role.

User Services is available as an orderable service and it is also added by default when you create an order for a service.

The User Services Entry fields table describe the various fields for configuring the User Services.

Step 7 Click **Continue**.

Step 8 In the Order confirmation page, click **Confirm.**

Table 66: User Services Entry Fields

Field	Description
Service Template	Choose the service template that you want to use.
Enable Service Settings	
Enable User for Unified CM IM and Presence	Used to enable or disable Unified CM IM and Presence.
Home Cluster	Indicates whether this cluster is the home cluster for the user.
UC Service Profile	Used to associate a service profile to a user.
User Profile	Indicates the profile that is associated to a user.
User Locale	From the drop-down list, choose the locale that is associated with the user. The user locale identifies a set of detailed information to support users, including language and font.
User Information	

Self-Provisioning User ID	For Cisco Unified Communications Manager 10.0 and above, when you create an order for line service, Self-Provisioning User ID is added to the Directory Number of the user by default (based on the primary extension number). If you want to change the Self-Provisioning User ID: **1.** 1. Place your cursor on the quick view icon displayed next to the User Services, and click **Change**. **2.** In the Change Order page, update the S elf-Provisioning User ID, and then click **Continue**. **3.** In the Confirm Details page, click **Confirm**. For Cisco Unified Communications Manager 10.x, Self-Provisioning User ID field will not be displayed.
Extension Mobility	
Default Profile	From the drop-down list, choose a default extension mobility profile for this user.
Subscribe Calling Search Space	From the drop-down list box, choose the calling search space to use for presence requests for the user. If you do not select a calling search space for the user from the drop-down list, the Subscribe calling search space defaults to None.
Enable Extension Mobility Cross Cluster	Check this check box to enable this user to use the Cisco Extension Mobility Cross Cluster feature.
Directory Number Association	
Primary Extension	This field represents the primary directory number for the user.
Mobility Information	
Enable Mobile Voice Access	Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Mobile Connect calls and activate or deactivate Mobile Connect capabilities.
Maximum Wait Time for Desk Pickup	Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desktop phone.
Multilevel Precedence and Preemption Authorization Settings	
MLPP User Identification Number	The MLPP User Identification number must be composed of 6 - 20 numeric characters.

MLPP Precedence Authorization Level	The Precedence Authorization level can be set to any standard precedence level from Routine to Executive Override.
Groups and Roles	
Groups	This list box displays after an end user record has been saved. The list box displays the groups to which the end user belongs. To add the user to one or more user groups: **1.** Click the Add button. **2.** Locate the groups to which you want to add the user, and check the check boxes beside those groups. **3.** Click **Add Selected** at the bottom of the window. To remove the user from a group, highlight the group in the Groups list box and click the Remove button.
Roles	The list box displays the roles that are assigned to the user.
Conference Now Information	
Enable End User to Host Conference Now	Check this check box to enable the user to host a conference.
Meeting Number	This is a display-only field. This field displays the Self-Service user id, which is used to join the conference.
Attendees Access Code (Optional)	This field represents the access code, which is used by the attendees to join the conference. You can enter value in this field, only if the **Enable End User to Host Conference Now** check box is checked.

Note Conference Now settings field is available only for Cisco Unified Communications Manager 11.x and above versions.

Related Topics

Associating User Roles with Services, on page 75

Associating a User Profile to a User

You must assign a user profile to a user for enabling Self-Care for the user.

The User Services includes the user profile provisioning attribute. The User Services will list all the configured user profiles. You can select the desired profile for the user at the time of ordering the service.

The user profile attribute is also available in the service template for User Services. If user profile is configured at service area level, when the first order is placed for a user, the value will be retrieved from the service area and associated to the user.

Note The user profile attribute is supported for Cisco Unified Communications Manager 10.x and above.

If User Data Service (UDS) feature is enabled in Cisco Prime Collaboration Provisioning, user will be provisioned in all clusters, but the user profile will be assigned to the user only in the cluster where the first order is placed.

Assigning user profile to a user automatically

You can configure the user profile attribute at service area level by using the Service Templates for automatically associating the user profile to a user. At the time of user creation, the value of user profile will be rendered from the corresponding service area and added in the Add User request.

Assigning user profile to a user manually

To assign a user profile to a user manually, you must configure the User Services. You must select the desired user profile from the drop down list and place the order to associate the user profile to the user .

You can change the configured user profile by updating the User Services. If the user profile is configured for a user, the configured user profile value will be displayed in the Service details page.

Note As part of the user synchronization, the user profiles will be imported from call processor and stored in the Provisioning inventory.

Managing Endpoints without an Associated User

The Pseudo user role allows you to provision endpoints without an associated user in the Call Processor.

Provisioning an endpoint for a Pseudo user is the same as that for a regular user, except that a user is not created in the Call Processor. You can order any services that include the following base services for a Pseudo user:

- Endpoint (including all endpoint types)
- Line
- Voicemail

Changing a user’s role from Pseudo to a regular role or vice versa is allowed only if the user does not have any services configured.

The following procedure describes how to associate the endpoints that do not have an associated user to a pseudo or existing user.

Procedure

Step 1 Export all endpoints that do not have an associated user to a file (see Exporting Endpoints Without Associated Users, on page 293).

Step 2 Modify the exported file so that each endpoint can be associated to a new Pseudo user or desired existing user.

Step 3 Create a batch action file using the modified file, and then run the batch project (see Batch Provisioning, on page 127).

Step 4 Upon completion of the batch project, you must run a Domain synchronization to assign a Service Area to the endpoint so that the endpoint will be displayed in the user record.

Note If a Service Area was listed in the file, the endpoint will be assigned to that Service Area (if an exact match is found) after a Domain synchronization is run.

Exporting Endpoints Without Associated Users

You can export endpoints without associated users and batch import the endpoints with real or pseudo usernames.

Note You can export hardware phones. You cannot export SoftPhones or Extension Mobility.

Procedure

Step 1 Choose **Advanced Provisioning** > **Manage Endpoints**.

Step 2 In the Endpoint Inventory Management page, select the Call Processor and endpoint model, and then click **Search Endpoints Without Associated User**.

Step 3 In the Endpoints Without Associated Users page, check the check box next to the endpoints that you want to export, and then click **Export Selected Endpoints**.

Step 4 If you plan to use the exported file for batch import of endpoints, specify the domain and suffix for user IDs in the Export Endpoints without Associated Users dialog box.

Step 5 Click **Export**.

Replacing Existing Endpoints

Through the Replace feature, you can replace an existing endpoint for a user, change the endpoint's MAC address, or update other endpoint settings.

Note

- The Replace feature does not allow you to change the line positions of assigned lines.
- The Replace feature does not support the change of the device protocol (SCCP/SIP). Cancel the existing endpoint, and provision the new endpoint with the differing protocol selected.

You can pick the same endpoint type, or choose from a list of other available endpoint types for the user. The endpoint types that users have access to are determined by their user role, and the number of lines on the endpoint that you are replacing. Endpoints that do not support the required number of lines are not available during the change order process.

When a endpoint is replaced, all of its lines are transferred to the new endpoint. The Service Area assigned to the new endpoint is the same as for the original endpoint.

Users with the ordering authorization role can replace their own endpoints, or those of other users.

When you submit a replace endpoint order, remember the following:

- Any attributes that are not supported by Cisco Prime Collaboration Provisioning and exist on the endpoint before placing a replace endpoint order will either be reset to their default values or dropped from the endpoint.
- The lines assigned to the original endpoint are associated to the newly added endpoint. But the newly selected associated endpoint button template must support the same number (or more) of assigned lines as the original endpoint.
- Only services that are configured for the Domain will be kept after an endpoint replace order is performed. If any other services existed on the endpoint, they will be dropped.
- Some attributes may not be supported by a particular endpoint type on a given protocol, so when placing endpoint orders, you should only set values for attributes that are supported by the chosen endpoint type and protocol. If you do not, orders may fail.
- While replacing endpoint orders, you should provide a supported value for the DND Option attribute based on the endpoint type. Certain endpoint types like Nokia and iPhone accepts only one value whereas other endpoints supports up to 3-4 values for this attribute. If you provide wrong values for DND Option the order will not be replaced.

  To replace endpoints for users, in the Services pane, hover over the endpoint that you want to replace, and then click Replace in the Actions list.

  To change the basic and advanced settings for an endpoint or service, click Change in the Actions list.

  Note You cannot change the voicemail alias for all Provisioning versions. For Cisco Unity Connection, you can change the voicemail alias for all versions.

Changing the Owner of an Endpoint

You can change the ownership of an endpoint from one user to another user in the same Domain.

To change the owner of an endpoint, in the Services pane, hover over the endpoint that you that you want to change, and then click Change Owner in the Actions list.

When you change ownership of an endpoint, all services associated to the endpoint (Line, Email, Voicemail, and Unified Messaging) are also changed.

You can enter different values for the Email ID and Display Name, if applicable. If you do not change the e-mail ID, e-mail display name, voicemail alias, or voicemail display name, the services on the Unified Message Processor do not change. Only the user records in Provisioning for the old and new owners are changed.

However, if any of these settings are changed, the voicemail and e-mail accounts on the Unified Message Processor are deactivated and then reactivated.

The Service Area assigned to the new owner is the same as the Service Area assigned to the original owner.

Note Users with the Ordering or Advanced Ordering role can make these changes, either to their own endpoints or to those of other users.

Attributes that contain the user's login ID (first name and last name) are updated with the new user's information (depending on the Domain rules and the user's provisioning attributes).

The following attributes may contain the user's login ID:

- Endpoint Description
- Alerting Name (online)
- Endpoint Owner User ID
- ASCII Display (Internal Caller ID)
- ASCII Line Text Label
- Line Text Label ASCII Alerting Name

Note the following points when changing the owner of an endpoint:

If the line is moved, the new user's and old user's telephone number and primary extension are updated accordingly.

If an endpoint is shared, you cannot change owners of the endpoint. The Change Owner button is not displayed.

If there are open orders against any of the associated services, a warning message appears, and you cannot continue.

Changing Line Information

You can submit an order to change line details. The following line details can be changed:

- Directory number
- Line position
- Provisioning attributes

You can change details on Line, Line on Shared Endpoint, and Extension Mobility Line products.

There are two sets of Provisioning Attributes on line products. One set is on the directory number level and the other is on the line level. When multiple lines share the same directory number, provisioning attributes set on the directory number level are common and shared among the line. Changing the provisioning attributes on one line impacts all of the lines.

Provisioning attributes set on the line level are not shared. Changing the provisioning attributes on one line does not impact the other lines.

To update Line details, in the Services pane, hover over the line that you want to change, and then click Change in the Actions list.

Unlocking Voicemail Accounts

If a voicemail account becomes locked (due to either user or system error), you can unlock the account through Cisco Prime Collaboration Provisioning.

You can unlock the following accounts:

- Voicemail account - For Cisco Unity Connection, and Cisco Unity Express devices.
- Web access account - For Cisco Unity Connection devices.

Before you begin

To unlock voicemail accounts, you must configure the Cisco Unity Connection devices (see Managing Devices Overview, on page 43).

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click the desired user.

Step 3 In the Services pane, hover over voicemail that you want to unlock. The Actions list with the option buttons appears. It enables you to perform the actions for the selected product.

Step 4 Click **Unlock**.

Note For Cisco Unity Connection, you may have a choice of either the voicemail or web access account. Select the desired account to unlock.

Step 5 Click **Confirm** and then click **OK**.

Searching for an Order

You can search for orders using any of the following information:

- Order information:
  - Order number

    - Author—Person who placed the order
    - Order status
    - Extended status—The state that the order is in (for example, being provisioned, waiting for approval, or waiting to ship)
- User information:
    - Login
    - First or last name
    - Phone number
    - Email
    - Department
    - Domain
- Order date
- Requested delivery date

To search for an order, choose **Activities> Provisioning History**. In the search page, enter the search information, and then click **Search.**

You can click **Export** to export the search details as a tab delimited file. Any changes made to the order can be viewed in this report.

Processing Orders

After you have submitted orders for users, they are approved and then shipped. Depending on how your Provisioning system has been configured, these steps may be automatic or may require processing by users.

There are four possible activities that can be assigned to users during the order processing stage. The activities are assigned based on the rules set for the Domain.

- Approve orders—Approves orders before provisioning can occur, and can also reject orders. This user must be assigned the Approval authorization role. This is controlled by the following rules:
    - IsAuthorizationRequiredForAddOrder
    - IsAuthorizationRequiredForChangeOrder
    - IsAuthorizationRequiredForCancelOrder
- Assignment—Assigns MAC address to an endpoint. This user must be assigned the Assignment role. This is controlled by the rule PhoneAssignmentDoneBy.
- Shipping—Ships the order. This user must be assigned the Shipping authorization role. This is controlled by the rule PhoneShippingDoneBy.
- Receiving—Done by the user who has the Receiver user role. Indicates that an ordered endpoint has been received. This is controlled by the rule PhoneReceiptDoneBy.

Note A Provisioning administrator can configure how these activities are assigned.

Related Topics

Business Rules for Domain Synchronization, on page 102

Approving Orders

To approve orders, you must be assigned the Approval authorization role .

After an order is approved or rejected, an e-mail is sent to the user for whom the order was placed. The following business rules must be enabled for the e-mail to be sent :

- EmailSender
- MailHost
- OrderProvisionedEmailTemplate
- OrderRejectedEmailTemplate

The e-mail is sent to the e-mail account configured for the user.

Note If an order is rejected, the order status is set to Cancel in the user record, and no provisioning is performed. If the order encounters a problem and the user chooses to abort the remainder of the order in the error handling workflow step, then the order status is set to Hold.

Procedure

Step 1 Choose**Activities** > **My Activities**.

Step 2 In the My Activities page, click the order that you want to process.

Step 3 In the Viewing Activity page, click **Accept.**

The Viewing Activity page appears with the Add a Note field added.

Note You can also decline the order or delegate it to another user or group. If you delegate the activity, new user or group is assigned to the activity.

Step 4 Enter the MAC Address for the endpoint and click **Step Complete**.

Related Topics

Overview of Authorization Roles, on page 210
Overview of Business Rules, on page 163

Stopping an Order

Cisco Prime Collaboration Provisioning provides you the option to stop an order that takes a long time to complete.

Procedure

Step 1 Choose **Administration > Settings** and select the required stop interval time from **Allow orders in progress to be stopped after** drop-down.

Step 2 Choose **Activities > All Activities/My Activities/Activities for Group/Activities for User**.

Step 3 In the next page, select an order and click **Stop order**.

Note The order check box is enabled based on the time interval selected in the **Allow orders in progress to be stopped after** drop-down.

Troubleshooting

Issue: If you are able to view pending orders, but unable to select an order from the list to abort, it might be that the minimum configured time limit for the order has not elapsed.

Recommended Action: Wait for the minimum time before trying to abort. By default, any order can be aborted after 15 minutes.

Issue: Orders are in unrecoverable error state and not showing up in All/My Activities page.

Recommended Action: Check "Include System Activities" in All Activities page to view all the activities of the order and proceed to abort.

Shipping Endpoints

Depending on how your Provisioning system is configured, this step may not be required. If your administrator has enabled shipping, you must be assigned the Shipping authorization role to perform this procedure . Shipping endpoints consists of two parts: assigning MAC addresses and shipping.

Procedure

Step 1 Choose **Activities > My Activities**.

Step 2 In the **My Activities** page, click the order that you want to ship.

Step 3 In the Viewing Activity screen, click **Accept**. The MAC Address field is active in the Viewing Activity endpoint Assignment page.

Step 4 In the MAC Address field, type a hexadecimal value. Valid values are alphanumeric characters (A-Z, a-z, 0-9). The value must be 12 characters in length.

Note The MAC address is available on a sticker on the endpoint set, and on the endpoint setting display on the handset.

Step 5 After you have added the required information, click **Step Complete.**

Step 6 In the **My Activities page**, click the Refresh icon.

Step 7 Click the order that appears in the **My Activities** page.

Step 8 In the Viewing Activities Form page, click **Accept.**

Step 9 Click **Step Complete**. If you did not create the order, the order no longer appears on the My Activities page.

To accept the endpoints, in My Activities page, click the order that you require, and then click Accept. You must be assigned the Receiving authorization role to accept the endpoints.

Related Topics

Overview of Authorization Roles, on page 210

Canceling Services

To cancel services, you must submit a cancel order. When you cancel a service, all services associated with it are also canceled. See Table 67: List of Associated Services, on page 300 for a list of associated services.

Note For the Single Number Reach Service, canceling the Enable Mobility service does not cancel the Remote Destination Profile or Remote Destination Profile Line services. Also, canceling the Remote Destination Profile service does not cancel the Enable Mobility service.

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click the desired user. In the service details pane, hover over the service that you want to cancel. The Actions list with the option buttons appears. It enables you to perform the actions for the selected service.

Step 3 Click **Cancel** and then click **Submit** in the **Order Cancel Form** pane.

Step 4 Click **OK** to confirm, and then click **Done.**

The canceled order appears in the **View Orders** pane with Completed status.

Note In the services section, an information icon (i) appears next to the service to indicate that the service has an order running against it. When the order has finished processing, the information icon disappears.

After the order has been processed, the canceled services are no longer displayed in the service User Record Details pane.

Table 67: List of Associated Services

Service Name	Associated Services
Voicemail	Unified Messaging
Line	Voicemail, Unified Messaging.

Service Name	Associated Services
Endpoint	Line, Voicemail, Unified Messaging. **Note** Cancelling an endpoint removes the associated directory numbers from the Cisco Unified Communications Manager.
Remote Destination Profile	Remote Destination Profile Line. **Note** Cancelling a Remote Destination Profile Line removes the associated directory numbers from the Cisco Unified Communications Manager.

Work Order States

This section explains the states an order goes through after it is entered.

Following are the work order states:

- Initial
- Released
- Completed
- Hold

When an order is placed, a work order is created and is in the Initial state. When execution of the workflow begins, the order transitions to the Released state. After completion of the workflow, the order transitions to the Complete state if all steps were successful, or to the Hold state if any of the steps failed. For the order to change to the Hold state, you may need to acknowledge that the order failed, or the change may occur automatically, depending on the origin of the work order.

Work orders also have an extended status field.

- If the order is in execution, the extended status is Being Provisioned.
- If the order failed, the extended status is Recoverable Error or Unrecoverable Error.

  If valid values are not provided while creating order, the order fails with the extended status unrecoverable error. The orders in unrecoverable error state cannot be provisioned, hence it must be stopped and a new order can be raised with valid values.

  If the device is unreachable, the order fails with extended status recoverable error. The orders in recoverable error state can be approved and provisioned.
- If the order is waiting for a user action, the extended status is set to a specific Wait status. Wait states are usually for assignment, often for shipping or receiving.

Changes in the extended status can occur without the work order changing state.

When a work order fails, the transition behavior from Released to Hold depends on which of the following was used to submit the work order:

- Provisioning NBI transitions from Released to Hold.

- Provisioning user interface remains in the Released state, waiting for you to take action on the order.
- Batch provisioning depends on the extended status. If the failure is a recoverable error, the order remains in the Released state, waiting for you to take action on it. If the failure is an unrecoverable error, the order transitions to Hold.

E-mail Notifications

E-mail Notifications improve manageability of notifications by allowing you to view critical events such as:

- Order approvals
- Order failures
- Synchronization failures
- Diskspace threshold

Notifications can be set at two levels:

- Domain Settings—For workflow events such as order approvals, assignment, shipping, and receiving in the Domain.
- System Settings—For system events such as order failures and synchronization failures.

Note Only users with global admin and domain admin roles can configure the notification settings.

You can test System and Domain notification configurations to ensure that the SMTP host and other settings are valid.

For Cisco Prime Collaboration Provisioning release 12.5 and later

You can use the **Disk Space Threshold** option to set a threshold for the disk space usage. The default value is 75%. You can change it to any number between 50 and 95. Cisco Prime Collaboration Provisioning checks for the disk usage at an interval of four hours. If at the time of checking the disk usage, the value crosses limit, then Cisco Prime Collaboration Provisioning sends Email notifications to both system users and external email addresses, if configured.

Related Topics

Configuring a Domain Notification Template, on page 302
Configuring Domain Notification, on page 304
Configuring System Notifications, on page 305
Testing Notification Settings, on page 306

Configuring a Domain Notification Template

Notification settings for Domain-specific events such as Order Approvals, Handle Assignment, Handle Shipping, and Handle Receiving can be set at the Domain level. A Domain notification template can be used to set up values that will be applied to any new Domains created in the system. Additionally, you can also choose to apply the values from the template to all the existing Domains in the system.

Procedure

Step 1 Choose **Administration** > **Domain Notification Settings**.

Step 2 In the Domain Notification Settings page, modify the Domain template, if required.

In the Email Settings pane, SMTP server details and the From Address values are inherited from the system settings and are displayed in read-only format. These settings cannot be changed in the Domain template; however, for specific Domains, these settings can be overridden.

Step 3 Set the time slot for the Aggregation and Escalation window to appear.

Step 4 Click **Test Settings** to ensure that SMTP host and other details are set up correctly.

Step 5 In the Notification Events pane, select events for which you have to send notifications.

Note The Workflow Pending Activity field contains events such as Order Approvals, Handle Assignment, Handle Shipping, Handle Receiving, and so on.

Step 6 In the Approval Notification Group, Assignment Notification Group, Shipping Notification Group, and Receiving Notification Group panes, do the following:

- External email addresses—Enter the e-mail addresses to which to send notifications.
- Aggregation window—Choose a setting to determine whether notifications of Domain events are aggregated or sent out as soon as an event occurs. The value <Not Set> results in no aggregation, and notifications are sent out immediately upon occurrence of an event.

  Any other value makes the system wait after an event to occur, for the time set in the aggregation window. During this time, if other related events occur, an aggregated notification with details of all such events is sent in a single e-mail.

  Note Events are based on workflow event type. Approval notifications and assignment notifications are aggregated in separate e-mails.

- Escalation Window—Choose a setting to determine whether inaction on workflow events results in an escalation e-mail to the system administrators. The value <Not set> means no escalation e-mails will be sent out.

  Any other value triggers the system to send out an e-mail to the system administrators after the time specified if no action was taken for the triggering event (for example, order approvals).

Step 7 Do either of the following:

- Click **Apply to domain template** only to save the settings as defaults for the Domains that will be created in the future.
- Click **Apply to all domains** to apply the notification settings to the existing Domains.

Related Topics

Testing Notification Settings, on page 306

Configuring Domain Notification

Notification settings for Domain-specific events such as Order Approvals, Handle Assignment, Handle Shipping, and Handle Receiving can be set at the Domain level. The settings on this page are inherited from the Domain configuration template if the Domain was created after the template was set up, or if the Apply to all domains option was selected when the template was set up.

Procedure

Step 1 Choose **Administration** > **Domain Notification Settings**.

Step 2 In the Domain Notification Settings page, select the desired Domain from the drop-down list. The page refreshes and displays the notification settings specific to the selected Domain.

Step 3 In the Email Settings pane, enter the following SMTP server details:

- Mail Server Name—SMTP server hostname or IP address (for example mailer.company.com).
- Mail Server Port—SMTP Server port. Optional setting if a nondefault port is used.
- Mail Server User Name—Username of the SMTP Server account. Specify only if an authenticated SMTP server is used.
- Mail Server User Password—Password of the SMTP server account. Specify only if an authenticated SMTP server is used.
- From address—Email address to use as the "from" address in Provisioning notifications (for example, ProvisioningManagerNotification@company.com).

Step 4 Click **Test Settings** to ensure that SMTP host and other details are set up correctly.

Step 5 In the Notification Events pane, select events for which to send notifications.

The Workflow Pending Activity field contains events such as Order Approvals, Handle Assignment, Handle Shipping, Handle Receiving, and so on.

Step 6 In the Approval Notification Group pane, for the external e-mail addresses, enter e-mail addresses to which to send notifications.

The approval notification group is a group of users with permission to perform order approvals in the Domain. Users configured in the system with this role for the Domain are displayed as System Users. These users are always notified of approval events.

Step 7 In the Assignment Notification Group, Shipping Notification Group, and Receiving Notification Group panes, for the external e-mail addresses, enter e-mail addresses to which to send notifications.

The assignment notification group is a group of users with permission to assign MAC addresses for phone orders in the Domain. Users configured in the system with this role for the Domain are displayed as System Users. These users are always notified of approval events.

The shipping notification group is a group of users with permission to perform shipping activities in the Domain. Users configured in the system with this role for the Domain are displayed as System Users. These users are always notified of shipping events.

The receiving notification group is a group of users with permission to perform receiving activities in the Domain. Users configured in the system with this role for the Domain are displayed as System Users. These users are always notified of receiving events.

Step 8 Click **Save** to apply the settings.

You can configure the aggregation and escalation settings for notifications that are sent to the assignment notification group.

Related Topics

Configuring a Domain Notification Template, on page 302
Testing Notification Settings, on page 306

Configuring System Notifications

Notification settings can be set at system level to manage notifications corresponding to system events such as synchronization failures and order failures.

Procedure

Step 1 Choose **Administration > System Notification Settings**.

Step 2 In the Email Settings pane, enter the following SMTP server details:

- Mail Server Name—SMTP server name or IP address (for example, mailer.company.com).
- Mail Server Port—SMTP Server port. This field is optional if a default port is used.
- Mail Server User Name—Username of the SMTP Server account. Specify only if an authenticated SMTP server is used.
- Mail Server User Password—Password of the SMTP server account. Specify only if an authenticated SMTP server is used.
- Confirm Mail Server User Password—Reenter the SMTP server account password to confirm.
- From address—Email address from which Cisco Prime Collaboration Provisioning sends notifications (for example, CUPMNotification@company.com).

Step 3 Click **Test Settings** to ensure that SMTP host and other details are set up correctly.

Step 4 In the Email Content URL Parameters pane, enter the following details, which will be used to construct a URL that will appear in the e-mail content:

- Protocol—Protocol to access Cisco Prime Collaboration Provisioning.
- Host—Hostname or IP address to access Cisco Prime Collaboration Provisioning.
- Port—Port used to access Cisco Prime Collaboration Provisioning (required only if a port other than 80 is used).

Note The fields in the Email Content URL Parameters pane are automatically populated with the relevant details.

Step 5 In the Notification Events pane, select events for which you have to send notifications.

Step 6 In the Administration Notification Group pane, set the following details:

- External Email Addresses—Email IDs of users or mailing lists to which to send e-mail notification of the chosen system events. Notifications are sent to administrators if their e-mail addresses are specified in the system. This list is displayed as read-only text in the System Users field.
- Aggregation window—Choose a setting to determine whether notifications of system events are aggregated or sent out as soon as an event occurs. The value <Not Set> results in no aggregation, and notifications are sent out immediately upon occurrence of an event.

  Any other value makes the system wait after an event occurs, for the time set for aggregation window. During this time, should other related events occur, an aggregated notification with details of all such events is sent in a single e-mail.

  Note Events are aggregated based on type. Synchronization failures and order failures are aggregated in separate e-mails.

Step 7 Click **Save.**

Related Topics

Testing Notification Settings, on page 306

Testing Notification Settings

You can test the notification configurations for the system and Domains to ensure that the SMTP host and other details are set up correctly.

To test your notification settings:

Procedure

Step 1 Choose either of the following:

- **Administration > System Notification Settings**
- **Administration > Domain Notification Settings**

Step 2 Click **Test Settings** and enter an e-mail address in the **Send Test Email To** field.

Step 3 Click **Send Test Email** to send an e-mail using the current settings.

Note If the test fails, an error message is displayed. Make the necessary changes in the settings and run the test again. However, a successful test will not automatically save the settings. Be sure to close the Test Email Settings page and save your settings.

CHAPTER 13

Cisco Prime Collaboration Provisioning Migration - 12.1

Cisco Prime Collaboration Provisioning Migration —12.1

You can migrate from Cisco Prime Collaboration Provisioning 11.1 and above to 12.1 either through **Dashboard** or **Administration > Updates > Launch Migration Tool** in the Cisco Prime Collaboration Provisioning user interface. You can migrate to Cisco Prime Collaboration Provisioning 12.1 in two ways:

- Running System—Select this option to migrate from a running Provisioning server.
- Migration File—Select this option to migrate from a file created by command-line migration backup tool, BackUpToolFor12_1Migration.

Note The following scenarios are not supported in 12.1 migration features:

- If Cisco Prime Collaboration Provisioning 11.x server is configured with SSO setup, then the same configuration does not work in Cisco Prime Collaboration Provisioning 12.1 server after migration, the user needs to configure the SSO again in the 12.1 server after the migration.
- If Cisco Prime Collaboration Provisioning 11.x server is enabled with FIPS mode, then the same configuration does not work in Cisco Prime Collaboration Provisioning 12.1 server after migration, the user needs to enable FIPS mode after the migration.
- If a user is having their own certificated in Cisco Prime Collaboration Provisioning 11.x server, then the same certificate does not get copied to Cisco Prime Collaboration Provisioning 12.1 server as part of migration, the user needs to upload the certificate in 12.1 server after the migration.

Before you begin

Ensure that you have:

- Taken a database backup of your existing 11.1/11.2/11.5/11.6 as suitable.
- New license files for 12.1. The license files must be updated after upgrade is complete.

- You must take a snapshot of Cisco Prime Collaboration Provisioning 12.1 Virtual Machine instance before starting the migration, and this snapshot can be deleted after the successful 12.1 migration.

Migration from Running System

You must provide the following server information:

Procedure

Step 1 Enter **Server IP Address** and **11.x's root Password**.

Step 2 Click **Next** to take a backup of the database.

Note Time taken to backup database depends upon the size of PCP database.

Step 3 Click **Begin Migration** to complete the process.
Once the migration is complete, you are redirected to the login page.

Note After migrating from Cisco Prime Collaboration Provisioning 11.x to 12.1, the 11.x server will not be accessible. The Administrator must manually restart the services to enable11.x server up and running.

Migration Using Migration File

You must provide the location of the migration file.

Procedure

Step 1 Select **SFTP** or **FTP** as suitable.

Step 2 Enter the following details.

- IP Address—IP Address of the server, where the back-file is saved
- Port—Disabled for FTP by default
- Path— The user needs to provide the path along with the file name
- Username— The back-up server's FTP/SFTP login username
- Password— The back-up server's FTP/SFTP login password

Step 3 Click **Next** to download the back-up file.

Step 4 Click **Begin Migration** to complete the process.
Once the Migration is complete, you are redirected to the login page.

Note You may have to repeat these steps to take the back-up from BackUpToolFor12_1Migration

CHAPTER 14

Maintaining the Server

Managing Log Files

Cisco Prime Collaboration Provisioning writes application log files for the Service Enabling Platform (SEP) module (sep.log), the Network Interface and Configuration Engine (NICE) service (nice.01.log), Unified CM AXL responses and requests, Unity Connection SQL queries, and Presence AXL information.

As an administrator, you can manage the log files using:

- Cisco Prime Collaboration Provisioning user interface, where the log files can be viewed and downloaded by navigating through **Administration** > **Logging and ShowTech**.

You cannot disable logging. However, you can:

- Collect more data when needed by increasing the logging level
- Return to the default logging level (NORMAL)

Following are the available logging levels:

- DETAIL
- NORMAL

- HIGH

The log files are backed up every hour, or when they reach their maximum log size limit. The default size limit is 20 Mb (see Changing the Maximum Log File Size). The files are saved in the format sep.log.date stamp timestamp.

The log files are deleted from the Cisco Prime Collaboration Provisioning server when their size exceeds 5000 MB or the number of log files in the logs folder exceeds 500. If you want to change these levels, see Changing the Log Purging Level.

Changing the Log Level (GUI)

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Logging and ShowTech**.

Step 2 In the **View and Set Logging Levels** pane, you can view the existing logging levels and change them to the desired level.

Following are the available logging levels:

- DETAIL (provides detailed log information and uses more disk space)
- NORMAL (provides the basic information)
- HIGH (provides high-level log information only)

Note By default, the log level is set to NORMAL. To view the Unified CM AXL responses and requests logs, the logging level must be set to Normal or Detail.

Step 3 Click **Save Settings**.

Changing the Maximum Log File Size

Procedure

Step 1 On the Cisco Prime Collaboration Provisioning system, go to the `opt/cupm/sep` folder.

If you accepted the default location during installation, the installation location is /opt/cupm.

Step 2 Open the dfc.properties file and change the dfc.log.maxsize property to the desired size (default is 20 Mb).

Step 3 Save the changes and restart the Provisioning services as your changes will not take effect until Cisco Prime Collaboration Provisioning is restarted. To restart:

a) Log into the server using SSH.

b) Go to /opt/cupm folder and execute the ./cupm-app-service.sh stop command.

c) Check whether the services are down by executing the following command:

```
ps -aef | grep startcupm
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
ps -aef | grep nice
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
```

d) Check if the port 46009 is free (used by JBoss):

```
netstat -a | grep 46009
```

If this port is in use, wait till it gets free.

Step 4 Start the application services:

```
execute ./cupm-app-service.sh start
```

Wait for the services to start.

Changing the Log Purging Level

Procedure

Step 1 On the Cisco Prime Collaboration Provisioning system, go to the `/opt/cupm/sep` folder. If you accepted the default location during installation, the installation location is /opt/cupm.

Step 2 Open the ipt.properties file, and do one or both of the following:

- To change the maximum file size level, update the dfc.purgelog.maxused_mb property to the desired level.
- To change the maximum number of log files level, update the dfc.purgelog.maxlogsaved property to the desired level.

Step 3 Save the changes, and restart the Cisco Prime Collaboration Provisioning services, as your changes will not take effect until Cisco Prime Collaboration Provisioning is restarted.

a) Log into the server using SSH.
b) Go to /opt/cupm folder and execute the ./cupm-app-service.sh stop command.
c) Check whether the services are down by executing the following commands:

```
ps -aef | grep startcupm
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
ps -aef | grep nice
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
```

d) Check if the port 46009 is free (used by JBoss):

```
netstat -a | grep 46009
```

If this port is in use, wait till it gets free.

Step 4 Start the application services:

```
execute ./cupm-app-service.sh start
```

Wait for the services to start.

Generating and Downloading Showtech Files

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Logging and ShowTech** .

Step 2 Click **Generate ShowTech**. The **Collect ShowTech** window opens.

Step 3 Enter the following information:

- File Name—Enter the file name as it is mandatory. By default, it is auto-populated as ShowTech-2014-12-01-012705.
- Duration—Select the duration
  - Range—By default, the date range is the server-installed date. You can modify this date but make sure the From date is greater than the server-installed date and the To date is lesser or equal to the current server time.
  - Last—You can select a relative duration with this option.
- Select Components—Select the required components. By default, all components are selected.

Step 4 Click **Start Collection** to collect the showtech information for the selected duration. Once the showtech collection is complete, you can see the showtech zip file generated in the table.

Step 5 Unzip the file to view the showtech information.

Browsing Logs

Cisco Prime Collaboration Provisioning allows you to launch and view the following logs for online troubleshooting:

- Application and NICE logs

Note By default, user name during login is case sensitive. If "Login user name is case-insensitive" setting is enabled, Cisco Prime Collaboration Provisioning will perform case insensitive authentication.

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Logging and ShowTech**.

Step 2 In the **Browse Logs** pane, click the Application and NICE Logs link. The logs are fetched from the server and you can view them on the browser for troubleshooting.

Step 3 (Optional) To download a log file:

a) In the Application and NICE Logs page, click the download icon for that file.

b) In the popup window, select the **Save File** option and click **OK**.

The log file is downloaded to your local machine.

Troubleshooting Account

For Cisco Prime Collaboration Provisioning 12.5 and later

When you log in to the Troubleshooting Account User login page for the second time, it displays the successful date and time of the previous login.

This feature enables you, as a user with full access, to create a troubleshooting account (**Administration > Logging and ShowTech**) from Cisco Prime Collaboration Provisioning to debug and monitor issues. In addition, you can use a troubleshooting user interface to debug and monitor the Cisco Prime Collaboration Provisioning server. The troubleshooting user interface displays details of logs, process management, DB Restore, memory usage, disk usage, and so on.

To create a troubleshooting account and launch the troubleshooting UI:

Before you begin

- The option to create a troubleshooting account is only available to a user with full access.
- As a troubleshooting user, you cannot delete your account.
- As a troubleshooting user, you cannot change your password.

- Only one troubleshooting account is valid per Cisco Prime Collaboration Provisioning server.

Note Only a privileged user can restart the three services (JBoss, NICE and Trouble shooting Service) and a user can be assigned privilege to restart only one service at any point of time.

Procedure

Step 1 Choose **Administration > Logging and ShowTech > Troubleshooting Account**.

Step 2 Enter the User ID with which you can login to the troubleshooting account. Valid values are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), space ( ), apostrophe, and at sign (@).

Step 3 Choose the number of hours the account should be active from the **Expires in** drop-down.

Step 4 Click **Create Account**.

Step 5 Click **Click to create email** to pass the account details to TAC to generate the password for the troubleshooting account that has been created.

Step 6 Once the account is created you can launch the Troubleshooting UI in two ways:

- Click **Go to Log In** and enter the credentials to login. You are redirected to **Cisco Prime Collaboration Provisioning - Troubleshooting** page where **Logs** menu is displayed by default.
- Through the **https://pcp-server-ip-address:28080/index** URL syntax. This option checks if the troubleshooting account already exists or not. If the account exists, you are redirected to the login page, and using troubleshooting user credentials you can access the menus. If the troubleshooting account does not exist, you are redirected to create an account.

Note Once you login into Cisco Prime Collaboration Provisioning as a troubleshooting user (choose **Troubleshooting** menu), you can either click **Launch** to launch the Troubleshooting UI or **SEP Admin** to launch the sep admin page.

You can also delete the troubleshooting account (**Delete Account**).

Managing System Settings

Cisco Prime Collaboration Provisioning allows you to manage various system settings through the Provisioning interface. It provides you the options to select or unselect the following feature settings:

- Analog Endpoint Support—This setting allows analog endpoints to be provisioned.
- Maintenance Mode Popup Notification—This setting, when enabled, gives a message to all logged in users when the system falls to maintenance mode.
- Allow orders in progress to be stopped after—This setting allow you to schedule time interval to stop the processing orders.
- **For Cisco Prime Collaboration Release 11.6 and later**

Disable 'globaladmin' account—This checkbox (**Administration > Settings > General**) is used to disable globaladmin user account.

Note This checkbox will be available only for users with full access. Once globaladmin account is disabled, you cannot undo and the checkbox is replaced with a green tick mark.

- Password Policy Settings—These settings allow you to manage your user passwords. Refer Managing User Passwords section for more information on password settings.
- Self-Care Feature Access Settings—These settings allow you to have access to all self-care features when you log into the self-care account. It is recommended not to disable these settings.
- **For Cisco Prime Collaboration Release 11.5 and later**

  Federal Information Processing Standard (FIPS)—This setting allows you to enable or disable FIPS. Refer Configure FIPS, on page 319 for more information on FIPS settings.
- **For Cisco Prime Collaboration Release 11.6 and later**

  Banner and Login Message—The **Administration > Settings > Banner and Login Message** setting enables you, as a user with Full Access privilege, to customize a banner on the login page, all pages of Cisco Prime Collaboration Provisioning, and self-care portal. You can define the classification text to be added for the reports or documents generated out of Cisco Prime Collaboration Provisioning.

  - The banner screen contains **Show Banner Message**, **Show Banner for Exported Reports** and **Show Login Message** checkboxes, which are disabled by default. When you select a checkbox, the appropriate banner is displayed.
  - You can customize the banner message using the appropriate **Color Scheme** and **Text Size** drop-down list.
  - You can classify any data using the banner, such as classifying the output of reports generated from Cisco Prime Collaboration Provisioning, classifying the output for sample batch files, and classifying the output for all log files. The following table lists the reports that are considered for classification.

Report	Report Type
Service Area	Print
Resource Configuration	Print
Service Configuration	Print
Directory Number Inventory	Print
Directory Number Block	Print
Endpoint Inventory	Export
Endpoint Line Mismatch	Export
Audit Trail	Export
Custom Reports	Export

Report	Report Type
Access Control	Export
Export Endpoints without associated users	Export

- You can customize your own messages, such as information of maintenance mode or application upgrade.

- **For Cisco Prime Collaboration Release 12.1 and later**

  Read-only and Security Changes—This feature enables you to list application users in Cisco Prime Collaboration Provisioning and supports Service Provisioning for the application users, mainly endpoint and line services. In addition, this feature enables you to add Controlled Devices to the application users.

  Check **Manage CUCM Application Users as Provisioning User** checkbox in Cisco Prime Collaboration Provisioning (**Administration > Settings**) to manage the application users. If the setting is enabled, the application user in Cisco Unified CM is synchronized in Cisco Prime Collaboration Provisioning and displayed on the **User Provisioning** page as a normal user. The devices associated to the application user in Cisco Unified CM are displayed in the customer record page

  Disable write access for North Bound API (Read-Only Allowed)—This checkbox (**Administration > Settings > General**) is used to disable write access for North Bound API and allows only get and list requests.

- **For Cisco Prime Collaboration Release 12.3 and later**

  Number of failed login attempts before locking account-- This setting allows the user to set the limits for the number of failed login attempts. The user can select the number from the drop-down list.

  Lock the user account-- This setting allows the user to select the time period for which the account will be locked after the number of failed login attempts exceeds the set limit. Temporarily and Permanently are the two options available.Temporarily is the default option. For upgraded system, the default option is Permanently.

  All user accounts will be unlocked after--- This setting allows the user to set a time period after which the account will be unlocked. In case of the Temporarily option, the user can select a value from the drop-down list. In case of the Permanently option, all the user accounts need to be unlocked manually. However, for globaladmin and the users of the Administration Group, the user can set the time period after which the account will be unlocked using the drop-down list.

Note By default, all system settings are enabled.

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration > Settings**.

Step 2 In the System Settings pane, check or uncheck the required check boxes and click **Update**.

Custom Settings

Custom settings are intended for debugging.

Note Restart the application, if a setting is removed.

Warning Do not try to configure any values in the Custom Settings text box as it is recommended only for Cisco Support. Setting an inappropriate value may cause the application to stop functioning.

Configure FIPS

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Provisioning supports the Federal Information Processing Standards (FIPS). The **Federal Information Processing Standard (FIPS)** option under **System Administration** > **Settings** is accessible only to the users with administrator privileges.

FIPS are U.S. government computer-security standards. The FIPS-140 series of standards specifies requirements for cryptography modules. For more information, see http://www.nist.gov/itl/fips.cfm.

Note By default, FIPS is disabled in Cisco Prime Collaboration Provisioning. The administrator can configure FIPS in the Cisco Prime Collaboration Provisioning server. Once the changes are updated, the system restarts automatically.

Before you proceed to enable or disable FIPS, ensure that:

- No active orders are in progress.
- No active batch projects are in progress.
- No synchronization in progress.
- The third-party CA signed certificates meet the FIPS approved encryption algorithm requirements.

You can perform the following actions:

To perform this action:	Do the following:
Enable FIPS	**1.** Choose **Administration** > **Settings**. **2.** Click **Federal Information Processing Standard (FIPS)**, and check the **Federal Information Processing Standard (FIPS)** check box. **3.** Click **Update**. **4.** Click **Yes** in the confirmation message box to continue, otherwise click **No** to return to the Settings page.
Disable FIPS	**1.** Choose **Administration** > **Settings**. **2.** Click **Federal Information Processing Standard (FIPS)**, and uncheck the **Federal Information Processing Standard (FIPS)** check box. **3.** Click **Update**. **4.** Click **Yes** in the confirmation message box to continue, otherwise click **No** to return to the Settings page.
Check FIPS status	**1.** Choose **Administration** > **Settings**. **2.** Click **Federal Information Processing Standard (FIPS)**, If the **Federal Information Processing Standard (FIPS)** check box is checked, FIPS is enabled otherwise it is disabled.

Process Management

For Cisco Prime Collaboration Release 11.1 and later

The **Process Management** menu enables you to restart the Cisco Prime Collaboration Provisioning application services from the user interface. This feature eliminates the need to log in as a root user into the system and restart the services.

Navigate to **Administration > Process Management** to view the **Process Management** page.

On the **Process Management** page, you can view the current state of the processes such as PostgreSQL, Apache, JBOSS, and NICE.

Also, you can restart individual or all the processes as follows:

- Restart All Processes—To restart all the processes such as Apache, JBOSS, PostgreSQL, and NICE, click **Restart All Processes**.
- Restart Individual Processes—To restart specific processes click the **Restart** against the respective process name. You can restart the process such as Apache, JBOSS, PostgreSQL, and NICE.
- Reboot Server—To reboot the Linux server and restart PCP Application, click **Reboot Server**.

In a distributed environment, you can reboot the Application server and restart services such as Apache, JBOSS, and NICE. The Reboot option is not available for the Database Server. However, you can restart PostgreSQL on the Database Server.

The **Process Management History** displays the restart history details such as the user who initiated the restart operation, process name, restart date, and reason for restart. Using restart history, you can analyze when, why, and who restarted the service. For services which are restarted automatically, the user is displayed as **System** and the reason is displayed as **Service restarted automatically**.

Note

- The **Process Management** page provides only static or snap-shot information about the processes. Refresh the **Process Management** page to know the status of the process. Click the refresh icon in the top left corner of the page to refresh the page.
- For all the operation except NICE restart, you are redirected to **Application Unavailable** page. On completion of the restart or reboot operation, you are redirected to the application **Login** page and the details are updated in the restart history table.
- For NICE, when you restart the process, instead of redirecting to the **Application Unavailable** page, the **Restart** button is disabled. The **Restart** button gets enabled automatically on completion of the restart operation and the details are updated in the restart history table.

Managing Localization Languages

As an administrator, you can upload a new language file or modify an existing language file and manage localization directly from the Cisco Prime Collaboration Provisioning interface.

To upload a new language file:

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Updates**. The Application Software Updates page shows a table with the list of supported languages for localization.

Step 2 Click **Add**. In the **Add a Language Pack** dialog box, choose a new language file and click **Upload**. If there is a new language pack for the existing language, you have an option to overwrite the same.
A popup appears saying that the new language pack is successfully uploaded.

Step 3 Change your browser settings to select a preferred language.

Step 4 Refresh the browser to see the changes to the Cisco Prime Collaboration Provisioning interface in your preferred language.

Certificates Supported in Cisco Prime Collaboration Provisioning

There are two types of certificates supported in Cisco Prime Collaboration Provisioning:

- LDAP certificates
- Provisioning application server certificates

LDAP certificates

LDAP certificate is the certificate from an external directory server to be used in Cisco Prime Collaboration Provisioning for secured communication. This certificate is imported into the Provisioning key store located in

`/opt/cupm/sep/dfc.keystore`

Provisioning application server certificates

Provisioning application server certificates provides an identity of the Cisco Prime Collaboration Provisioning server. The types are:

- Self-Signed—The identity certificate of the Cisco Prime Collaboration Provisioning server.
- CA-Signed—To obtain a CA–signed certificate, you must:
  1. Create a Certificate Signing Request (CSR)—A CSR is a block of encrypted text that is generated on the Cisco Prime Collaboration Provisioning server. It contains information such as your organization name, common name (domain name), locality, and country.
  2. Submit it to a Certificate Authority.
  3. Obtain the signed certificate
  4. Import the CA certificates from **Administration > Updates**.

Managing SSL Certificate

For Cisco Prime Collaboration Release 11.1 and later

Cisco Prime Collaboration Provisioning enables the administrator to generate and download SSL (Secure Socket Layer) certificates. Using these certificates you can eliminate browser security warnings and secure your internet communication.

To view the existing SSL certificates, navigate to **Administrator > Updates**. In the **SSL Certificate** pane, you can view the list of existing certificates along with its type, expiry date, and usage (LDAP or Provisioning Web Access) details. The expiry date is displayed only for signed certificates.

In addition, you can perform the following operations in the **SSL Certificate** pane:

Note You must have the administrator privilege to perform these tasks.

- Generate CSR(Certificate Signing Request)—For steps to generate a CSR, refer Generate CSR, on page 323. You can have only one CSR in the system. So, when you generate a CSR, it overwrites the old CSR.
- Upload certificate—You must get the generated CSR signed from the CA (Certificate Authority) and upload the signed certificate. You can also upload LDAP certificate. For steps to upload the SSL certificate, refer Upload SSL Certificate, on page 326.
- View certificate—To view the certificate contents, click the required certificate name and click **View**.
- Download—To download the certificate, click the required certificate name and click **Download CSR**.
- Delete—To delete a certificate, click the required certificate name and click **Delete**. You can delete only LDAP certificate.

Generate CSR

To generate a CSR :

Before you begin

You must have administrator privilege to perform this task.

Note The CSR generated from the Cisco Prime Collaboration Provisioning user interface does not include alternate names. To generate a CSR with alternate names using CLI, refer to Generate CSR with Alternate Names, on page 324.

Procedure

Step 1 Choose **Administration** > **Updates**.

Step 2 In the SSL certificate pane, click **Generate CSR**.

Step 3 Enter the required details in the **Generate Certificate Signing Request** window. An asterisk next to a field indicates a mandatory field. Refer Table 68: Generate CSR Fields, on page 324 for field description.

Step 4 Click **Generate** to generate the CSR. The generated CSR is added to the top of the table.

Note Generated CSR overwrites any existing CSR.

- The default value for Key Length is 2048 bits.
- The default value for Hash Algorithm is SHA256.

Table 68: Generate CSR Fields

Field	Description
Certificate Name	Name of the certificate.
Country Name	Two-letter ISO abbreviation of your country.
State or Province	State or Province where the organization is located.
Locality Name	City where the organization is located.
Organization Name	Name of the organization.
Organization Unit Name	Section of the organization.
Common Name	Fully qualified domain name.
Email Address(Optional)	Email address to contact the organization.

Generate CSR with Alternate Names

Perform the following steps to create a Certificate Signing Request (CSR) with alternate names. The CSR with alternate names allows you to access Cisco Prime Collaboration Provisioning with multiple Domain Name Server (DNS) entries using the same certificate.

Before you begin

Obtain the following:

- Certified Authority (CA) signed Cisco Prime Collaboration Provisioning certificate.
- Root access to the Cisco Prime Collaboration Provisioning CLI.

Note For Cisco Prime Collaboration Provisioning 12.x and above:

- Contact TAC for CLI access.
- Prefix all the commands that are executed as a console account user with **Sudo**.

Procedure

Step 1 Log in to PCP as the root user.

Step 2 Enter the command, **cd /opt/cupm/httpd/** to navigate to the httpd folder.

Step 3 Enter the command, **vi san.cnf** to create a new blank file, **san.cnf**.

Step 4 Press the I key to edit the san.cnf file.

Step 5 Copy and paste the following text in the file:

```
[req]
default_bits         = 2048
distinguished_name   = req_distinguished_name
req_extensions       = req_ext
[req_distinguished_name]
countryName          = Country Name (2 letter code)
stateOrProvinceName  = State or Province Name (full name)
localityName         = Locality Name (eg, city)
organizationName     = Organization Name (eg, company)
commonName           = Common Name (e.g. server FQDN or YOUR name)
[req_ext]
subjectAltName       = @alt_names
[alt_names]
DNS.1 = pcptest23.cisco.ab.edu
DNS.2 = pcptest.gov.cisco.ca
```

Where:

- DNS.1 = Primary DNS
- DNS.2 = Secondary DNS

You can access the PCP using either of these DNS entries.

Step 6 Enter the commands, **esc** followed by **:wq!** to save the file.

Step 7 Restart all the services for the config file:

a. Enter the command, **/opt/cupm/bin/cpcmcontrol.sh stop** to stop the services.

b. Enter the command, **/opt/cupm/bin/cpcmcontrol.sh status** to verify that all the services have stopped.

c. Enter the command, **/opt/cupm/bin/cpcmcontrol.sh start** to restart all the services.

Step 8 Enter the command, **pwd** to verify that your current directory is **/opt/cupm/httpd/**.

Step 9 Enter the following command to generate the Private key and CSR:

openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout PCPSAN.key -config san.cnf

```
[root@ryPCP11-5 httpd]# openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout
private.key -config san.cnf
Generating a 2048 bit RSA private key
.........+++
.........+++
writing new private key to 'private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields, but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:TX
Locality Name (eg, city) []:RCDN
Organization Name (eg, company) []:CISCO
Common Name (e.g. server FQDN or YOUR name) []:doctest.cisco.com
[root@ryPCP11-5 httpd]#
```

Step 10 Enter the following command to verify if the CSR contains the correct alternate names:

openssl req -noout -text -in PCPSAN.csr | grep DNS

```
[root@ryPCP11-5 httpd]# openssl req -noout -text -in PCPSAN.csr | grep DNS
DNS:pcptest23.cisco.ab.edu,
DNS:pcptest.gov.cisco.ca [root@ryPCP11-5 httpd]#
```

Step 11 Move the .csr from the PCP server to your desktop.

Step 12 Use an FTP client to connect to PCP as the root user and navigate to the `/opt/cupm/httpd/` directory.

Step 13 Sign the CSR with your CA using a windows server or online.

Step 14 Log in to the PCP server and navigate to **Administration** > **Updates** > **SSL Certificates** to install the PCP Certificate.

Step 15 Install the required browser certificate. Clear the cache and close the browser window.

Step 16 Log in to the PCP server to verify that the security error is not displayed.

Upload SSL Certificate

You can upload either LDAP or provisioning SSL certificate.

To upload SSL certificate:

Before you begin

You must have administrator privilege to perform this task.

Procedure

Step 1 Choose **Administration** > **Updates** .

Step 2 In the **SSL Certificate** pane, click **Upload** and choose **LDAP** or **Provisioning Certificate**.

Step 3 In the **Upload LDAP/Provisioning Certificate** dialog box, browse through the local file system and choose the required file.

Note The valid certificate file formats are .crt and .cer for provisioning certificate and .cer for LDAP certificate.

Step 4 Click **Upload**. The uploaded certificate is added to the top of the table.

After uploading the certificate, you must restart the server to activate the certificate.

Based on the type of the uploaded certificate, restart the server as follows:

- LDAP certificate—restart provisioning server.
- Provisioning certificate:
  - restart apache server.
  - from Troubleshooting UI "Restart all processes" must be done to apply the certificate for Troubleshooting UI.

Note To upload TLS 1.2 certificates, follow the same steps as above.

Cisco Prime Collaboration Provisioning does not support chained certificates.

Note A certificate chain is a sequence of certificates, where each certificate in the chain is signed by the subsequent certificate. The purpose of a certificate chain is to establish a chain of trust from a peer certificate to a trusted CA certificate.

Managing Endpoints

Using Cisco Prime Collaboration Provisioning , you can upload new and existing endpoints through the user interface. You can add or update endpoints by uploading the endpoint files (valid zip file containing list of supported endpoints). The endpoint bundle eliminates the need to login as root into the system and restart services. The details about endpoints are automatically updated in the table based on the endpoints added to Cisco Prime Collaboration Provisioning. The Endpoint Bundles pane displays a table with the list of endpoints that are available in the system and its supported Cisco Unified Communications Manager versions. To manage endpoints:

Note The endpoint zip files are available on Cisco.com.

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Updates**. The **Endpoint Bundles** pane displays a table with the list of endpoints that are available in the system and its supported Cisco Unified CM versions.

Unified Communications Manager versions are automatically updated in the table based on the endpoints added to Provisioning.

Step 2 Click **Add** and in the **Add Endpoint Bundles** dialog box, browse for the appropriate zip file and click **Upload**.

A warning message appears with the details of number of endpoints that are to be added to the endpoint bundle table.

Step 3 To proceed with the process, click **Continue**. The new/updated endpoints are included to the system and the user can be provisioned with the new endpoints immediately without a restart.

Note When you update the existing endpoints, a warning message is displayed stating how many endpoints and what endpoints are going to be updated.

Enabling Data Purging for Provisioning

You can configure Cisco Prime Collaboration Provisioning to purge data at a scheduled interval.

Cisco Prime Collaboration Provisioning retains the following types of data:

- Order—When an order is placed for any product provisioning (for example: endpoint, line, voicemail or any bundle), an order data object is created and stored in the system.
- ServiceAction—Objects that are created when the application is communicating with the device during product provisioning. By default, purging of Service Action data is enabled.
- Task—Scheduling of infrastructure configuration updates. Through Infrastructure Configuration you can save configurations locally. The saved configurations can then be bundled in a Task and pushed to the device.
- Workflow—After an order is placed for a product, it goes through a workflow (approval, shipping, and receiving) before going to the service activator.
- Audit Trail—An audit entry is created for every PIN or Password change, PIN or Password reset, PIN or Password change on next login, unlock voice mail of a user in a Unity or Unity Connection device, login management, user management, pin or password management, changes in access control group and user roles, self-care, system settings, and synchronization. By default, purging of Audit Trail data is enabled.

Note Data is purged when the retention time or retention count criterion is met. For example, if the data is older than the retention time it will be removed. Also, if the data amount exceeds the retention count, it will be removed.

Procedure

Step 1 Choose **Administration > Data Maintenance** . (See Table 1 for navigation in the Cisco Prime Collaboration Provisioning application.)

Step 2 Check the check box in the row for the data you want to schedule for purging.

Step 3 In the **Retention Time in Days** column, change the number of days for which you want to retain the data (default is seven days except for Audit Trail and ServiceAction, which is 30 days).

Step 4 In the **Retention Count** column, select the amount of data that you want to retain.

Note Retention count is the number of objects that you want Provisioning to keep and not purge. For example, if there are 1000 total orders and the retention count is 200, Provisioning will purge 800 orders and keep the last 200 orders.

The default settings for the Retention Count are:

- Orders—latest 100 orders
- ServiceAction—Unlimited
- Task—50
- Workflow—50
- **(For Cisco Prime Collaboration Release 11.2 and earlier)** Audit Trail—50
- **(For Cisco Prime Collaboration Release 11.5 and later)** Audit Trail—100,000

  Note 1000K is the maximum retention count that can be set for the audit trail.

Step 5 (Optional) To export the purged data to a file before it is removed, in the Export Before Purge field select **Yes**. .

Only Orders and Workflow data is exported. Service action data cannot be exported.

Step 6 Select a purge interval (the default is 24 hours), and click **Update.**

The Purging Information pane displays the time of the next scheduled purge and the last purge.

To purge Provisioning data, choose **Administration > Data Maintenance** (In the Cisco Prime Collaboration Provisioning application, choose **Administration > Data Maintenance**). You can provide the data in the Data Maintenance Configuration page.

Note During 12.1 migration, the purged data is not copied to the 12.1 server automatically. If 11.x server purged data is required, then these files must be copied manually.

Maintenance Mode

You can put Cisco Prime Collaboration Provisioning into maintenance mode to perform user-impacting actions that are not available in normal mode, such as deleting Domains, processors, and Service Areas.

Any user other than administrator will be able to access all non Provisioning pages as per the roles assigned to him. Though Provisioning links are available, when user tries to access these pages, a message appears indicating that the application is currently in Maintenance mode.

Note The user needs to log off from the application mode, and re-login to the maintenance mode, for the maintenance mode rules to be applicable.

Procedure

Step 1 Choose **Administration** > **Maintenance Mode** .

The Application Mode Management page appears with the following message:

Exiting Maintenance mode will restore access to all users. Delete operations on processors (Call Processors, Unified Message Processors), LDAP and ACS Servers, Domains, and Service Areas will no longer be available.

Step 2 Select a time delay from the **Delay Before Maintenance Mode Begins (mins)** drop-down list. You can select a time delay between 1 minute to 60 minutes. To put Cisco Prime Collaboration Provisioning to maintenance mode immediately, select **Immediately.**

Step 3 In **Message to Display to Logged-in Users**, enter a message. This message will appear on the screens of the logged-in users. You can enter a maximum of 200 characters.

Step 4 Click **Enter Maintenance Mode**, and then click **Yes** to confirm.

A warning appears on the login page, notifying users that the system use is limited to users with administrative privileges. Maintenance options that are not available in normal mode, such as deleting Domains, become available.

Step 5 Perform any maintenance activities, such as deleting a Domain.

Step 6 When you have completed the maintenance activities, select **Maintenance Mode**.

Step 7 Click **Exit Maintenance Mode**.

The warning on the login page is removed and users can now log in as usual. Maintenance options such as deleting Domains are no longer available.

An email notification will be sent to all the administrators when Cisco Prime Collaboration Provisioning is going into maintenance mode. The following notification event must be enabled to send an email notification:

When system enters or exits Maintenance Mode (email will be sent to the logged in administrators)

To configure notification settings, see Configuring System Notifications, on page 305

Backup and Restore

Cisco Prime Collaboration Provisioning allows you to backup your data and restore it. You can schedule periodic backups using the Provisioning UI (Schedule Backup Using the Provisioning User Interface, on page 331).

Note **For upgrading Cisco Prime Collaboration Provisioning 12.4 and later releases**

In Cisco Prime Collaboration Provisioning 12.4, backup and restore requires a mandatory password for enhanced security. Hence, after the upgrade to 12.4, all scheduled backup jobs from 12.x fail. Once upgrade from 12.x to 12.4 is complete, you can cancel all the previously scheduled and saved jobs. The admin has to either reset the password and schedule the backup again or delete the scheduled backup job and reschedule it on 12.4. You can view the upgrade logs for the appropriate message.

There are two backup and restore scenarios; select the set of procedures that matches your scenario:

- Backup and restore with the same installation or a new installation. For this scenario, see Schedule Backup Using the Provisioning User Interface, on page 331.

Note When backing up files, place the files on a different file server. Also, burn the backup data onto a CD.

Cisco Prime Collaboration Provisioning allows you to back up system data and restore it on a different system in the event of total system failure. To restore the backup from another system, the following prerequisites must be met:

- Ensure that the server to which data is restored has the same MAC address as that of the system that was backed up (the IP address and the hostname can be different).
- If you are unable to assign the MAC address of the original system (the one that was backed up) to another system, contact the Engineering Team for information on a new license file (for a new MAC address).
- The procedure to backup and restore data on a different system is the same as the procedure to backup and restore data on the same system.

Schedule Backup Using the Provisioning User Interface

You can create periodic backups of the Provisioning database using the Provisioning User Interface. You must be logged in as an administrator to perform the backup.

Before you begin

The prerequisites for a successful SFTP backup for a non-root user are as follows:

- The backup folder is manually created in advance.
- The backup folder has the group or owner as root.
- The backup folder has the correct read and write permissions.

Before performing the upgrade, ensure to take a snapshot of the existing setup.

Procedure

Step 1 Choose **Administration** > **Backup Management**.

Step 2 In the Backup Management page, click **New.**

Step 3 Enter a backup title in the Create New Backup page.

Step 4 From the Backup Connection drop-down list, select SFTP, FTP, or Local to save your backup files.

a) If you select SFTP or FTP, provide the following details:

- IP address of the server where the backup files need to be saved.

- Path to the backup location and port details (for SFTP only).

  Note The backup location is relative to the specified SSH user home directory. The relative path must contain directory details (for example DIRNAME or DIRNAME 1 / DIRNAME 2), to avoid backup in root directory.

- Username and password information. Testing the SFTP or FTP password is optional.

Note Taking backup through SFTP on another PCP server in FIPS mode is not supported.

b) If you select Local, the backup files are saved to the CUPM local directory.

Note Ensure that the destination path for SFTP, FTP, or Local is not given as “opt/backup”

Note If backup fails, verify whether the temporary backup folder "**backup**" is present at /opt. If present, delete it:

a. Create a console account from the troubleshooting web application.

b. Log in to console and delete the content of the /opt/backup folder and then the backup folder.

c. Trigger the backup again.

Step 5 For a local backup, select the number of backup files you want to save on your local machine from the Backup History drop-down list.

The default value is 2. By default, you can save two recent backup files. You can save up to 9 recent backup files.

Step 6 Enter the scheduling details to schedule a backup.

The time displayed is the server browser time. The default recurrence type for a new backup job is None. After a backup job is created with default settings, the backup will start immediately.

Step 7 Enter email address to receive status notification for the scheduled backup. You can enter multiple email addresses separated with a comma.

Step 8 Click Save. The scheduled backup appears in the Backups table on the Backup Management page.

Step 9 Click Run Now, to run a backup immediately.

Prime Collaboration Provisioning enters maintenance mode before backup starts. A notification will be displayed for all logged-in users stating that the users will be logged out of Prime Collaboration Provisioning 10 minutes before the scheduled backup starts. Users must save their work and log out before the backup starts, else they will be logged out automatically, and will not be able to access Prime Collaboration Provisioning.

The backup table provides information on the status and history of each backup job. The Next Run Time option provides details on the next periodic schedule.

The Last Run Status column shows the status of the last run backup job. The status of a backup job can be Scheduled, In Progress, Success or Failed.

When a backup job reaches the scheduled time, the last run status changes to Scheduled. After entering into maintenance mode, that is after 10 minutes, the status will change from Scheduled to In Progress.

After the backup job is complete, the status is either Success or Failure.

To know about the history of any backup job, click **Run History Count**, and open the dialog box. You can view the start time, end time, status and file size of the backup. You can delete the run history logs. The backed up files are not deleted when the backup logs are deleted.

Managing Backup Jobs

With the scheduled jobs, you can:

- Edit and Delete: The Edit and Delete options are disabled during Scheduled and In Progress states. You cannot edit or delete a backup job when the backup is in Scheduled or In Progress state. You can edit only one backup job at a time.
- Cancel: You can cancel a running backup job which is in Scheduled or In Progress state only.

Back Up Provisioning Database from Console CLI — 11.x and below

This procedure requires that you have administrator level access to the Provisioning database (the PostgreSQL database).

Procedure

Step 1 Login as troubleshooting user using SSH with port 22

Step 2 Navigate to the **/opt/cupm** folder and enter the following command:

```
sudo ./cupm-app-service.sh stop
```

Step 3 Stop Apache, JBoss, and NICE Services using the following commands:

```
ps -aef | grep startcupm
ps -aef | grep nice
kill -9 <startcupm process ID>
kill -9 <nice process ID>
```

Step 4 Go to the directory using the command:

```
cd /opt/postgres/pghome/bin
```

Step 5 Run the following command:

```
sudo ./pg_dumpall -o -Upmadmin > /<backup_directory_name>/<backup_file_name>
```

where,

- *pmadmin*—postgres user id
- *backup_directory_name*— For sudo user, the directory name is **/home/<sudo User directory>**. For Example: If sudo user is 'testuser' , directory name will be /home/testuser/
- *backup_file_name*—Backup will be created with this file name.

Step 6 In a backup folder, make copies of the following files and directories:

- /opt/cupm/sep/dfc.properties
- /opt/cupm/sep/ipt.properties
- /opt/cupm/sep/dfc.keystore
- /opt/cupm/jboss/server/cupm/conf/login-config.xml
- /opt/cupm/jboss/server/cupm/deploy/dfc-ds.xml
- /opt/cupm/sep/ipt/.system/.pcprandom.key

Step 7 Start Apache, JBoss, and NICE Services using the following commands:

```
cd /opt/cupm
sudo ./cupm-app-service.sh start
```

APPENDIX A

Provisioning Attributes

Provisioning Attribute Description in Batch Help

You can access the provisioning attributes and their descriptions from the Batch help feature available in Cisco Prime Collaboration Provisioning 11.0 user interface and later.

1. Log in to the Cisco Prime Collaboration server.
2. Choose **Advanced Provisioning > Batch Provisioning**.
3. Click the Batch Help icon at the top right corner of the Batch Provisioning page. The Batch Action Help link opened in a new tab displays the attributes and description for different services.

Note To set a service template as default created by batch service, you need to use attribute 'ServiceArea and UserRole' as below.

ServiceArea and UserRole - SA:Employee:Yes , where:

- SA : Service Area
- Employee : User Role
- Yes : Default

APPENDIX B

Infrastructure Configuration Product Fields

Infrastructure Data Object Fields

To create Configuration Templates, you must add infrastructure Configuration Products to the Configuration Template.

Not all fields in an infrastructure configuration template are applicable on all Cisco Unified Communications Manager versions.

Note All the Infrastructure Configuration Product fields, where you manually enter text, are case sensitive.

CTI Route Point Configuration Product Fields

Table 69: CTI Route Point Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Device Pool	List of available device pools. The device pool specifies a collection of properties for this device, including Unified CM Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Common Device Config	Configuration of common device settings, such as the softkey template and user locale.
Call Search Space	Specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed.

Field	Description
Location	Specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the location feature does not keep track of the bandwidth that this route point consumes.
Directory Numbers	Enter directory numbers. These directory numbers must not exist on the Cisco Unified Communications Manager.
Route Partition for Directory Numbers	Available route partitions.
Media Resource Group List	Provides 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 according to the priority order that is defined in a Media Resource Group List. If this field is left blank, the Media Resource Group that is defined in the device pool is used.
User Locale	User location associated with the user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
User Hold MOH Audio Source	The audio source that plays Music On Hold when the user initiates a hold action.
Network Hold Audio Source	The audio source that plays when the network initiates a hold action.

Call Park Infrastructure Configuration Product Fields

Table 70: Call Park Infrastructure Configuration Product Fields

Field	Description
Number/Range	Enter the call park extension number or a range of numbers. **Note** Call Park template allows you to add the same range of numbers in different partitions.
Description	Optional description.
Route Partition	List of available route partitions.

Field	Description
Unified CM	List of available Cisco Unified Communications Managers.

Call Pickup Group Infrastructure Configuration Product Fields

Table 71: Call Pickup Group Infrastructure Configuration Product Fields

Field	Description
Call Pickup Group Information	
Name	Infrastructure Configuration Product name.
Number	Unique directory number (integers).
Description	Optional description.
Route Partition	List of available route partitions.
Call Pickup Group Notification Settings	
Call Pickup Group Notification Policy	From the drop-down list box, choose one of the following notification types: • No Alert • Audio Alert • Visual Alert • Audio and Visual Alert
Call Pickup Group Notification Timer (seconds)	Enter the seconds of delay (integer in the range of 1 to 300) between the time that the call first comes into the original called party and the time that the notification to the rest of the call pickup group is to occur.
Associated Call Pickup Group Information - Find Pickup Numbers by Numbers/Partition	
Partition	See Partition in Call Pickup Group Information in this table.
Call Pickup Group Numbers Contain	Enter the DN or part of the DN of the call pickup group that you want to find; then, click Find.
Available Call Pickup Groups	To add a member to the associated call pickup group list in the Current Associated Call Pickup Groups area.
Associated Call Pickup Group Information - Current Associated Call Pickup Groups	

Field	Description
Selected Call Pickup Groups	To change order of the Call Pickup Groups listings, use the Up and Down arrows on the right side of this box to move the listings.
Removed Call Pickup Groups	Use the Up and Down arrows above this box to move a call pickup group from this box to the Selected Call Pickup Groups box.
Call Information Display For Call Pickup Group Notification	
Calling Party Information	Check the check box if you want the visual notification message to the call pickup group to include identification of the calling party.
Called Party Information	Check the check box if you want the visual notification message to the call pickup group to include identification of the original called party.

Call Search Space Infrastructure Configuration Product Fields

Table 72: Call Search Space Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Available Route Partitions	List of available route partitions. The route partitions list is not strictly required, but you should provide at least one value. You must reference a route partition that already exists on the Cisco Unified Communications Manager, or define one in the same Configuration Template before to this call search space.

Called Party Transformation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 73: Called Party Transformation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Pattern	Enter the transformation pattern, including numbers and wildcards (do not use spaces).

Field	Description
Partition	Choose the desired partition to restrict access to the transformation pattern from the drop-down list box.
Description	Optional description.
Numbering Plan	Choose a numbering plan.
Route Filter	Choosing an optional route filter restricts certain number patterns.
Urgent Priority	Check this check box to interrupt interdigit timing and route the call immediately.
MLPP Preemption Disabled	Check this check box to make the numbers in a transformation pattern nonpreemptable.
Called Party Transformation	
Discard Digits	Choose the discard digit instructions that you want to be associated with this calling party transformation pattern.
Called Party Transformation Mask	Enter a transformation mask value.
Prefix Digits	Enter the prefix digits.
Called Party Number Type	Choose the format of the number type in called party directory numbers.
Called Party Numbering Plan	Choose the format of the numbering plan in called party directory numbers.

Calling Party Transformation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 74: Calling Party Transformation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Pattern	Enter the transformation pattern, including numbers and wildcards (do not use spaces).
Partition	choose the desired partition to restrict access to the transformation pattern from the drop-down list box.
Description	Optional description.

Field	Description
Numbering Plan	Choose a numbering plan.
Route Filter	Choosing an optional route filter restricts certain number patterns.
Urgent Priority	Check this check box to interrupt interdigit timing and route the call immediately.
MLPP Preemption Disabled	Check this check box to make the numbers in a transformation pattern nonpreemptable.
Calling Party Transformations	
Using calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Discard Digit Instructions	Choose the discard digit instructions that you want to be associated with this calling party transformation pattern.
Calling Party Transformation Mask	Enter a transformation mask value.
Prefix Digits	Enter the prefix digits.
Calling Line ID Presentation	Used as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis.
Calling Party Number Type	Choose the format of the number type in calling party directory numbers.
Calling Party Numbering Plan	Choose the format of the numbering plan in calling party directory numbers.

Common Device Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 75: Common Device Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Softkey Template	Softkey template that determines the configuration of the softkeys on Cisco IP Phones.
User Hold MOH Audio Source	The audio source that plays Music On Hold when the user initiates a hold action.

Field	Description
Network Hold Audio Source	The audio source that plays when the network initiates a hold action.
User Locale	User location associated with the user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
IP Addressing Mode	Choose the version of IP address that the device (SIP trunk or phone that runs SCCP) uses to connect to the system.
IP Addressing Mode Preference for Signaling	For dual-stack phones, which support both IPv4 and IPv6 addresses, choose the version of IP address that the phone prefers to establish a connection to the system during a signaling event.
Use Trusted Relay Point	Choose one of the following options: • On—To allow the IP Phones to send multicast echo request messages. • Off—To disable sending multicast echo request messages. • Default—To use the configuration for the Reply Multicast Echo Request enterprise parameter, choose this option.
Use Intercompany Media Services (IMS) for Outbound Calls	Check this check box to enable the devices that associate with this common device configuration to use a trusted relay point.

Field	Description
Allow Auto-Configuration for Phone	This drop-down list box supports IPv6 for dual-stack Cisco Unified IP Phones that run SCCP: • On—Depending on how the M bit is set through stateless address autoconfiguration on the router, the phone is allowed to use the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address. Phones also require a TFTP server address to register with the system. You can manually configure the TFTP server address through the interface on the phone, or you can obtain it from a DHCPv6 server. • Off—The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server. • Default—To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option.
Allow Duplicate Address Detection	This drop-down list box supports an IPv6 parameter for Cisco IP Phone: • On—The phone performs duplicate address detection on each of the addresses in all the identity associations that it receives in the Reply message. • Off—The phone does not perform duplicate address detection. • Default—To use the configuration for the Allow Duplicate Address Detection enterprise parameter, choose this option.
Accept Redirect Messages	This drop-down list box supports an IPv6 parameter for Cisco IP Phones: • On—The phone accepts the redirect messages from the same router that is used for the destination number. • Off—The phone ignores the redirect messages. • Default—To use the configuration for the Accept Redirect Messages enterprise parameter, choose this option.

Field	Description
Reply Multicast Echo Request	This drop-down list box supports an IPv6 parameter for Cisco IP Phones: • On—The phone sends an Echo Reply message in response to an Echo Request message sent to an IPv6 address. • Off—The phone does not send Echo Reply messages. • Default—To use the configuration for the Reply Multicast Echo Request enterprise parameter, choose this option.
MLPP Indication	Specifies whether devices in the device pool that are capable of playing precedence tones use the capability when the devices place an MLPP precedence call.
MLPP Preemption	Specifies whether devices in the device pool that are capable of preempting calls in progress use the capability when the devices place an MLPP precedence call.
MLPP Domain	Multilevel Precedence and Preemption (MLPP) Domain that is associated with this device.
Confidential Access Mode	Select one of the following options to set the CAL mode: • Fixed—CAL value has higher precedence over call completion. • Variable—Call completion has higher precedence over CAL level.
Confidential Access Level	Select the appropriate CAL value.

Common Phone Profile Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 76: Common Phone Profile Infrastructure Configuration Product Fields

Field	Description
Common Phone Profile Information	
Name	Enter a name to identify the common phone profile; for example, CPP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.

Field	Description
Description	Identify the purpose of the common phone profile; for example, common phone profile for the 7905 phone. 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 (<>).
Local Phone Unlock Password	Enter the password that is used to unlock a local phone. Valid values comprise 1 to 15 characters.
DND Option	When you enable Do Not Disturb (DND) on the phone, this parameter allows you to specify how the DND features handle incoming calls: • Call Reject—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. • Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so that you can accept the call. **Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

Field	Description
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • Disable—This option disables both beep and flash notification of a call, but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display, and no information gets sent to the device. • Beep Only—For an incoming call, this option causes the phone to beep. • Flash Only—For an incoming call, this option causes the phone to display a flash alert.
Enable End User Access to Phone Background Image Setting	Check this check box to change the background image on phones that use this common phone profile.
Feature Control Policy	You can choose a feature control policy that has already been configured in the Feature Control Policy configuration.
Wi-Fi Hotspot Profile	Select a Wi-Fi Hotspot Profile from the drop-down list.
Secure Shell Information	
Secure Shell User	Enter a user ID for the secure shell user. The Engineering Team uses secure shell for troubleshooting and debugging. Contact the Engineering Team for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH credentials to the phone in the clear.
Secure Shell User Password	Enter the password for a secure shell user. Contact the Engineering Team for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH passwords to the phone in the clear.

Field	Description
Phone Personalization Information	
Phone Personalization	The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. From the Phone Personalization drop-down list box, choose one of the following options: • Disabled—You cannot customize the Cisco Unified IP Phone by using Phone Designer. • Enabled—You can use Phone Designer to customize the phone. • Default—The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window. Install and configure Phone Designer to customize the phone. Before that, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer documentation. For more information on Phone Designer, see the Phone Designer documentation.
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Services Provisioning	From the drop-down list, choose how the phone will support the services: • Internal—The phone uses the phone configuration file to support the service. Choose this option or Both for Cisco-provided default services where the Service URL has not been updated; that is, the service URL indicates Application:Cisco/<name of service>; for example, Application:Cisco/CorporateDirectory. Choose Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file. • External URL—Choosing External URL indicates that the phone ignores the services in the phone configuration file and retrieves the services from a Service URL. If you configured a custom Service URL for a service, choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the phone. • Both—Choosing Both indicates that the phone support both the services that are defined in the configuration file and external applications that are retrieved from custom service URLs. If you have phones in your network that can obtain the service information from the phone configuration file and phones in your network that can only use custom service URLs for obtaining the information, choose **Both**.
VPN Information	
VPN Group	From the drop-down list, choose the VPN Group for the phone. For information about creating VPN groups, see the Virtual Private Network Configuration chapter in the Cisco Unified Communications Manager Security Guide.
VPN Profile	From the drop-down list, choose the VPN profile for the phone. For information about creating VPN profiles, see the Virtual Private Network Configuration chapter in the Cisco Unified Communications Manager Security Guide.
Service Specific Configuration Layout	

Field	Description
Disable USB	Disable the USB ports on the device and dock. This is a required field. Default: False **Note** A reset of the device is required for this parameter to take effect.
Back USB Port	Indicates whether the back USB port on the phone is enabled or disabled. This is a required field. Default: Enabled
Side USB Port	Indicates whether the side USB port on the phone is enabled or disabled. This is a required field. Default: Enabled
Enable/Disable USB Classes	Indicates which the USB Classes on the phone are enabled or disabled. Default: Audio Class
SDIO	Indicates whether the SDIO device on the phone is enabled or disabled. This is a required field. Default: Disabled
Bluetooth	Indicates whether the Bluetooth device on the phone is enabled or disabled. This is a required field. Default: Enabled
Bluetooth Profiles	Indicates which bluetooth profiles on the phone are enabled or disabled. This is a required field. Default: Handsfree
Allow Bluetooth Contacts Import	Indicates whether the Bluetooth device on the phone is allowed to sync the contacts from the phone. This is a required field. Default: Enabled

Field	Description
Allow Bluetooth Mobile Handsfree Mode	Indicates whether the user is allowed to enable or disable 2 way audio between devices with HFP. This is a required field. Default: Enabled
Console Access	Indicates whether the USB serial console is enabled or disabled. This is a required field. Default: Disabled
Cisco Camera	Indicates whether the Cisco Camera on the phone is enabled or disabled. This is a required field. Default: Disabled
Enable Power Save Plus	To enable the Power Save Plus feature, select the day(s) that you want the phone to power off on schedule. You can select multiple days by pressing and holding the Control key. while clicking on the days that you want Power Save Plus to operate. The default is disabled (no days selected). Power Save Plus mode turns off the phone for the time period specified in the Phone Off Time and Phone On Time fields. This time period is usually outside of your organization's regular operating hours. Power Save Plus mode turns on the phone automatically when Phone On Time arrives. When you select day(s) in this field, the following notice displays to indicate e911 concerns. By enabling Power Save Plus, you are agreeing to the terms specified in this Notice. While Power Save Plus Mode is in effect, endpoints configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: • You are taking full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect. • Cisco has no liability with your selection of the mode and all liability with enabling the mode is your responsibility. • Users should be aware of the effects of the mode on calls, calling and otherwise.

Field	Description
Enable Audible Alert	This check box, when enabled, instructs the phone to play an audible alert ten minutes prior to the time specified in the field, Phone Off Time. To also audibly alert the user, enable this check box. The default is disabled. This check box only applies if the Enable Power Save Plus list box has one or more days selected. This is a required field. Default: False
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. A few conditions apply; first, one or more days must be selected in the Enable Power Save Plus field. If the Enable Power Save Plus list box does not have any days selected, the phone ignores the EnergyWise directive to turn off the phone. Second, the settings in Unified CM Administration takes effect on schedule even if EnergyWise sends an override. For example, assume the Display Off Time is set to 22:00 (10 p.m.), the value in the Display On Time field is 06:00 (6 a.m.), and the Enable Power Save Plus has one or more days selected. If EnergyWise directs the phone to turn off at 20:00 (8 p.m.), that directive will remain in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6 a.m. At 6 a.m., the phone will turn on and resume receiving its power level changes from the settings in Unified CM Administration. To change the power level on the phone again, EnergyWise must reissue a new power level change command. Also, any user interaction will take effect so if a user presses the select softkey after EnergyWise has directed the phone to power off, the phone will power on as a result of the user action. The default is unchecked. This is a required field. Default: False
EnergyWise Domain	This field defines the EnergyWise domain in which the phone is participating. An EnergyWise domain is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, provide an EnergyWise domain. The default is blank. Maximum length: 127

Field	Description
EnergyWise Endpoint Security Secret	This field defines the password (shared secret) used to communicate within the EnergyWise domain. An EnergyWise domain and secret is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, provide an EnergyWise domain and secret. The default is blank. Maximum length: 127
Phone On Time	This field determines the time that the phone turns on automatically on the days that are selected in the Enable Power Save Plus list box. Enter the time in 24 hour format, where 00:00 represents midnight. For example, to automatically turn the phone on at 7:00 a.m., (0700), enter 07:00. To turn the phone on at 2:00 p.m. (1400), enter 14:00. If this field is blank, the phone automatically turns on at 00:00. Default: 00:00 Maximum length: 5
Phone Off Time	This field determines the time of day that the phone will turn itself off on the days that are selected in the Enable Power Save Plus list box. Enter the time in the following format hours: minutes. If this field is blank, the phone automatically turns off at midnight (00:00). **Note** If Phone On Time is blank (or 00:00) and Phone Off Time is blank (or 24:00), the phone will remain on continuously, effectively disabling the Power Save Plus feature unless you allow EnergyWise to send overrides. Default: 24:00 Maximum length: 5

Field	Description
Phone Off Idle Timeout	This field represents the number of minutes that the device must be idle before the device will request the power sourcing equipment (PSE) to power down the device. The value in this field takes effect: • When the device was in Power Save Plus mode as scheduled and was taken out of Power Save Plus mode via some user interactions. • When the phone is repowered by the attached switch. • When the Phone Off Time is met but the phone is in use. The unit is minutes. The range is 20 to 1440. This is a required field. Default: 60 Minimum: 20 Maximum: 1440
Days Display Not Active	This field allows the user to specify the days that the backlight is to remain off by default. Typically this would be Saturday and Sunday for US corporate customers. Saturday and Sunday should be the default. The list contains all of the days of the week. To turn off backlight on Saturday and Sunday the User would hold down Control and select Saturday and Sunday.
Display On Time	This field indicates the time of day the display is to automatically turn itself on for days listed in the off schedule. The value should be in a 24 hour format. Where 0:00 is the beginning of the day and 23:59 is the end of the day. Leaving this field blank will activate the display at the beginning of the day (e.g. - "0:00"). To set the display to turn on at 7:00AM the user would enter "07:00" without the quotes. If they wanted the display to turn on at 2:00PM they would enter "14:00" without the quotes. Default: 07:30 Maximum length: 5

Field	Description
Display On Duration	This field indicates the amount of time the display is to be active for when it is turned on by the programmed schedule. No value indicates the end of the day. Maximum value is 24 hours. This value is in free form hours and minutes. "1:30" would activate the display for one hour and 30 minutes. Default: 10:30 Maximum length: 5
Display Idle Timeout	This field indicates how long to wait before the display is turned off when it was turned on by user activity. This inactivity timer will continually reset itself during user activity. Leaving this field blank will make the phone use a pre-determined default value of one hour. Maximum value is 24 hours. This value can be in free form hours and minutes. "1:30" would turn off the display after one hour and 30 minutes of inactivity. Default: 01:00 Maximum length: 5
Display On When Incoming Call	When the device is in screen saver mode, this will turn the display on when a call is ringing. This is a required field. Default: Enabled
Incoming Call Toast Timer	This parameter specifies the maximum time in seconds that the toast displays a new incoming call notification. This is a required field. Default: 5
Enable Mute Feature	Enable mute feature to provide Mute softkey on 7906/7911. This is a required field. Default: False
Join And Direct Transfer Policy	This field indicates join and direct transfer policy for same line and across line. This is a required field. Default: Same line, across line enable
Medianet Statistics Interval	Medianet statistics reports are updated periodically during active media sessions. Set stats collection interval in seconds. Default: 15

Field	Description
RTCP	Maintains statistic for audio. This is a required field. Default: Disabled
Advertise G.722 and iSAC Codecs	Indicates whether Cisco Unified IP Phones will advertise the G.722 codec to Cisco Unified CallManager. Codec negotiation involves two steps: first, the phone must advertise the supported codec(s) to Cisco Unified CallManager (not all endpoints support the same set of codecs). Second, when Cisco Unified CallManager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. Valid values specify Use System Default (this phone will defer to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (this phone will not advertise G.722 to Cisco Unified CallManager) or Enabled (this phone will advertise G.722 to Cisco Unified CallManager). This is a required field. Default: Use System Default
Video Calling	When enabled, indicates that the phone will participate in video calls when connected to an appropriately equipped PC. This is a required field. Default: Enabled
Wifi	Indicates whether the Wi-Fi on the phone is enabled or disabled. This is a required field. Default: Enabled

Field	Description
Wi-Fi Hotspot	Indicates whether the personal Wi-Fi Hotspot capability on the phone is enabled or disabled. In order for a phone to provide a hotspot, at least three conditions must be met: • This flag must be enabled. • Phone must provide a hotspot. • An appropriate Wi-Fi Hotspot Profile must be given on the Device Pool Configuration or the Phone Configuration page. This is a required field. Default: Disabled
PC Port	Indicates whether the PC port on the phone is enabled or disabled. The port labeled "10/100 PC" on the back of the phone connects a PC or workstation to the phone so they can share a single network connection. This is a required field. Default: Enabled
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the Phone Port to the PC Port. Select Enabled if an application is being run on the PC Port that requires monitoring of the IP Phone's traffic such as monitoring and recording applications (common in call center environments) or network packet capture tools used for diagnostic purposes. To use this feature PC Voice VLAN access must be enabled. This is a required field. Default: Disabled
PC Voice VLAN Access	Indicates whether the phone will allow a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the phone. Set this setting to Enabled if an application is being run on the PC that requires monitoring of the phones traffic. These could include monitoring and recording applications and use of network monitoring software for analysis purposes. This is a required field. Default: Enabled

Field	Description
PC Port Remote Configuration	Allows remote configuration of the speed and duplex for the PC port of the phone, which overrides any manual configuration at the phone. This is a required field. Default: Disabled
Switch Port Remote Configuration	Allows remote configuration of the speed and duplex for the switch port of the phone, which overrides any manual configuration at the phone. Be aware that configuring this port may cause the phone to lose network connectivity. This is a required field. Default: Disabled
Automatic Port Synchronization	Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds. This is a required field. Default: Disabled
Cisco Discovery Protocol (CDP) Switch Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the switch port. This is a required field. Default: Enabled **Note** CDP should only be disabled on the Network port if this phone is connected to a non-Cisco switch. For further details, see the *Cisco Unified Communications Manager Administration Guide*.
Cisco Discovery Protocol (CDP) PC Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the PC port. This is a required field. Default: Enabled **Note** Disabling CDP on the PC port will prevent Cisco VT Advantage or Unified Video Advantage from working properly on this phone. For further details, see the *Cisco Unified Communications Manager Administration Guide*.

Field	Description
LLDP-MED- Switch Port	Media Endpoint Discover (LLDP-MED): Switch Port: Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the switch port. This is a required field. Default: Enabled
Link Layer Discovery Protocol (LLDP)- PC Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the PC port. This is a required field. Default: Enabled
LLDP Asset ID	Allows administrator to set Asset ID for Link Layer Discovery Protocol. Maximum length: 32
LLDP Power Priority	Allows administrator to set Power Priority for Link Layer Discovery Protocol. This is a required field. Default: Unknown
Power Negotiation	Allows administrator to enable or disable Power Negotiation. This is a required field. Default: Enabled
802.1x Authentication	Specifies the 802.1x authentication feature status. This is a required field. Default: User Controlled
FIPS Mode	This parameter sets the Federal Information Processing Standards (FIPS) mode for the phone. The phone is a FIPS 140-2 level 1 compliant device when this option is enable. This is a required field. Default: Disabled
80-bit SRTCP	Enable 80-bit authentication tag for SRTCP. This is a required field. Default: Disabled

Field	Description
Always On VPN	Indicates whether the device starts the VPN AnyConnect client and establish a connection with the configured VPN profile from the Cisco Unified Communications Manager. This is a required field. Default: False
Store VPN Password on Device	This parameter controls whether VPN password can be stored on the device. Its value is used only when Password Persistence is set to true. If disabled, the user's VPN password is stored in memory and is automatically resubmitted upon subsequent connects. However, when the device reboots, the user has to re-enter their VPN password again. If enabled, the user's VPN password is stored on the device and persist across reboots. This is a required field. Default: False
Allow User-Defined VPN Profiles	This parameter controls whether the user can use the AnyConnect VPN client to create VPN profiles. If disabled, the user cannot create VPN profiles. This is a required field. Default: True
Require Screen Lock	This parameter indicates whether screen lock is required on the device. If "User Controlled" is selected, the device will not prompt for a PIN or password. The "PIN" and "Password" options require the user to enter a password to unlock the screen. A "PIN" is a numeric password that is at least four digits long. A "Password" is an alphanumeric password, consisting of at least 4 alphanumeric characters, one of which must be a nonnumeric number, and one must be a capital letter. This is a required field. Default: PIN

Field	Description
Screen Lock Timeout	Maximum idle time in seconds before the device automatically locks the screen. After the screen is locked, the user password is required to unlock it. This is a required field. Default: 600 Minimum: 15 Maximum: 1800
Enforce Screen Lock During Display-On Time	This parameter provides an unobtrusive lock policy that allows users to work freely with their device throughout the workday, without the device locking after the interval that is set in Cisco Unified Communications Manager. After work, the device locks as defined in the policy, to prevent unauthorized users from accessing it. The device always supports the user-controlled manual lock option (power button), for meetings or lunch breaks. The device remains locked until the user enters the PIN/password on next use. • ON—Device locks during the workday or during display-on time (default setting). • OFF—Device locks only during display-off time or after work hours, based on day or time settings listed above. This is a required field. Default: True
Lock Device During Audio Call	When the device is in a charging state and an active voice call is in progress, an administrator can override the screen lock PIN enforcement timer to keep the screen active during an audio call. Screen lock timer takes effect after audio call is completed and timer is exceeded. This is a required field. Default: Disabled
Kerberos Server	Authentication server for web proxy Kerberos. Maximum length: 256
Kerberos Realm	Realm for web proxy Kerberos. Maximum length: 256

Field	Description
TLS Resumption Timer	This parameter controls the maximum number of seconds that a peer can reuse the TLS session without doing a full handshake authentication. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. Only apply to TLS session for HTTPS on Cisco IP phones. This is a required field. Default: 3600 Minimum: 0 Maximum: 3600
User Credentials Persistent For Expressway Sign in	This parameter enables the phone to persistently store user credentials used for authentication with Expressway Sign in. This is a required field. Default: Disabled
WLAN SCEP Server	Indicates the SCEP Server the phone uses to obtain certificates for WLAN authentication. Enter the hostname or the IP address (using standard IP addressing format) of the server. Maximum length: 256
WLAN Root CA Fingerprint (SHA256 or SHA1)	Indicates the SHA256 or SHA1 fingerprint of the Root CA to use for validation during the SCEP process when issuing certificates for WLAN authentication. It is recommended to utilize the SHA256 fingerprint, which can be obtained via OpenSSL (i.e. openssl x509 -in rootca.cer -noout -sha256 -fingerprint) or using a Web Browser to inspect the certificate details. Enter the 64 hexadecimal character value for the SHA256 fingerprint or the 40 hexadecimal character value for the SHA1 fingerprint with a common separator (colon, dash, period, space) or without a separator. If using a separator, then the separator should be consistently placed after every 2, 4, 8, 16, or 32 hexadecimal characters for an SHA256 fingerprint or every 2, 4, or 8 hexadecimal characters for an SHA1 fingerprint. Maximum length: 95
Outbound Rollover	When the number of calls on the line is exceeded, a new created call will roll over to the next line. This is a required field. Default: Disabled

Field	Description
Detect Unified CM Connection Failure	This field determines the sensitivity that the phone application has for detecting a connection failure to Cisco Unified Communications Manager, which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. The precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing. This only applies to the wired Ethernet connection. Default = Normal. This is a required field. Default: Normal
Time to Wait for Seamless Reconnect After TCP Drop or Roaming	This field indicates a grace period to establish a new TCP connection via keep-alive registration after the original TCP connection is torn down. The Seamless Reconnect is disabled if the value is set to 0. Default: 5 Minimum: 0 Maximum: 300
Load Server	Indicates that the phone uses an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IP address (using standard IP addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades. Maximum length: 256

Field	Description
IPv6 Load Server	Indicates that the phone will use an alternative IPv6 server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local IPv6 server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IPv6 address (using standard IPv6 addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades. Maximum length: 25
Peer Firmware Sharing	Enables or disables Peer to Peer image distribution in order to allow a single phone in a subnet to retrieve an image firmware file then distribute it to its peers; thus reducing TFTP bandwidth and providing for a faster firmware upgrade time. This is a required field. Default: Enabled
Log Server	Specifies an IP address and port of a remote system where log messages are sent. Maximum length: 32
IPv6 Log Server	Specifies an IPv6 address and port of a remote system where log messages are sent. The format is: [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]:ppppp@@options. Options will be format as: • base=x (value range is 0~7) (default value is 7) • pfs=y (value range is 0~1) (default value is 0) And the two parameters are optional.
Log Profile	Run the pre-defined debug command remotely. Default: Preset
Remote Log	This parameter specifies where to send the log data by serviceability. If enabled, the log data is copied by serviceability to the place specified by Log Server/IPV6 Log Server. If disabled, the log data will not be copied by serviceability to the place specified by Log Server/IPV6 Log Server.

Field	Description
HTTPS Server	Allows Administrator to permit http and https or https only connections if Web Access is enabled. This is a required field. Default: http and https Enabled
Web Access	This parameter indicates whether the phone accepts connections from a web browser or other HTTP client. Disabling the web server functionality of the phone blocks access to the phones internal web pages. These pages provide statistics and configuration information. Features, such as Quality Report Tool (QRT), will not function properly without access to the phones web pages. This setting will also affect any serviceability application such as CiscoWorks 2000 that relies on web access. This is a required field. Default: Disabled
Settings Access	Indicates whether the Settings button on the phone is functional. When Settings Access is enabled, you can change the phone network configuration, ring type, and volume on the phone. When Settings Access is disabled, the Settings button is disabled; no options appear when you press the button. Also, you cannot adjust the ringer volume or save any volume settings. This is a required field. Default: Enabled
SSH Access	This parameter indicates whether the device accepts SSH connections. Disabling the SSH server functionality of the device blocks access to the device. This is a required field. Default: Disabled
Ring Locale	IP Phone has distinctive ring for On-net/Off-net or line based, but its ring cadence is fixed, and it is based on US standard only. Ring cadence in US standard is opposite to Japan standard. To support Japan ring cadence, the ring cadence is be configurable according to Ring Locale. This is a required field. Default: Default

Field	Description
Android Debug Bridge or ADB	This parameter enables or disables the Android Debug Bridge (ADB) on the device. This is a required field. Default: Disabled
Customer support upload URL	This URL is used to upload problem report files when the user has run the "Problem Reporting Tool" on the endpoint. Maximum length: 256
Allow Applications from Unknown Sources	This parameter controls whether the user can install Android applications on the device from a URL or from Android packages (APK) that are received through email, instant message (IM), or from a Secure Digital (SD) card. This is a required field. Default: Disabled
Allow Applications from Android Market	This parameter controls whether the user can install Android applications from the Google's Android Market. This is a required field. Default: False
Allow Applications from Cisco AppHQ	This parameter controls whether the user can install Android applications from the Cisco AppHQ. This is a required field. Default: False
AppHQ Domain	The fully qualified domain name to use when users log into AppHQ. If empty, the user will specify their own domain name along with their username. The AppHQ domain is used to associate the user to a given Custom AppHQ store, if it exists. Example: cisco.com. Maximum length: 256
Enable Cisco UCM App Client	This parameter controls whether the Application Client runs on the device. When the Application Client is enabled, you can select the applications they want to install from the Cisco Unified Communications Manager. This is a required field. Default: False

Field	Description
Company Photo Directory	This parameter specifies the URL which the device can query for a user and get the image associated with that user. Maximum length: 256
Voicemail Server (Primary)	Hostname or IP address of the primary mailstore voicemail server. Maximum length: 256
Voicemail Server (Backup)	Hostname or IP address of the backup mailstore voicemail server. Maximum length: 256
Presence and Chat Server (Primary)	Hostname or IP address of the primary presence server. Maximum length: 256
Alternate phone book server type	By default the endpoint uses the UDS server on the UCM it's registered to, but if you wish to use an alternate phone book server, this parameter combined with an alternate phone book address overrides the default setting of the endpoint. UDS sets the alternate phone book type as UDS. This is a required field. Default: UDS
Alternate phone book server address	By default the endpoint uses the UDS server on the UCM it's registered to, but if you wish to use an alternate phone book server, this parameter combined with the alternate phone book type will override the default setting of the endpoint. The field requires a full URL for the phone book servers. Example for UDS server url: https://uds-host-name:8443/cucm-uds/users. Maximum length: 256
Presence and Chat Server Type	This parameter indicates the type of server specified in the "Presence and Chat Server" field. This is a required field. Default is Cisco WebEx Connect.
Presence and Chat Single Sign-On (SSO) Domain	The enterprise domain used by Cisco WebEx Connect Cloud to perform Single-Sign-On (SSO) authentication against an enterprise. Maximum length: 256

Field	Description
Device UI Profile	Changes the device's user interface characteristics to optimize for specific user personas such as basic video callers (Simple), public space phone(Public) or general collaboration users (Enhanced). This is a required field. Default: Simple
Multi-User	This parameter indicates whether multi-user is enabled or disabled on the device. This is a required field. Default: Disabled
Multi-User URL	This parameter specifies the URL of the extension mobility server. Maximum length: 256
Email address for customer support	This sets an email address to which you can send problem report files from the 'Problem Reporting Tool' on the phone. Maximum length: 256
PSTN Mode	Enable PSTN Mode for IP Phone 6921/6941/6961. This is a required field. Default: Disabled
Background Image	This parameter specifies the default wallpaper file. Only the administrator disables end user access to phone wallpaper list, could this parameter take effect. Maximum length: 64
Simplified New Call UI	This parameter specifies if use simplified call UI style when the phone is Off-hook. Those who like the New Call Window can continue to use that at the same time that those who prefer the Simplified New Call Session can use that method. This is a required field. Default: Disabled
Revert to All Calls	When enabled, phone will revert to All Calls after any call is ended if the call is on a filter other than Primary line or All Calls. This is a required field. Default: Disabled

Field	Description
RTCP for Video	RTCP enable for both Video and audio RTP streams which for RTP statistic and lip sync purpose. With this disable, video lipsync relays on free run mode. This is a required field. This is a required field. Default: Enabled
Provide Dial Tone from Release Button	Indicates whether Dial Tone is provided when Release Button is pressed. If the value is true, then in "Off Hook Dialing/RingingOut/Connected" state, a new Call Windows will be brought out after Release Button is pressed. If "Revert To All Calls" feature was enabled, it should be active first before "Dial Tone" feature. This is a required field. Default: Disabled
Hide Video By Default	This field provides an additional flexibility of hiding video window by default if "Hide Video By Default" is enabled. This is a required field. Default: Disabled With "Hide Video by default" feature enabled, the video window is initially hidden on video calls. If "Auto Transmit Video" is "on," the phone displays a "Hide Video View", while the video is being transmitted to the remote party. This may make distinguishing video calls from voice calls more difficult for end users. The benefit of "Hide Video by default" is that, in work environments where users are more likely to mute their video or close the shutters on the camera, the far end user will see the audio call plane rather than a black "mute" box on their phone. "Hide Video by Default" is not recommended for work environments where video calling is used often with cameras open, enabled, and unmuted.

Field	Description
VXC VPN Option	This field indicates how VXC VPN is supported. If "Dual Tunnel" is selected, phone establishes two VPN tunnels, one for Phone and another for VXC device. If "Single Tunnel" is selected, phone establishes only one VPN tunnel for phone and VXC-device to share. Where uncompromised voice or video quality is required the dual VPN tunnel solution is recommended. Dual Tunnel—Through the use of two VPN tunnels the host Cisco IP Phone is able to provide prioritization of its CPU and memory resources to the data associated with the Phones Voice or video functions over that of the data associated with the VXC VPN tunnel. This approach requires two manual login entries (dependent on security parameters), one for Phone's Voice or Video VPN and another for VXC VPN. The two tunnel approach also requires two VPN concentrator ports and two IP addresses adding potential costs. Single Tunnel—A single VPN tunnel option is implemented for those customers willing to trade off potential voice/video quality for a simplified operating model. The solution consists of operating over a single VPN tunnel by sharing the available 89/99xx processor and memory resources across the voice, video and VDI services. The IP Phone is unable to prioritize data handing of one service over another. This is a required field. Default: Dual Tunnel

Field	Description
VXC Challenge	This field indicates whether or not to challenge VXC device. If "Challenge" is selected, VXC device will be challenged. For "Single Tunnel" VXC VPN Option, Phone VPN Sign In window will pop up for user to input credentials and re-establish Phone VPN tunnel. For "Dual Tunnel" VXC VPN Option, VXC VPN Sign In window will pop up for user to input credentials and re-establish VXC VPN tunnel. If "No Challenge" is selected, VXC challenge will be bypassed. For "Single Tunnel" VXC VPN Option, VXC traffic will silently be permitted to go over phone VPN without VXC challenge. For "Dual Tunnel" VXC VPN Option, credentials of Phone VPN tunnel will be reused to re-establish VXC VPN tunnel. This is a required field. Default: Challenge
VXC-M Servers	VXC Management Server IP address list, separated with comma. Maximum length: 255
Record Call Log from Shared Line	This field indicates whether to record call log from shared line. This is a required field. Default: Disabled
Show Call History for Selected Line Only	When enabled, the phone shows call history for selected line only. This is a required field. Default: Disabled
Actionable Incoming Call Alert	Show an Alert with Answer, Divert, and Ignore softkeys when there is an incoming call alerting for user to act. This is a required field. Default: Show for all Incoming Call
DF bit	Configure the DF bit in IP header. This is a required field. Default: 0

Field	Description
Separate Audio and Video Mute	Indicates whether separate audio and video mute. When enabled this parameter, the Mute key affects only the audio; When disabled this parameter, the Mute key affects the audio and the video. By default, Separate Audio and Video is disabled. This is a required field. Default: Disabled
Softkey Control	Indicates whether phone softkeys are controlled by Feature Control Policy or Softkey Template. This is a required field. Default: Feature Control Policy
Start Video Port	This field defines the beginning of video RTP port
Stop Video Port	This field defines the end of video RTP port
Lowest Alerting Line State Priority	When disabled, if there is an incoming call alerting on the shared line, the LED/Line state icon reflects the alerting state instead of Remote-In-Use. When enabled, you see the Remote-In-Use state when there is call alerting on the shared line. This is a required field. Default: Disabled
One Column Display for KEM	When disabled. The KEM displays 18 Line/Button configured. Each line item uses half of the KEM screen width. When enabled, each line item will occupy entire KEM screen width for being able to show more characters. Total 9 Line/Button configured is displayed on one KEM. This is a required field. Default: Disabled
Audio EQ	This field configures handset or handsfree mode audio equalization setting. This is a required field.
Customer Support Use	This parameter specifies some special issue. Please split the special issue ID with semicolon." Maximum length: 64

Field	Description
Energy Efficient Ethernet(EEE): PC Port	This parameter indicates enable or disable Energy Efficient Ethernet(EEE) on PC port. This is a required field. Default is Enable.
Energy Efficient Ethernet(EEE): SW Port	This parameter indicates enable or disable Energy Efficient Ethernet(EEE) on switch port This is a required field. Default is Disabled.
WLAN Authentication Attempts	This parameter specifies the number of authentication attempts when there is explicit failure due to invalid credentials. This is a required field. Default: 2
WLAN Profile 1 Prompt Mode	This parameter enables or disables WLAN prompt mode, where user is prompted to re-enter password on device start-up or reboot. This is a required field. Default: Disabled
Line Mode	This parameter allows admin to switch between Session Line Mode and Enhanced Line Mode. While in Session Line Mode, the buttons on the left of the screen can be configured as programmable line keys and the buttons on the right of the screen are always session keys. While in Enhanced Line Mode, all the buttons can be configured as programmable line keys. This is a required field. Default: Session Line Mode
Interactive Connectivity Establishment (ICE)	

Field	Description
ICE	Specifies if clients use the ICE protocol to choose optimal paths for sending and receiving media. If you select Enabled, clients use the ICE protocol to choose optimal media paths. Using the ICE protocol can improve the quality of audio and video calls for users outside the corporate network. If you select Disabled, clients do not use the ICE protocol or attempt to communicate using optimal media paths. If you select Disabled as the value, no other ICE settings take effect. Select Disabled if your network does not include TURN servers or if all client communication takes place within the corporate network. Default: Enabled
Default Candidate Type	Defines the initial method that clients use to communicate with each other. Choose one of the following values: The default setting controls the initial communication path for the first few seconds of a call. If the ICE protocol can establish a more optimal media path than the default candidate type, clients use that path. For example, if you specify Server Reflexive as the default, clients communicate through NAT enabled routers when calls start. If clients can use the Host candidate type, they stop communicating through NAT enabled routers and communicate directly with each other. If clients cannot establish communication using the default candidate type, they use the next candidate type in order of performance. For example, you leave the default value of Host. For the initial attempt to establish communication, clients try to communicate directly. If clients cannot communicate directly with each other, clients use the Server Reflexive candidate type and attempt to communicate through NAT enabled routers. If clients cannot communicate through NAT enabled routers, they use the Relay candidate type. Default: Host

Field	Description
Server Reflexive Address	Specifies if clients can communicate through NAT enabled routers. If you enable this setting, clients can communicate directly with each other, through NAT enabled routers, or through TURN servers. Enable this setting if you specify Server Reflexive as the default candidate type. If you disable this setting, clients can communicate directly with each other or through a TURN server. You should disable this setting if your TURN servers apply Quality of Service (QoS) settings to improve media quality. Default: Enabled
Primary TURN Server Host Name or IP Address	Specifies the primary Traversal Using Relay for NAT (TURN) server. The ICE protocol uses TURN servers to provide addresses and ports to clients so that they can establish optimal media paths. Usually, TURN servers relay media between clients and the corporate network when calls begin. If clients can establish a more optimal media path using the ICE protocol, clients stop relaying media through TURN servers and use the optimal media path. You do not need to specify a TURN server address if your edge device includes a built-in TURN server. In other words, you do not need to specify a TURN server address if that address is the same as the address for your edge server. If your edge device does not include a built-in TURN server, and you do not specify a TURN server address, the ICE protocol does not take effect. You can specify either an IP address or FQDN. Maximum length: 1024
Secondary TURN Server Host Name or IP Address	Specifies the secondary TURN Server that the ICE protocol uses. You can specify either an IP address or FQDN. Maximum length: 1024
TURN Server Transport Type	Defines the protocol the client uses to send requests to TURN servers. Clients can send requests over UDP, TCP, or TLS over TCP. Select Auto to allow clients to set an appropriate transport type. Default: Auto

Field	Description
TURN Server Username	If you do not specify a username or do not apply this parameter, clients attempt to authenticate to TURN servers with the users' Cisco Unified Communications Manager username. If your deployment uses single sign-on (SSO), you must specify a username. TURN servers do not support SSO. Maximum length: 127
TURN Server Password	If you do not specify a password or do not apply this parameter, clients attempt to authenticate to TURN servers with the users' Cisco Unified Communications Manager password. If your deployment uses single sign-on (SSO), you must specify a password. TURN servers do not support SSO. Maximum length: 127
Instant Messaging	
File Types to Block in File Transfer	A semicolon separated list of file types to block during file transfer operations. Maximum length: 1024
URLs to Block in File Transfer	A semicolon separated list of URLs to block during file transfer operations. Maximum length: 1024
Desktop Client Settings	
Automatically Start in Phone Control	If enabled, the client starts in desktop phone control mode. This is a required field. Default: Disabled
Automatically Control Tethered Desk Phone	If enabled, the client automatically controls the tethered desktop phone. This is a required field. Default: Disabled
Extend and Connect Capability	Indicates if Extend and Connect capabilities are enabled for the client. This allows the client to monitor and control calls on Third party PBX, PSTN, and other remote phones. This is a required field. Default: Enabled

Field	Description
Display Contact Photos	Indicates if contact photo retrieval and display are enabled or disabled for the client. This is a required field. Default: Enabled
Number Lookups on Directory	Indicates if phone number lookups using the Corporate Directory are enabled or disabled for the client. This is a required field. Default: Enabled
Jabber For Windows Software Update Server URL	The URL of the Software Update Server that the Jabber For Windows Client uses when the User selects the Update Jabber link. The default is blank. Maximum length: 1024
Analytics Collection	Indicates if analytics collection is enabled or disabled for the client. This is a required field. Default: Disabled
Problem Report Server URL	The URL of the Problem Report Server that is used by the client. The default is blank. Maximum length: 1024
Analytics Server URL	The URL of the analytics server that is used by the client. The default is blank. Maximum length: 1024
Cisco Support Field	A semicolon separated list of custom settings that are used by the client to assist with deployment. This field is used only with the assistance of Cisco Support personnel. The default is blank. Maximum length: 1024

Conference Bridge Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 77: Conference Bridge Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.

Cisco IOS Enhanced Conference Bridge

For Cisco Prime Collaboration Release 11.5 and later

Table 78: Cisco IOS Enhanced Conference Bridge Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Device Security Mode	This field displays for Cisco IOS Enhanced Conference Bridge only. If you choose non-secure Conference Bridge, the non-secure conference establishes a TCP port connection to Cisco Unified Communications Manager on port 2000. **Note** Ensure that this setting matches the security setting on the conference bridge, or the call fails. The Encrypted Conference Bridge setting supports the secure conference feature.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. 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.

Cisco Conference Bridge Hardware

For Cisco Prime Collaboration Release 11.5 and later

Table 79: Cisco Conference Bridge Hardware Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Hardware Conference Bridge Info	
MAC Address	Enter a unique device MAC address.
Description	Enter a description for your conference bridge.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. 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.
Special Load Information	Enter any special load information or leave blank to use system default.

Cisco IOS Conference Bridge

For Cisco Prime Collaboration Release 11.5 and later

Table 80: Cisco IOS Conference Bridge Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.

Field	Description
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. 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.

Cisco TelePresence MCU

For Cisco Prime Collaboration Release 11.5 and later

Table 81: Cisco TelePresence MCU Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Device Information	
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Conference Bridge Prefix	Conference Bridge Prefix is used only for centralized deployments when the conference resources are deployed across a Small Medium Enterprise (SME). HTTP and SIP signaling are intended for different destinations. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
SIP Trunk	Select a SIP trunk to use for this conference bridge from a list of existing SIP trunks.

Field	Description
Allow Conference Bridge Control of the Call Security Icon	Check this check box to allow the Cisco TelePresence Conductor to control the display of the call security icon.
HTTP Interface Info	
Override SIP Trunk Destination as HTTP Address	Check this check box to override the SIP trunk destination. Use this feature if the HTTP and SIP signaling are intended for different destination IP addresses. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
Host Name IP Address	
Username	Enter the Cisco TelePresence Conductor administrator username.
Password	Enter the Cisco TelePresence Conductor administrator password
Confirm Password	Re-enter the Cisco TelePresence Conductor administrator password
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence Conductor. The default HTTPS port is 443.
HTTP Port	Enter the Cisco TelePresence Conductor HTTP port. The default port is 80.

Cisco TelePresence Conductor

For Cisco Prime Collaboration Release 11.5 and later

Table 82: Cisco TelePresence Conductor Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Conference Bridge Prefix	Conference Bridge Prefix is used only for centralized deployments when the conference resources are deployed across a Small Medium Enterprise (SME). HTTP and SIP signaling are intended for different destinations. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.

Field	Description
SIP Trunk	Select a SIP trunk to use for this conference bridge from a list of existing SIP trunks.
Allow Conference Bridge Control of the Call Security Icon	Check this check box to allow the Cisco TelePresence Conductor to control the display of the call security icon.
HTTP Interface Info	
Override SIP Trunk Destination as HTTP Address	Check this check box to override the SIP trunk destination. Use this feature if the HTTP and SIP signaling are intended for different destination IP addresses. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
Host Name IP Address	Enter one or more hostnames or IP addresses for the HTTP signaling destination if you have selected to override the SIP trunk destination.
Username	Enter the Cisco TelePresence Conductor administrator username.
Password	Enter the Cisco TelePresence Conductor administrator password
Confirm Password	Re-enter the Cisco TelePresence Conductor administrator password
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence Conductor. The default HTTPS port is 443.
HTTP Port	Enter the Cisco TelePresence Conductor HTTP port. The default port is 80.

Cisco Conference Bridge (WS-SVC-CMM)

For Cisco Prime Collaboration Release 11.5 and later

Table 83: Cisco Conference Bridge (WS-SVC-CMM) Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Choose Cisco Conference Bridge (WS-SVC-CMM).
Media Server Conference Bridge Info	
MAC Address	Enter a unique device MAC address.
Subunit	From the drop-down list box, choose the value for the daughter card for a given slot on the Communication Media Module card.
Description	Enter a description for your conference bridge.

Field	Description
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. 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.
Maximum Capacity	Choose the maximum number of streams for a given service on a daughter card. Possible values include 32, 64, 96, and 128 streams. Ensure that each daughter card has as many ports as the value that you choose.
Service Specific Configuration Layout	
General	
RTP Timeout (sec)	This defines the RTP timeout value.
Signaling Diffserv Code Points (DSCP)	This defines DSCP for signaling.
Audio Diffserv Code Points (DSCP)	This defines DSCP for audio.
Enable G.729 Voice Activity Detection	This enables or disables the Voice Activity Detection(VAD) for G.729 codec. When music is played in the transcoding session, the quality is degraded since VAD is enabled by default in G.729. VAD can be disabled to address this issue.
Codec Packetization Rate	
G.711ulaw	This defines the packetization rate for codec G.711ulaw. "None" defaults to 60ms.
G.711alaw	This defines the packetization rate for codec G.711alaw. "None" defaults to 60ms.

Field	Description
G.729/G.729b	This defines the packetization rate for codec G.729/G.729b. "None" defaults to 60ms.
G.729a/G.729ab	This defines the packetization rate for codec G.729a/G.729ab. "None" defaults to 60ms.
G.723	This defines the packetization rate for codec G.723. "None" defaults to 60ms.
Connection Options	
Switchover Method	Timing mechanism to switch over to a backup CallManager. • Graceful—The switchover happens only after all the active sessions are terminated. • Immediate—The switchover to the backup CallManager happens immediately.
Switchback Method	Timing mechanism to switch back to a primary CallManager. • Graceful—The CallManager switchback happens only after all the active sessions are terminated. • Guard (graceful guard)—The CallManager switchback happens when either the active sessions are terminated gracefully or when the guard timer expires, whichever happens first. • Immediate—Switchback to the higher order CallManager happens immediately. • Scheduled—The CallManager switchback happens during the scheduled time. • Uptime—The uptime timer is started once the higher order CallManager comes alive; once this timer expires, the CallManager switchback happens.
Switchback Interval (sec)	The Switchback Interval timer is used to control the polling of the primary or higher order CallManager(s). If attempt to switchback to a higher order CallManager fails, the Switchover Interval timer is started. When the timer expires, another attempt to switchback to a higher order CallManager is initiated.
Switchback guard timeout	This defines the guard timeout value. With the guard (graceful guard) method, the CallManager switchback happens when either the active sessions are terminated gracefully or when the guard timer expires, whichever happens first.
Switchback uptime timeout	This defines the uptime timeout value. With the uptime method, the uptime timer is started once the higher order CallManager comes alive; once this timer expires, the CallManager switchback happens.

Field	Description
Switchback scheduled timeout	This defines the scheduled time value. With the scheduled method, the CallManager switchback happens during the scheduled time.
CallManager Connect Retries	This defines the number of polling retries before connectivity to the CallManager is considered down. When the number of polling attempts reaches the Connect Retries value, connection to the next CallManager is attempted.
CallManager Connect Interval (sec)	The Connect Interval timer is used to control the polling interval of the CallManager. If the current CallManager connection fails, the Connect Interval timer is started. When the timer expires, another attempt to connect to the CallManager is initiated.
Keepalive Retries	This defines the number of keepalive retries before connectivity to the CallManager is considered down. When the number of unacknowledged keepalive messages reaches the Keepalive Retries value, CallManager switchover happens.
Keepalive Timeout (sec)	This defines the keepalive timeout value. A timer is started whenever a keepalive message is sent to the CallManager. Once the timeout occurs, the next keepalive message is sent unless the number of unacknowledged keepalive messages reaches the Keepalive Retries value.
Registration Retries	This defines the number of registration retries with one CallManager before registering to the next CallManager in the CallManager group.
Registration Timeout (sec)	This defines the registration timeout value. A timer is started whenever a registration message is sent to the CallManager. Once the timeout occurs, the next registration message is sent unless the number of unacknowledged registration messages reaches the Registration Retries value.

Cisco Video Conference Bridge (IPVC-35xx) Configuration Settings

For Cisco Prime Collaboration Release 11.5 and later

Table 84: Cisco Video Conference Bridge (IPVC-35xx) Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Choose Cisco Conference Bridge(IPVC-35xx).
Media Server Conference Bridge Info	
MAC Address	Enter a unique device MAC address.
Description	Enter a description for your conference bridge.
Device Pool	Choose a device pool or choose Default.

Field	Description
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. 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.
Service Specific Configuration Layout	
General	
DSCP for Control Messages	This parameter specifies the Quality of Service field to be used in the IP packets of the SCCP protocol from the Conference Bridge to the Call Manager.
Local Base Port	The Local Base Port parameter chooses the first port used by the Conference Bridge to connect to its Cisco CallManager(s). The connection is used for SCCP messaging.
Registration Info	
Failover Recovery Mode	Failover recovery occurs when a new TCP connection to a higher priority Cisco CallManager is opened, while the Conference Bridge is connected to a lower priority Cisco CallManager. The recovery mode determines when the Conference Bridge registers to the new Cisco CallManager. • Immediate—As soon as the new connection is opened. • Graceful—Only when the Conference Bridge is free of active calls. • Timeout—When the Conference Bridge is free of active calls or when the timer expires.
Failover Recovery Timeout	This value is only active when the Failover Recovery Mode is set to Timeout. This parameter determines the time that the Conference Bridge waits before performing failover recovery regardless of the existence of active calls.

Field	Description
Keepalive Message Timeout	The keepalive message to the Cisco CallManager is typically answered by an Acknowledge Message to the Conference Bridge. The Keepalive Message Timeout determines how long the Conference Bridge should wait for the Acknowledge message before assuming that the Acknowledge will not arrive.
Keepalive Retries	The keepalive message to the Cisco Call Manager should be followed by an Acknowledge Message to the Conference Bridge. The Keepalive Message Retries determines the number of times that the keepalive message is sent (without receiving an acknowledgment) before the connection will be considered dead.
Register Messages Retries	The register and unregister messages to the Cisco CallManager should be followed by an Acknowledge message to the Conference Bridge. The Register Message Retries determines how many times the Conference Bridge retries registration before giving up on the currently configured Cisco CallManager and turning to a lower priority one if such a Cisco CallManager exists.
Register Messages Timeout	The register and unregister messages to the Cisco Call Manager should be followed by an Acknowledge message to the Conference Bridge. The Register Message Timeout determines how long the Conference Bridge should wait for an Acknowledge message before retrying the registration.
Wait For Primary Cisco CallManager Timeout	When the Conference Bridge is not connected to any Cisco CallManager, this parameter specifies how much time the bridge should wait for the primary Call Manager, before connecting to the backup Call Manager.

BLF Presence Group Fields Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 85: BLF Presence Group Fields Infrastructure Configuration Product Fields

Field	Description
BLF Presence Group Information	
Name	Enter the name of the BLF presence group that you want to configure.
Description	Enter a description for the BLF presence group that you are configuring.
Modify Relationship to Other BLF Presence Groups	
BLF Presence Group	Select one or more BLF presence groups to configure the permission settings for the named group to the selected groups.

Field	Description
Subscription Permission	For the selected BLF presence groups, choose one of the following options from the drop-down list box: • Use System Default—Set the permissions setting to the Default Inter-Presence Group Subscription cluster-wide service parameter setting (Allow Subscription or Disallow Subscription). • Allow Subscription—Allow members in the named group to view the real-time status of members in the selected groups. • Disallow Subscription—Block members in the named group from viewing the real-time status of members in the selected groups.

Unity Distribution List Infrastructure Configuration Product Fields

Table 86: Unity Distribution List Infrastructure Configuration Product Fields

Field	Description
Alias	Alias name of the distribution list.
Display Name	Name of the distribution list.
Extension	Extension that the phone system uses to connect.
Owner	Owner of the Call Handler for any user or distribution list.
Owner Type	Type of the owner.
Show Distribution List in Email Server Address Book	Displays the distribution list name in the email server's address book.
Member List	List of members associated with the distribution list. Use the format Alias/MemberType. **Note** You cannot remove the default system distribution list.

Unity Connection Distribution List Infrastructure Configuration Product Fields

Table 87: Unity Connection Distribution List Infrastructure Configuration Product Fields

Field	Description
Alias	Alias name of the distribution list.
Display Name	Name of the distribution list.

Field	Description
Extension	Extension that the phone system uses to connect.
Partition	Partition that is used to define the scope of the distribution list that a user or outside caller can reach.
Allow Contacts	Specifies whether contacts can be added as members of the distribution list.
Accept Messages from Foreign Systems	Allows users on remote voice messaging systems that are configured as VPIM locations to send messages to this distribution list.
Member List	List of users associated with the distribution list. Use the format Alias/MemberType. You are allowed to add, modify, or delete only 200 members at a time. For better performance, we recommend a maximum of 20 distribution lists, each with 500 members. If you want to manage more than 500 members, you can use a nested distribution list.

Directed Call Park Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 88: Directed Call Park Infrastructure Configuration Product Fields

Field	Description
Directed Call Park Configuration	
Number	Enter the directed call park number.
Description	Provide a brief description of this directed call park number or range.
Partition	If you want to use a partition to restrict access to the directed call park numbers, choose the desired partition from the dropdown list. If you do not want to restrict access to the directed call park numbers, leave the partition to use system default.
Reversion Number	Enter the number to which you want the parked call to return if not retrieved, or leave the field blank.
Reversion Calling Search Space	Choose the calling search space from the dropdown list or leave the calling search space to use the system default.

Field	Description
Retrieval Prefix	This required field, enter the prefix for retrieving a parked call.

Device Pool Infrastructure Configuration Product Fields

Table 89: Device Pool Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Cisco Unified CM Group	List of available Cisco Unified Communications Manager groups.
Date/Time Group	The date/time group to assign to devices in this device pool.
Region	The Cisco Unified Communications Manager region to assign to devices in this device pool.
Softkey Template	Softkey template that determines the configuration of the softkeys on Cisco IP Phones.
SRST Reference	A survivable remote site telephony (SRST) reference to assign to devices in this device pool.
Calling Search Space for Auto-Generation	The calling search space to assign to devices in this device pool that auto-registers with Cisco Unified Communications Manager.
Local Route Group	List of available local route groups.
Media Resource Group List	Provides 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 according to the priority order that is defined in a Media Resource Group List. If this field is left blank, the Media Resource Group that is defined in the device pool is used.
Network Hold MOH Audio Source	The audio source that plays when the network initiates a hold action.
User Hold MOH Audio Source	The audio source that plays Music On Hold when the user initiates a hold action.
Network Locale	The locale that is associated with endpoints and gateways.

Field	Description
User Locale	User location associated with the user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Connection Monitor Duration	Defines the amount of time that the IP phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and re-registers to Cisco Unified Communications Manager.
MLPP Indication	Specifies whether devices in the device pool that are capable of playing precedence tones will use the capability when the devices place an Multilevel Precedence and Preemption (MLPP) call.
MLPP Preemption	Specifies whether devices in the device pool that are capable of preempting calls in progress will use the capability when the devices place an MLPP call.
MLPP Domain	MLPP Domain that is associated with this device.
Emergency Location (ELIN) Group	Choose the ELIN group to associate with the device pool. **Note** This setting is applicable only if the Emergency Location Service is enabled in the Cisco Unified Communications Manager.

Feature Control Policy Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 90: Feature Control Policy Infrastructure Configuration Product Fields

Field	Description
Feature Control Policy Info	
Name	Name of the Feature Control Policy.
Description	Optional description.
Feature Control Section	

Field	Description
Enable Setting	For each feature listed, choose whether you want to enable or disable the setting: • Check the **Enable Setting** check box to enable the setting for the feature. • Uncheck the **Enable Setting** check box to disable the setting for the feature.

Feature Group Template Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 91: Feature Group Template Infrastructure Configuration Product Fields

Field	Description
Feature Group Template	
Name	Enter the feature group template name.
Description	Optional description.
Features	
Home Cluster	Check this check box if the end user is homed to this cluster.
Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)	Check this check box to enable the end user (on the home cluster) for IM and Presence
Include meeting information in Presence (Requires Exchange Presence Gateway to be configured on Unified Communications Manager IM and Presence server)	Check this checkbox to enable the end user to include meeting and calendar information in IM and Presence Service.
Service Profile	Choose a service profile.
User Profile	Choose a user profile.
Enable End User to Host Conference Now	Check this check box to allow the user to host a conference.
Allow Control of Device from CTI	Check this check box to allow control of the device from Computer Telephony Integration (CTI) applications.
Enable Extension Mobility Cross Cluster	Check this check box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature.

Field	Description
Enable Mobility	Check this check box to activate Cisco Unified Mobility.
Enable Mobile Voice Access	Check this check box to allow the user to access the Mobile Voice Access Integrated Voice Response (IVR) system.
Maximum Wait Time for Desk Pickup	Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call.
Remote Destination Limit	Enter the maximum number of phones to which the user is permitted to transfer calls.
BLF Presence Group	Choose a BLF presence group for the end user.
SUBSCRIBE Calling Search	Choose the SUBSCRIBE calling search space that is used to route the presence requests from the end user.
User Locale	Choose the locale that is associated with the user.

H323 Gateway Infrastructure Configuration Product Fields

Table 92: H323 Gateway Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Device Pool	List of available device pools. The device pool specifies a collection of properties for this device including Unified CM Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Call Classification	Determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet).
Media Resource Group List	Provides a prioritized grouping of media resource groups.
Location	Location for this device.
Media Termination Point Required	If Media Termination Point is used to implement features that H.323 does not support (such as hold and transfer), select Yes.
Retry Video Call As Audio	Applies to video endpoints that receive calls.

Field	Description
Wait for Far End H.245 Terminal Capability Set	Specifies that Cisco Unified Communications Manager needs to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set.
MLPP Domain	Multilevel Precedence and Preemption (MLPP) Domain to associate with this device.
Significant Digits Value	Represents the number of final digits that are retained on inbound calls.
Calling Search Spaces	Specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed.
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.
Prefix DN	The prefix digits that are appended to the called party number on incoming calls.
Redirecting Number IE Delivery - Inbound	Selecting Yes accepts the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent.
Calling Party Presentation	Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number.
Called Party IE Number Type Unknown	Choose the format for the number type in called party directory numbers.
Calling Party IE Number Type Unknown	Choose the format for the number type in calling party directory numbers.
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers.
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers.
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits.

Field	Description
Display IE Delivery	Enables delivery of the display IE in Setup, Connect, and Notify messages for the calling and called party name delivery service.
Redirecting Number IE Delivery - Outbound	Includes the Redirecting Number IE in the outgoing Setup message from the Cisco Unified Communications Manager to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded.
Packet Capture Mode	Configure this field if you need to troubleshoot encrypted signaling information for the H.323 gateway.
Common Device Config	Configuration of common device settings, such as the softkey template and user locale.
SRTP Allowed	Select Yes if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the gateway.
Enable Outbound FastStart	Select Yes to enable the H323 FastStart feature for outgoing calls.
AAR Group	Select an alternate routing group if there is insufficient bandwidth.
Packet Capture Duration	Configure this field if you need to troubleshoot encrypted signaling information for the H.323 gateway.

Hunt List Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 93: Hunt List Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Cisco Unified CM Group	List of available Cisco Unified Communications Manager groups.
Enable this Hunt List	Check this check box to enable the hunt list.
For Voice Mail Usage	If this hunt list is used for voicemail, check this check box.

Field	Description
Hunt List Member Information	
Line Group	Select one or more line groups from the **Available** list.

Hunt Pilot Infrastructure Configuration Product Fields

Table 94: Hunt Pilot Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Hunt Pilot	The hunt pilot, including numbers and wildcards (do not use spaces). You can enter + or \+ to indicate the international escape character. **Note** Ensure that the directory hunt pilot, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the hunt pilot, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries.
Route Partition	If you want to use a partition to restrict access to the hunt pilot, choose the desired partition.
Description	Enter a description of the hunt pilot. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Numbering Plan	Choose a numbering plan.
Route Filter	If your hunt pilot includes the @ wildcard, you may choose a route filter.
MLPP Precedence	MLPP precedence setting.
Hunt List	Choose the hunt list for which you are adding a hunt pilot.
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.

Field	Description
ASCII Alerting Name	Enter an alerting name for the hunt pilot in ASCII format.
Route Option	The Route Option designation indicates whether you want this hunt pilot to be used for routing calls or for blocking calls.
Provide Outside Dial Tone	Check this check box for each hunt pilot that routes the call off the local network and provides outside dial tone to the calling device.
Urgent Priority	To interrupt inter digit timing and route the call immediately.
Hunt Call Treatment Settings	
Forward Hunt No Answer	When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded.
Forward Hunt Busy	When the call that is distributed through the hunt list is busy in a specific period of time, this field specifies the destination to which the call gets forwarded.
Calling Party Transformations	
Use Calling Party’s External Phone Number Mask	Select Yes if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transformation Mask	Enter a transformation mask value.
Calling Party Prefix Digits (Outgoing Calls)	Enter the prefix digits.
Calling Line ID Presentation	Used as a supplementary service to allow or restrict the originating caller's phone number on a call basis.
Display Line Group Member DN as Connected Party	Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.
Calling Name Presentation	Used as a supplementary service to allow or restrict the originating caller's name on a call-by-call basis.
Calling Party Number Type	Choose the format for the number type in calling party directory numbers.
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers.

Field	Description
Connected Party Transformations	
Connected Line ID Presentation	Used as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis.
Display Line Group Member DN as Connected Party	Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.
Connected Name Presentation	Used as a supplementary service to allow or restrict the called party's name on a call-by-call basis.
Called Party Transformations	
Called Party Discard Digits	Select the discard digits instructions that you want to associate with this hunt pilot.
Called Party Transformation Mask	Enter a transformation mask value.
Called Party Prefix Digits (Outgoing Calls)	Enter the prefix digits.
Called Party Number Type	Choose the format for the number type in called party directory numbers.
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers.
AAR Group Settings	
AAR Group	Choose an Automated Alternate Routing (AAR) group from the drop-down list box.
External Number Mask	Enter an external number mask value for the hunt pilot.
Queuing **Note** Forward Hunt No Answer or Forward Hunt Busy settings are designed to move calls through the route list. Queuing, on the other hand, is used to hold callers in a route list. Therefore, if queuing is enabled, both Forward Hunt No Answer and Forward Hunt Busy are automatically disabled. Conversely, if Forward Hunt No Answer or Forward Hunt Busy are enabled, queuing is automatically disabled.	
Queue Calls	Check this check box to enable Call Queuing.
Network Hold/MOH Source and Announcements	Choose the audio source file that contains the music on hold and announcement to be played when a call is held in a queue.

Field	Description
Maximum Number of Callers Allowed in a Queue	Enter a value that specifies the maximum number of callers to be queued per hunt pilot. Call Queuing allows up to 100 callers to be queued per hunt pilot. Once this limit is reached on a particular hunt pilot, subsequent calls can be routed to an alternate number.
Maximum Wait Time in Queue	Enter a value (in seconds) that specifies the maximum wait time for each call in a queue. Each caller can be queued for up to 3600 seconds per hunt pilot. Once this limit is reached, that caller is routed to an alternate number.
When No Hunt Members are Logged In or registered	Check this check box to route the calls to an alternate number when none of the hunt members are logged in or registered.
Park Monitoring	
Park Monitoring Forward No Retrieve Destination	When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) to forward the parked call when the service parameter Park Monitoring Forward No Retrieve Timer expires. If the parameter value of the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter is blank, then the call will be forwarded to the destination configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires. Specify the following values • Destination-This setting specifies the directory number to which a parked call is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination. • Calling Search Space-A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

Intercom Calling Search Space Infrastructure Configuration Product Fields

Table 95: Intercom Calling Search Space Infrastructure Configuration Product Fields

Field	Description
Intercom Calling Search Space Information	
Name	Enter the intercom calling search space name.
Description	Optional description.
Intercom Route Partitions for this Calling Search Space	
Available Intercom Partitions	Choose an intercom partition in the Available Intercom Partitions list box and add it to the Selected Intercom Partitions list box by clicking the arrow button between the two list boxes.
Selected Intercom Partitions(Ordered by highest priority)	Displays all the selected intercom partition. To change the priority of an intercom partition, choose an intercom partition name in the Selected Intercom Partitions list box. Move the intercom partition up or down in the list by clicking the arrows on the right side of the list box.

Intercom Directory Number Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 96: Intercom Directory Number Infrastructure Configuration Product Fields

Field	Description
Intercom Directory Number Information	
Intercom Directory Number	Enter a phone number.
Route Partition	Choose the intercom partition to which the intercom directory number belongs.
Description	Enter a description of the intercom directory number and intercom route partition.
Alerting Name	Enter a name that you want to display on the phone of the caller.
ASCII Alerting Name	Enter the same information as the Alerting Name field, but limit input to ASCII characters.
Intercom Directory Number Settings	
Calling Search Space	Choose an intercom calling search space.
BLF Presence Group	Choose a BLF Presence Group for this intercom directory number.

Field	Description
Auto Answer	Choose the required auto answer feature for this intercom directory number.
Default Activate Device	Choose a default activated device for this intercom directory number.

Intercom Route Partition Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 97: Intercom Route Partition Infrastructure Configuration Product Fields

Field	Description
Intercom Partition Information	
Name	Enter the intercom partition name.
Description	Optional description.
Time Schedule	Choose the required time schedule.
Time Zone	Choose the required time zone. If you want the time zone to be same as that of the originating device, choose Originating Device. By default Originating Device option is selected.

Intercom Translation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 98: Intercom Translation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Intercom Translation Pattern	Intercom Translation Pattern, including numbers and wildcards (do not use spaces).
Partition	Choose an intercom partition.
Description	Optional description.
Numbering Plan	Choose a numbering plan.
Route Filter	Choosing an optional route filter restricts certain number patterns.
Calling Search Space	Choose the intercom calling search space for which you are adding an intercom translation pattern.

Field	Description
Pattern Definition	
Block this pattern	Choose the reason for which you want this intercom translation pattern to block calls.
Provide Outside Dial Tone	Check this check box to routes the calls off the local network.
Urgent Priority	Check this check box to interrupt interdigit timing and route the call immediately.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transform Mask	Enter a transformation mask value.
Prefix Digits (Outgoing Calls)	Enter the prefix digits.
Calling Line ID Presentation	Used as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis.
Calling Name Presentation	Used as a supplementary service to allow or restrict the originating caller's name on a call-by-call basis.
Connected Party Transformations	
Connected Line ID Presentation	Used as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis.
Connected Name Presentation	Used as a supplementary service to allow or restrict the called party's name on a call-by-call basis.
Called Party Transformations	
Discard Digits	Choose the discard digits instructions that you want to be associated with this intercom translation pattern.
Called Party Transform Mask	Enter a transformation mask value.
Prefix Digits (Outgoing Calls)	Enter the prefix digits.

Line Group Infrastructure Configuration Product Fields

Table 99: Line Group Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
RNA Reversion Timeout	Enter a time, in seconds, after which Cisco Unified Communications Manager 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.
Distribution Algorithm	Select a distribution algorithm, which applies at the line group level.
Hunt Algorithm No Answer	For a given distribution algorithm, select a hunt option for Cisco Unified Communications Manager to use if a call is distributed to a member of a line group that does not answer.
Hunt Algorithm Busy	For a given distribution algorithm, select a hunt option for Cisco Unified Communications Manager to use if a call is distributed to a member of a line group that is busy.
Hunt Algorithm Not Available	For a given distribution algorithm, select a hunt option for Cisco Unified Communications Manager to use if a call is distributed to a member of a line group that is not available.
Directory Numbers	Enter a directory number that already exists in Cisco Unified Communications Manager.

Local Route Group Names Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 100: Local Route Group Names Infrastructure Configuration Product Fields

Field	Description
Local Route Group Names	
Name	Enter a unique local route group name in this required field.
Description	Enter a description that will help you to distinguish between local route group names.

Location Infrastructure Configuration Product Fields

Table 101: Location Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kbps) that is available for all audio calls on the link between this location and other locations. **Note** This option is available for Cisco Unified Communications Manager 9.0 or higher versions.
Video Bandwidth	Enter the maximum amount of video bandwidth (in kbps) that is available for all video calls on the link between this location and other locations. Use 0 for Unlimited and -1 for None. **Note** This option is available for Cisco Unified Communications Manager 9.0 or higher versions.
Links	Bandwidth Between This Location and Adjacent Locations.
Location	Select a location from the list.
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 of all possible paths. Valid values are 0-100.

Media Termination Point Infrastructure Configuration Product Fields

Table 102: Media Termination Point Fields

Field	Description
Media Termination Point Type	Choose Cisco Enhanced Software Termination Point.
Media Termination Point Name	Enter a name for the media termination point upto 15 alphanumeric characters. **Note** You cannot use special characters as the MTP name, for example: !, @, #, $, or %.
Description	Enter any description for the media termination point.
Device Pool	Choose a device pool that has the highest priority.

Trusted Relay Point	Check this checkbox to designate this media termination point (MTP) as a trusted relay point (TRP) that Cisco Unified Communications Manager can use in a network virtualization environment.

Message Waiting Infrastructure Configuration Product Fields

Table 103: Message Waiting Fields

Field	Description
Message Waiting Number	Enter the Cisco Message Waiting directory number.You may use the following characters: 0 to 9, ?, [,], +, -, *, ^, #, !.
Partition	If partitions are being used, choose the appropriate partition from the drop-down list box.
Description	Enter up to 50 characters for a description of the message-waiting directory number. You may use any characters except the following: "", <, >, &, %.
Message Waiting Indicator	Click On or Off.
Calling Search Space	If partitions and calling search spaces are used, from the drop-down list box, choose a calling search space that includes the partitions of the DNs on all phones whose lamps you want to turn on (the partition that is defined for a phone DN must be in a calling search space that the MWI device uses).

Media Resource Group Infrastructure Configuration Product Fields

Table 104: Media Resource Group Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Available Devices	The available media resources that can be selected.
Is Multicast for MOH Audio	Click Yes to use multicast for Music On Hold Audio.

Media Resource Group List Infrastructure Configuration Product Fields

Table 105: Media Resource Group List Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Available Media Resource Group Names	The available media resource groups that can be selected.

Meet-Me Number/Pattern Configuration Product Fields

Table 106: Meet-Me Number/Pattern Configuration Product Fields

Field	Description
Directory Number or Pattern	Enter Meet-Me number/pattern or a range of numbers. To configure a range, the dash must appear within brackets and follow a digit; for example, to configure the range 1000 to 1050, enter 10[0-5]0. This field allows up to 24 characters.
Description	The description can include up to 50 characters. The following characters are not allowed: double-quotes ("), backslash (\), dash (-), percentage sign (%), ampersand (&), or angle brackets (<>).
Partition	To use a partition to restrict access to the Meet-Me number/pattern, choose the desired partition from the drop-down list.
Minimum Security Level	Choose the minimum security level for this Meet-Me number/pattern from the drop-down list. • Choose Authenticated to block participants with nonsecure phones from joining the conference. • Choose Encrypted to block participants with nonsecure phones from joining the conference. • Choose Non Secure to allow all participants to join the conference.

Partition Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 107: Partition Infrastructure Configuration Product Fields

Field	Description
Partition Information	
Name	Enter a partition name.
Description	Enter a description for the partition.
Time Schedule	Choose a time schedule to associate with this partition.
Time Zone	Choose one of the following options to associate a partition with a time zone: • Originating Device—If you choose this option, the system checks the partition against the associated time schedule with the time zone of the calling device. • Specific Time Zone—If you choose this option, the system checks the partition against the associated time schedule at the time that is specified in this time zone.

Recording Profile Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 108: Recording Profile Infrastructure Configuration Product Fields

Field	Description
Name	Enter a the recording profile name.
Recording Calling Search Space	Choose the calling search space that contains the partition of the route pattern that is associated with the SIP trunk that is configured for the recorder.
Recording Destination Address	Enter the directory number (DN) or the URL of the recorder that associates with this recording profile.

Region Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 109: Region Infrastructure Configuration Product Fields

Field	Description
Region Information	
Name	Enter a unique name for this region.
Modify Relationship to other Regions	
Region	The entries in this column display all regions for which non-default relationships have been configured.
Audio Codec Preference List	For each region that is specified in the Regions window pane, choose the corresponding value from the drop-down list box in this column to set the Audio Codec Preference list describing the network conditions between this region and the specified region. • Use System Default—Choose this value to use the system default value for link loss type. • Factory Default Low Loss—Choose this value to specify a low-loss link loss type. • Factory Default Lossy—Choose this value to specify a lossy link loss type.
Maximum Audio Bit Rate	For each region that is specified in the Regions window pane, choose the value from the drop-down list box in this column to set the maximum bit rate to use for audio between this region and the specified region. This setting applies to both audio and video calls and serves as an upper limit for the audio bit rate, which means that audio codecs with higher bit rates than the one that you specify are not used for these calls.
Maximum Session Bit Rate for Video Calls	Enter Kbps value or select either one of the below option in this column: • Use System Default—Select this option to use the default value. • None—If you select this option, the system does not allow video calls.
Maximum Session Bit Rate for Immersive Video Calls	Enter Kbps value or select either one of the below option in this column: • Use System Default—Click this button to use the default value. The default value normally specifies 2000000000 kbps. • None—If you select this option, the system does not allow immersive video calls.

Restriction Table Infrastructure Configuration Product Fields

Table 110: Restriction Table Infrastructure Configuration Product Fields

Field	Description
Remove-Restriction-Pattern	To delete a restriction pattern from a restriction table. The value is restriction pattern alone. This could have multiple values separated by semicolon (;) .For Example : +#99;+91.
Pattern	Enter specific numbers or patterns of numbers that can be permitted or restricted. Include external and long-distance access codes. Use digits 0 through 9 and the following special characters: • * to match zero or more digits. • ? to match exactly one digit. Each ? serves as a placeholder for one digit. • # to correspond to the # key on the phone. • + to call from one country to other country.
Display Name	Enter a descriptive name for the restriction table.
Update-Restriction-Pattern	To update a restriction pattern of a restriction table.This is combination of both restriction pattern and blocked attribute.This could have multiple values separated by semicolon (;) .For Example : +#99/False;+91/true.
New Restriction Patterns are Blocked by Default	Indicate whether new restriction patterns should be flagged as Blocked by default.Default setting: Check box not checked.
Minimum Length of Dial String	Enter the minimum number of digits-including access codes-in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits greater than or equal to the Minimum Length of Dial String value are checked against the restriction table. Dial strings that contain fewer than the Minimum Length of Dial String value are not permitted. For example, to prohibit users from using four-digit numbers, enter 5 in the Minimum Length of Dial String field. Default setting: 1 digit.
Blocked	Check this check box to have Unity Connection prohibit use of phone numbers that match the pattern.

Field	Description
Maximum Length of Dial String	Enter the maximum number of digits-including access codes-in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits fewer than or equal to the Maximum Length of Dial String value are checked against the restriction table. Dial strings that contain more than the Maximum Length of Dial String value are not permitted. For example, if local calls in your area are seven digits long, and you want to prevent users from using long distance phone numbers, enter 8 in the Maximum Length of Dial String field. (A local number plus the access code for the phone system equals 8 digits.)Default setting: 30 digits.
Add-Restriction-Pattern	To add a new restriction pattern to a restriction table.This is combination of both restriction pattern and blocked attribute.This could have multiple values separated by semicolon (;) .For Example : +#99/True;+91/false.

Route Group Infrastructure Configuration Product Fields

Table 111: Route Group Infrastructure Configuration Product Fields

Field	Description
Route Group Information	
Name	Infrastructure Configuration Product name.
Distribution Algorithm	The available options can be chosen.
Ports	If the device supports individually configurable ports, choose the port.
Route Group Member Information	
Find Devices to Add to Route Group	
Device Name contains	Enter the character(s) that are found in the device name that you are seeking and click the Find button. Device names that match the character(s) that you entered display in the Available Devices box.
Available Devices	Choose a device in the Available Devices list box and add it to the Selected Devices list box by clicking Add to Route Group.

Field	Description
Port(s)	If this device supports individually configurable ports, choose the port. (Devices that allow you to choose individual ports include Cisco Access Analog and Cisco MGCP Analog gateways and T1 CAS.) Otherwise, choose the default value (All or None Available, depending upon the device that is chosen). For a device that has no ports available (None Available), the device may already be added to the Route Group or cannot be added to the route group.
Current Route Group Members	
Selected Devices	To change the priority of a device, choose a device name in the Selected Devices list box.
Removed Devices	Choose a device in the Selected Devices list box and add it to the Removed Devices list box.
Route Group Members	
List of devices	This pane displays links to the devices that have been added to this route group. **Note** When you are adding a new route group, this list does not display until you save the route group.

Route List Infrastructure Configuration Product Fields

Table 112: Route List Infrastructure Configuration Product Fields

Field	Description
Route List Information	
Route List Name	Infrastructure Configuration Product name.
Description	Optional description.
Cisco Unified CM Group	List of available Cisco Unified Communications Manager groups.
Enable this Route List	Select Yes to enable the route list.
Run On All Active Unified CM Nodes	To enable the active route list to run on every node, check this check box.
Save	When you click this button to save a route list, a popup message reminds you that you must add at least one route group to this route list for it to accept calls.

Field	Description
Add Route Group	To add a route group to this route list, click this button and perform the procedure to add a route group to a route list.

Route Partition Infrastructure Configuration Product Fields

Table 113: Route Partition Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.

Route Pattern Infrastructure Configuration Product Fields

Table 114: Route Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Pattern	A valid route pattern, including numbers and wildcards.
Route Partition	If you want to use a partition to restrict access to the route pattern, select the desired partition.
Description	Optional description.
Numbering Plan	Numbering plan. The default setting is North American Numbering Plan (NANP).
Route Filter	If your route pattern includes the @ wildcard, you may choose a route filter.
MLPP Precedence	MLPP precedence setting.
For Cisco Prime Collaboration Release 11.5 and later Apply Call Blocking Percentage	Check this check box to enable the Destination Code Control (DCC) feature.
For Cisco Prime Collaboration Release 11.5 and later Blocked Call Percentage	Enter the percentage of calls to be blocked for this destination in numerals. **Note** The Blocked Call Percentage (%) field gets enabled only if the Apply Call Blocking Percentage check box is checked.

Field	Description
For Cisco Prime Collaboration Release 11.5 and later Resource Priority Namespace Network Domain	Choose a Resource Priority Namespace Network Domain from the drop-down list box.
For Cisco Prime Collaboration Release 11.5 and later Route Class	The route class is a DSN code that identifies the class of traffic for a call.
Gateway, Route List, or SIP Trunk	Choose the gateway or route list for which you are adding a route pattern. You can also enter a value that does not appear in the list. If you enter a custom value, specify whether it is a gateway, route list, or SIP trunk. After the name, add one of the following: • [GW]—Gateway • [RL]—Route list • [ST]—SIP trunk For example, gatewayname[GW].
Release Cause	Dependent on the Block Enabled field. If a release cause is selected, then Block Enabled must be set to True.
Allow Device Override	If Yes 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.
Urgent Priority	If Yes is selected, the interdigit timing is interrupted when Cisco Unified Communications Manager must route a call immediately.
For Cisco Prime Collaboration Release 11.5 and later Is an Emergency Service Number	Check this check box, if you are configuring an emergency service number. **Note** This setting is applicable only if the Emergency Location Service is enabled in the call manager.
Call Classification	Indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network.
Provide Outside Dial Tone	If Yes is selected, an outside dial tone is provided.
For Cisco Prime Collaboration Release 11.5 and later External Call Control Profile	Choose the external call profile that you want to assign to the route pattern.

Field	Description
For Cisco Prime Collaboration Release 11.5 and later Allow Overlap Sending	Check this check box to configure Allow Overlap Sending flag in the Route Pattern.
For Cisco Prime Collaboration Release 11.5 and later Require Forced Authorization Code	If you want to use forced authorization codes with this route pattern, check this check box.
For Cisco Prime Collaboration Release 11.5 and later Authorization Level	Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that needs to successfully route a call through this route pattern.
For Cisco Prime Collaboration Release 11.5 and later Require Client Matter Code	If you want to use client matter codes with this route pattern, check this check box.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Select Yes if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transformation Mask	Transformation mask value.
Calling Party Prefix Digits (Outgoing Calls) This field renamed as Prefix Digits (Outgoing Calls) from Cisco Prime Collaboration 11.5 and later.	Prefix digits.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this route pattern.
Calling Name Presentation	Determines whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party's name on the called party's phone display for this route pattern.
For Cisco Prime Collaboration Release 11.5 and later Calling Party Number Type	Format for the number type in calling party directory numbers.
For Cisco Prime Collaboration Release 11.5 and later Calling Party Numbering Plan	Format for the numbering plan in calling party directory numbers.
Connected Party Transformations	

Field	Description
Connected Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this route pattern.
Connected Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's name on the calling party's phone display for this route pattern.
Called Party Transformation	
Called Party Discard Digits (Outgoing Calls)	Determines the discard digits instructions that you want to associate with this route pattern.
Called Party Transformation Mask	Transformation mask value.
For Cisco Prime Collaboration Release 11.5 and later Prefix Digits (Outgoing Calls)	Prefix digits.
For Cisco Prime Collaboration Release 11.5 and later Called Party Number Type	Format for the number type in calling party directory numbers.
For Cisco Prime Collaboration Release 11.5 and later **For Cisco Prime Collaboration Release 11.5 and later** Called Party Numbering Plan	Format for the numbering plan in calling party directory numbers.
For Cisco Prime Collaboration Release 11.5 and later Network Service Protocol	Choose the PRI protocol that matches the protocol of the terminating gateway.
For Cisco Prime Collaboration Release 11.5 and later Carrier Identification Code	Carrier identification codes allow you to reach the services of interexchange carriers.
Network Service	Network Service.
Service Parameter Value	Service parameter value, valid entries include the digits 0 to 9.

Service Profile Infrastructure Configuration Product Fields

Table 115: Service Profile Infrastructure Configuration Product Fields

Field	Description
Name	Enter the name of the service profile. Maximum characters: 50 (ASCII only). Allowed Values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Description	(Optional) Enter a description that helps you to distinguish between service profiles when you have more than one configured. Allowed Values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Default profile	Check this check box to make this service profile the default option for the system. If you specify a default service profile, end users that do not have an associated service profile automatically inherit the default service profile settings.
Voicemail Profile	
Primary	Select the primary voicemail server with which you want to associate this service profile.
Secondary	Select a secondary voicemail server, if applicable.
Tertiary	Select a tertiary voicemail server, if applicable.
Credentials source for voicemail service	If user credentials for the voicemail service are shared with another service, select the appropriate service. The user credentials automatically synchronize from the service that you select. Default Setting: Not set
Mailstore Profile	
Primary	Select the primary mailstore server with which you want to associate this service profile.
Secondary	Select a secondary mailstore server, if applicable.
Tertiary	Select a tertiary mailstore server, if applicable.
Inbox folder	The name of the folder on the mailstore server in which to store new messages. Only change this value if the mailstore server uses a different folder name from the default folder. Default: Inbox
Trash folder	The name of the folder on the mailstore server in which to store deleted messages. Only change this value if the mailstore server uses a different folder name from the default folder. Default: Deleted Items

Polling Interval (in seconds)	The time (in seconds) that can elapse between polls of the IMAP server for new voice messages, when IDLE is not supported by the mailstore or when a connection failure occurs. Allowed values: 60 - 900 Default: 60
Allow dual folder mode	This dual folder setting is checked by default for use with mailstores that support the IMAP UIDPLUS extensions (RFC 2359 and 4315). By default, the Client Services Framework (CSF) detects if UIDPLUS is not supported and automatically reverts to Single Folder mode. Uncheck this check box if you know that UIDPLUS is not supported and you want to force the system to use Single Folder mode. Default: True
Conferencing Profile	
Primary	Select the primary conferencing server with which you want to associate this service profile.
Secondary	Select a secondary conferencing server, if applicable.
Tertiary	Select a tertiary conferencing server, if applicable.
Server Certificate Verification	Specify how the conferencing server associated with this profile supports TLS connections. This setting is for TLS verification of the conferencing servers listed for this conferencing profile. Select from the following options: • Any Certificate: Cisco Jabber accepts all valid certificates. • Self Signed or Keystore: Cisco Jabber accepts the certificate if the certificate is self-signed, or the signing Certificate Authority certificate is in the local trust store. **Note** A keystore is a file that stores authentication and encryption keys. Cisco Jabber accepts only certificates that are defined in the keystore. You must import the certificate or its Certificate Authority signing certificate into the local trust store.
Credentials source for web conferencing service	If user credentials for the meeting service are shared with another service, select the appropriate service. The user credentials automatically synchronize from the service that you select. Default Setting: Not set
Directory Profile	
Primary	Select the primary directory server with which you want to associate this service profile.
Secondary	Select a secondary conferencing server, if applicable. If you do not set up any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.

Tertiary	Select a tertiary conferencing server, if applicable. If you do not set up any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.
Use UDS for contact resolution	Check this check box if you want to use the UDS service provided in Cisco Unified Communications Manager for the directory lookup instead of external directory.
Use Logged On User Credential	Check this check box to prevent anonymous queries and force the user to enter credentials to sign in to the LDAP server.
Username	Enter the distinguished name for the user ID that is authorized to run queries on the LDAP server, in the format useraccount@domain.com. Maximum length: 128
Password	Enter the password for the Username that is authorized to run queries on your LDAP server. Maximum length: 128
Search Base	This field allows you to narrow your Cisco Unified Personal Communicator contact search queries to a certain part of the LDAP directory. Enter the container or directory on the LDAP server where you have configured your LDAP users. Example for the search base wtih Microsoft Active Directory integration: cn=users,DC=EFT-LA,DC=cisco,DC=com. Maximum length: 256
Recursive Search on All Search Bases	Check this check box to perform a recursive search of the directory starting at the search base. Recursive search allows for Cisco Unified Personal Communicator contact search queries to search all of the LDAP directory tree from a given search context (search base).
Search Timeout (seconds)	Set the default timeout for searches (default is 5 seconds).
Base Filter (Only used for Advance Directory)	Use this option only if the object type that you want to retrieve with queries that you execute against Active Directory is not a user object. Maximum length: 256
IM and Presence Profile	
Primary	Select the primary IM and Presence server with which you want to associate this service profile.
Secondary	Select a secondary conferencing server, if applicable.
Tertiary	Select a tertiary conferencing server, if applicable.
CTI Profile	
Primary	Select the primary CTI server with which you want to associate this service profile.
Secondary	Select a secondary CTI server, if applicable.
Tertiary	Select a tertiary CTI server, if applicable.

SIP Route Pattern Infrastructure Configuration Product Fields

Table 116: SIP Route Pattern Infrastructure Configuration Product Fields

Field	Description
Use Calling Party's External Phone Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.
Description	For this optional entry, 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 (<>).
Calling Line ID Presentation	Uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want your system 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.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9 and the wildcard characters asterisk (*) and octothorpe (#). The appended prefix digit does not affect which directory numbers route to the assigned device.
SIP Trunk/Route List	(Required) From the drop-down list choose the SIP trunk or route list to which the SIP route pattern should be associated. Click Edit to open the trunk or route list in the Trunk or Route List Configuration window. URI dialing is available over SIP trunks only. If you are using URI dialing and you select a route list from this drop-down list box, the route list must contain route groups with SIP trunks only.

Field	Description
IPv6 Pattern	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. If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv4 Pattern in addition to the IPv6 Pattern.
IPv4 Pattern	(Required) Enter the domain, sub-domain, IPv4 address, or IP subnetwork address. For DomainRouting pattern usage, enter adomain name IPv4 Pattern field that can resolve to an IPv4 address. The domain namecan contain the following characters: [, -, ., 0-9, A-Z, a-z, *, and]. For IPAddress Routing pattern usage, enter an IPv4 address the IPv4 Pattern field that follows the format X.X.X.X, where X representsa number between 0 and 255. For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, X.X.X.X/Y; where Y is the network prefix that denotes the number of bits in the address that will be the network address. If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.
Connected Line ID Presentation	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 your system 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 your system to block the display of the connected party phone number. If a call that originates from an IP phone on your system 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.

Field	Description
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9 and the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not checked, no calling party transformation takes place.
Connected Line Name Presentation	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 your system 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 your system to display the connected party name. Choose Restricted if you want your system to block the display of the connected party name.
Calling Line Name Presentation	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 your system 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 your system to display the calling name information. Choose Restricted if you want your system to block the display of the calling name information.
Block Pattern	If you do not want this pattern to be used for routing calls, click the Block Pattern check box.
Pattern Usage	(Required) From the drop-down list, choose either Domain Routing or IP Address Routing.

Field	Description
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, choose <None> for the partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more than 250 partitions are specified by using the Max List Box Items enterprise parameter, the Find button displays next to the drop-down list box. Click the Find button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click Add Selected. To set the maximum list box items, choose System>> Enterprise Parameters>> and choose CCMAdmin Parameters. Make sure that the combination of SIP route pattern, route filter, and partition is unique within the cluster.

SIP Trunk Infrastructure Configuration Product Fields

Table 117: SIP Trunk Infrastructure Configuration Product Fields

Field	Description
AAR Group	The Automated Alternate Routing (AAR) group provides the prefix digits that are used to route calls that are otherwise blockedbecause of insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Call Classification	Determines whether an incoming call that is using this trunk is considered off the network (OffNet) or on the network (OnNet), or should use the system default setting.

Field	Description
Common Device Config	Choose the common device configuration for which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration page.
Connected Party Transformation CSS	Choose to transform the connected party number on the device in order to display the connected number in another format, such as a DID or E164 number. Cisco Unified Communications Manager includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages. Ensure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. If you configure the Connected Party Transformation CSS as None, the transformation does not match and is not applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Device Name	Object name.
Description	Optional description.
Device Pool	List of available device pools. The device pool specifies a collection of properties for this device, including Unified CM Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Location	Specifies the total bandwidth that is available for calls between this location and the central location (or hub). A location setting of Hub_None specifies unlimited available bandwidth.
Media Resource Group List	Provides 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 according to the priority order that is defined in a Media Resource Group List.

Field	Description
Media Termination Point Required	Used to indicate whether a media termination point (MTP) is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use a media termination point to implement features. Deselect the Media Termination Point Required check box if you do not want to use a media termination point to implement features. Check this check box only for H.323 clients and those H.323 devices that do not support the H.245 Empty Capabilities Set, or if you want media streaming to terminate through a single source. If you check this check box to require an MTP, and either device is a video endpoint, the call operates as audio only.
Retry Video Call as Audio	Applies to video endpoints that receive calls. For trunks, it pertains to calls that are received from Cisco Unified Communications Manager but not to calls that are received from the wide area network (WAN). By default, the system checks 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 uncheck this check box, a video call that fails to connect as video will not try to establish an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and (or) route or hunt list.
Unattended Port	If selected, calls can be redirected, transferred, or forwarded to an unattended port, such as a voice mail port. The default value is deselected.

Field	Description
SRTP Allowed	Select if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the trunk. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP. If you check this check box, it is recommended that you configure IPSec, so you do not expose keys and other security-related information during call negotiations. If you do not configure IPSec correctly, you must consider signaling between Cisco Unified Communications Manager and the gateway as nonsecure.

Field	Description
Use Trusted Relay Point	From the list, enable or disable whether Cisco Unified Communications Manager inserts a Trusted Relay Point (TRP) device with this media endpoint. Choose one of the following values: • 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. A TRP device designates an MTP or transcoder device that is labeled as a TRP. Cisco Unified Communications Manager 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 is used as the required MTP. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP.
Incoming Calling Party Unknown Number Prefix	If this is set to Default, the Call Processor uses the prefix at the next level setting (Device Pool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty, in which case no prefix is assigned.

Field	Description
MLPP Domain	Choose an MLPP Domain to associate with this device. If you leave this field empty, the device inherits its MLPP Domain from the value that was set for the device pool. 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.
Remote-Party-Id	Allows the SIP Trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Cisco Unified Communications Manager to the remote destination. If you select Yes, the SIP Trunk always sends the RPID header.
Asserted-Identity	Allows the SIP Trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you select Yes, the SIP Trunk always sends the Asserted-Type header. Whether the SIP Trunk sends the SIP Privacy header depends on the SIP Privacy configuration. If you select No, the SIP Trunk does not include any Asserted-Type or SIP Privacy headers in its SIP messages. For more information, see the descriptions of Asserted-Type and SIP Privacy in this table.

Field	Description
Asserted-Type	Specifies the type of Asserted Identity header that SIP Trunk messages should include. Select one of the following values: • Default—Represents the default value. Screening indication information that the SIP Trunk receives from Cisco Unified Communications Manager Call Control determines the type of header the SIP Trunk sends. • PAI—The Privacy-Asserted Identity (PAI) header is sent in outgoing SIP Trunk messages. This value overrides the screening indication value that comes from Cisco Unified Communications Manager. • PPI—The Privacy Preferred Identity (PPI) header is sent in outgoing SIP Trunk messages. This value overrides the screening indication value that comes from Cisco Unified Communications Manager. **Note** These headers are sent only if the Asserted Identity check box is checked.

Field	Description
SIP Privacy	Specifies the type of SIP privacy header for SIP Trunk messages to include. Select one of the following values: • Default—Represents the default value. Name and number presentation values that the SIP Trunk receives from the Cisco Unified Communications Manager Call Control compose the SIP Privacy header. For example: • If the name and number presentation is restricted, the SIP Trunk sends the SIP Privacy header. • If the name and number presentation is allowed, the SIP Trunk does not send the Privacy header. • None—The SIP Trunk includes the header Privacy:none, which means that presentation is allowed. This value overrides the Presentation information that comes from Cisco Unified Communications Manager. • ID—The SIP Trunk includes the header Privacy:id, which means that the presentation is restricted for both name and number. This value overrides the presentation information that comes from Cisco Unified Communications Manager. • ID Critical—The SIP Trunk includes the header Privacy:id;critical, which means that presentation is restricted for both name and number. The critical label means that privacy services that are requested for this message are critical, and if the network cannot provide these privacy services, this request should be rejected. This value overrides the presentation information that comes from Cisco Unified Communications Manager. **Note** These headers are sent only if the Asserted Identity check box is checked.

Field	Description
Significant Digits	Represents the number of final digits that are retained on inbound calls. It is used 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 H.323 device. Select the number of significant digits to collect (0 to 32). Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called.
Connected Party ID Presentation	Cisco Unified Communications Manager 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. The default value is Default, which translates to Allowed. Select Default if you want Cisco Unified Communications Manager to send connected line information. Select Restricted if you do not want Cisco Unified Communications Manager to send connected line information.
Connected Name Presentation	Cisco Unified Communications Manager 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. The default value is Default, which translates to Allowed. Select Default if you want Cisco Unified Communications Manager to send connected name information. Select Restricted if you do not want Cisco Unified Communications Manager to send connected name information.
Calling Search Space	Available calling search spaces.
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.
Prefix DN	The prefix digits that are appended to the called party number on incoming calls.

Field	Description
Redirecting Diversion Header Delivery - Inbound	Select Yes (the default) to accept the Redirecting Number in the incoming invite message to the Cisco Unified Communications Manager. Select No to exclude the Redirecting Number in the incoming invite message to the Cisco Unified Communications Manager. You use Redirecting Number for voice messaging integration only. If your configured voice messaging system supports Redirecting Number, you should select Yes.
Called Party Transformation CSS	Allows you to localize the called party number on the device. The Called Party Transformation CSS that you choose must contain the called party transformation pattern that you want to assign to this device. If you configure the Called Party Transformation CSS as None, the transformation does not match and is not 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 Yes to use the Called Party Transformation CSS that is configured in the device pool that is assigned to this device. If you select No, the device uses the Called Party Transformation CSS that was configured for the device in the Trunk Configuration page.
Calling Party Transformation CSS	Enables you to localize the calling party number on the device. Ensure 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 Calling Party Transformation CSS as None, the transformation will not match and will not be applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

Field	Description
Calling Party Selection	Select the directory number that is sent on an outbound call on a gateway. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Sends the directory number of the redirecting device. • Last Redirect Number—Sends the directory number of the last device to redirect the call. • First Redirect Number (External)—Sends the external directory number of the redirecting device. • Last Redirect Number (External)—Sends the external directory number of the last device to redirect the call.
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP) as a supplementary service to control the display of the calling party number on the called party phone display screen. Select one of the following options: • Default—If you do not want to change the presentation setting. • Allowed—If you want the calling number information to be displayed. • Restricted—If you do not want the calling number information to be displayed.

Field	Description
Calling Name Presentation	Cisco Unified Communications Manager uses 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 the following options: • Default—If you do not want to change the presentation setting. • Allowed—If you want Cisco Unified Communications Manager to send calling name information. • Restricted—If you do not want Cisco Unified Communications Manager to send the calling name information.
Caller ID DN	Enter the pattern (0 to 24 digits) that you want to use to format the caller 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 appends the number with the area code if it is not specified. • 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 central office appends the number with the area code if it is not specified.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP device.
Redirecting Diversion Header Delivery - Outbound	If Yes is selected, the redirecting number is included in the outgoing invite message from Cisco Unified Communications Manager to indicate the original called party number and the redirecting reason for the call when the call is forwarded. If No is selected, the first redirecting number and the redirecting reason are excluded from the outgoing invite message. The redirecting number is used for voice messaging integration only. If your configured voice messaging system supports redirecting Number, you should select Yes.

Field	Description
Destination Address	The remote SIP peer with which this trunk will communicate. The allowed values for this field are a valid V4 IP address, a fully qualified Domain name, or a DNS SRV record (applies only if *yes* is selected in the Destination Address is an SRV field). SIP trunks only accept incoming requests from the configured destination address and the incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Cisco Unified Communications Manager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster.
Destination Address is an SRV	Specifies that the configured Destination Address is an SRV record.
Destination Port	Enter the destination port. Ensure that the value you enter specifies a port between 1024 and 65535 (the default value is 5060). You can specify the same port number for multiple trunks. Do not enter a value if the destination address is a DNS SRV port. The default port number 5060 indicates a SIP port.
Geolocation	An unspecified geolocation, which designates that this device does not associate with a geolocation. You can also select a geolocation that has been configured.
Geolocation Filter	Specifies the geolocation filter for the device.
Incoming Port	Incoming port number.
Outgoing Transport Type	Outgoing transport type (TCP or UDP).
MTP Preferred Originating Codec	Indicates the preferred outgoing codec. To configure G.711/G.729 codecs for use with a SIP Trunk, you must use a hardware MTP or transcoder that supports the G.711/G.729 codec.
Send Geolocation Information	Sends the geolocation information for the associated device.

Field	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 Cisco Unified Communications Manager 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. To identify the settings that the profile contains, on Cisco Unified Communications Manager choose **System > Security Profile > SIP Trunk Security Profile**. For information on how to configure security profiles, see *Cisco Unified Communications Manager Security Guide*.
Rerouting Calling Search Space	Determines where a SIP user (A) can refer another user (B) to a third party (C). After the referral 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).
Out-Of-Dialog Refer Calling Search Space	Used when a Cisco Unified Communications Manager refers a call (B) coming in to a SIP user (A) to a third party (C) when there is no involvement of a SIP user (A). In this case, the system uses the out-of-dialog calling search space of the SIP user (A).

Field	Description
Packet Capture Mode	Exists only for troubleshooting encryption. Packet capturing may cause high CPU usage or call-processing interruptions. Select one of the following options: • None—This option, which is the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified Communications Manager writes the decrypted or non encrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager 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 message. The IREC 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. You do not have to reset the trunk after enabling or disabling Packet Capture.
Packet Capture Duration	Exists only for troubleshooting encryption. Packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes allotted for one session of packet capturing. The default setting is 0, and the range is from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value “0” is displayed.

Field	Description
Presence Group	Configures the Unified Presence features. Select a Presence group for the SIP trunk. The selected group specifies the destinations that the device, application, or server that is connected to the SIP trunk can monitor. The default value for Presence Group specifies Standard Presence group, which is configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups.
PSTN Access	Indicates that the calls made through this trunk might reach the PSTN. Check this check box even if all calls through this trunk device do not reach the PSTN. For example, check this check box for tandem trunks or an H.323 gatekeeper-routed trunk if calls might go to the PSTN. When checked, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. By default, this check box remains checked.
Route Class Signaling Enabled	From the drop-down list, enable or disable route class signaling for the port. Select one of the following values: • Default—If you choose this value, the device uses the setting from the Route Class Signaling service parameter. • Off—Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter. • On—Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the Hotline feature.

Field	Description
Subscribe Calling Search Space	Determines how Cisco Unified Communications Manager routes presence requests from the device, server, or 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. Select a Subscribe calling search space to use for presence requests for the SIP Trunk. All calling search spaces that you configure in Cisco Unified Communications Manager Administration appear in the Subscribe Calling Search Space drop-down list box. If you do not select a different calling search space for the SIP Trunk from the drop-down list, the Subscribe calling search space defaults to None. To configure a Subscribe calling search space specifically for this purpose, you can configure a calling search space as you do all calling search spaces.
SIP Profile	Select the SIP profile that is to be used for this SIP Trunk.

Field	Description
Trunk Service Type	Specifies the type of the Trunk Service. Select one of the following options: • None—Select this option if the trunk will not be used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine. • Call Control Discovery—Selecting this option enables the trunk to support call control discovery. If you assign this trunk to the CCD advertising service in the Advertising Service window, the trunk handles inbound calls from remote call-control entities that use the SAF network. If you assign this trunk to the CCD requesting service in the Requesting Service window, the trunk handles outgoing calls to learned patterns. • Extension Mobility Cross Cluster—Select 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 unchecked 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.

Field	Description
Transmit UTF-8 for Calling Party Name	Specifies 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 check 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. The default value for Transmit UTF-8 for Calling Party Name leaves the check box unchecked.
Use Device Pool Connected Party Transformation CSS	Enables you to use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device. If you do not check this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.

Field	Description
DTMF Signaling Method	Select one of the following options: • No Preference (default)—Cisco Unified Communications Manager will pick the DTMF method to negotiate DTMF, so an MTP is not required for the call. If Cisco Unified Communications Manager does not have a choice but to allocate an MTP (if the Media Termination Point Required check box is checked), SIP Trunk will negotiate DTMF to RFC 2833. • RFC 2833—Select this configuration if the preferred DTMF method to be used across the trunk is RFC 2833. Cisco Unified Communications Manager makes every effort to negotiate RFC 2833 regardless of MTP usage. Out-of-band provides the fallback method if the peer endpoint supports it. • OOB and RFC 2833—Select this configuration if both out-of-band and RFC 2833 should be used for DTMF. If the peer endpoint supports both out-of-band and RFC 2833, Cisco Unified Communications Manager will negotiate both out-of-band and RFC 2833 DTMF methods. As a result, two DTMF events are sent for the same DTMF keypress (one out-of-band and the other RFC 2833).

Note You can provision SIP Trunk infrastructure Configuration Products in Session Management Edition (SME) devices if you add the SME device as a Call Processor in Provisioning.

SIP Profile Infrastructure Configuration Product Fields

Table 118: SIP Profile Infrastructure Configuration Product Fields

Field	Description
Name	Name of the SIP profile.
Description	Description of the SIP profile.

Field	Description
Default MTP Telephony Event Payload Type	Specifies the default payload type for RFC2833 telephony event.
Resource Priority Namespace List	Select a configured Resource Priority Namespace Network Domain list.
Early Offer for G Clear Calls	It supports both standards-based G.Clear (Clearmode) and proprietary Cisco Session Description Protocols (SDP).
SDP Session-level Bandwidth Modifier	Bandwidth needed when all the media streams are used. There are three Session Level Bandwidth Modifiers: Transport Independent Application Specific (TIAS), Application Specific (AS), and Conference Total (CT). Select one of the following options to specify which Session Level Bandwidth Modifier to include in the SDP portion of SIP Early Offer or Reinvite requests. • TIAS and AS • TIAS only • AS only • CT only Supported only for Cisco Unified Communications Manager 8.6.2 and above.

Field	Description
User-Agent and Server header information	This feature indicates how Cisco Unified Communications Manager handles the User-Agent and Server header information in a SIP message. Choose one of the following three 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. Cisco Unified Communications Manager passes through any contact headers untouched. This is the default behavior. • Pass Through Received Information as Contact Header Parameters —If this option is selected, the User-Agent or Server header information is passed as Contact header parameters. The User-Agent or Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent or Server headers. • Pass Through Received Information as User-Agent and Server Header—If this option is selected, the User-Agent or Server header information is passed as User-Agent or Server headers. The User-Agent or Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent or Server headers. Supported only for Cisco Unified Communications Manager 8.6.2 and above.
Accept Audio Codec Perferences in Received Offer	Select On to enable Cisco Unified Communications Manager to honor the preference of audio codecs in received offer and preserve it while processing. Select Off to enable Cisco Unified Communications Manager to ignore the preference of audio codecs in received offer and apply the locally configured Audio Codec Preference List. The default will select the service parameter configuration.

Field	Description
Dial String Interpretation	Cisco Unified Communications Manager uses the Dial String Interpretation policy to determine if the SIP identity header is a directory number or directory URI. Because directory numbers and directory URIs are saved in different database lookup tables, Cisco Unified Communications Manager examines the characters in the SIP identity header's user portion, which is the portion of the SIP address that is before the @ sign (for example, user@IP address or user@domain). To configure the Dial String Interpretation, choose one of the following options from the drop-down list box: • Always treat all dial strings as URI addresses—Cisco Unified Communications Manager treats the address of incoming calls as if they were URI addresses. • Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI. • Phone number consists of characters 0-9, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI. **Note** If the user=phone tag is present in the Request URI, Cisco Unified Communications Manager always treats the dial string as a number regardless of what option you choose for the Dial String Interpretation field.

Field	Description
Redirect by Application	Check this check box to configure this SIP Profile on the SIP trunk, which allows the Cisco Unified Communications Manager administrator to: • 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 call is routed correctly. • Prevent DOS attack by limiting the number of redirections (recursive redirections) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place.
Disable Early Media on 180	Check this check box to play local ringback on the calling phone and connect the media upon receipt of the 2000K response.
Outgoing T.38 INVITE include audio mline	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, you must configure a SIP trunk with this SIP profile.
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media.
Assured Services SIP conformance	This checkbox should be checked for third-party AS-SIP endpoints as well as 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.
MLPP User Authorization	Check this box to enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password.
Timer Invite Expires	The time, in seconds, after which a SIP Invite expires.
Timer Register Delta	Specifies the parameter is in conjunction with the Timer Register Expires setting. The phone re-reregisters Timer Register Delta seconds before the registration period ends. The registration period is determined by the value of the SIP Station KeepAlive Interval service parameter.

Field	Description
Timer Register Expires	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) is the default value. In the 2000K response to Register message, Cisco Unified Communications Manager will include an Expires header with the configured value of the SIP Station KeepAlive Interval service parameter. This value in the 2000K determines the time, in seconds, after which the registration expires. The phone refreshes the registration Timer Register Delta seconds before the end of this interval.
Timer T1	The lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number.
Timer T2	The highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number.
Retry INVITE	The maximum number of times that an Invite request will be transmitted. Valid values include any positive number.
Retry Non-INVITE	The maximum number of times that an Invite request will be retransmitted. Valid values include any positive number.
Start Media Port	The start real-time protocol (RTP) port for media. The ranges is from 16384 to 32767.
Stop Media Port	The stop real-time protocol (RTP) port for media. The ranges is from 16384 to 32767.
Call Pickup URL	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call pickup feature.
Call Pickup Group Other URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call pickup group other feature.
Call Pickup Group URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call pickup group feature.

Field	Description
Meet Me Service URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the meet me conference feature.
User Info	Configures the user = parameter in the Register message.
DTMF DB Level	Specifies in-band DTMF digit tone level.
Call Hold Ring Back	Allows the system to ring to let you know that you still have another party on hold.
Anonymous Call Block	Configures anonymous call block.
Caller ID Blocking	Configures the caller ID blocking.
Do No Disturb Control	Enables the Do Not Disturb feature.
Telnet Level for 7940 and 7960	Controls the telnet level configuration parameter for phones that support Telnet.
Timer Keep Alive Expires	Specifies the interval between keepalive messages that are sent to the backup Cisco Unified Communications Manager to ensure that it is available in the event that a failover is required.
Timer Subscribe Expires	Specifies the time, in seconds, after which a subscription expires. This value is inserted into the Expires header field.
Timer Subscribe Delta	Resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires.
Maximum Redirections	Specifies the maximum number of times that the phone will allow a call to be redirected before dropping the call.
Off Hook To First Digit Timer	Specifies the time, in microseconds, that passes when the phone goes off hook and the first digit timer is set. The range is from 0 - 150,000 microseconds.
Call Forward URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call forward feature.
Abbreviated Dial URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the abbreviated dial feature.

Field	Description
Conference Join Enabled	Specifies whether the Cisco Unified IP Phones 7940 or 7960, when the conference initiator that is using that phone hangs up, should attempt to join the remaining conference attendees.
RFC 2543 Hold	Specifies whether to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Cisco Unified Communications Manager. This allows backward compatibility with endpoints that do not support RFC3264.
Semi Attended Transfer	Specifies whether the Cisco Unified IP Phones 7940 or 7960 caller can transfer the second leg of an attended transfer while the call is ringing. Check the check box if you want semi attended transfer enabled; leave it unchecked if you want semi attended transfer disabled.
Enable VAD	Specifies whether you want voice activation detection (VAD) enabled; leave it unchecked if you want VAD disabled. When VAD is enabled, no media are transmitted when voice is detected.
Stutter Message Waiting	Specifies whether you want stutter dial tone when the phone goes off hook and a message is waiting; leave unchecked if you do not want a stutter dial tone when a message is waiting.
Incoming Requests FROM URI Settings	
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	

Field	Description
Reroute Incoming Request to new Trunk based on	Specifies the method that Cisco Unified Communications Manager uses to identify the SIP trunk where the call is rerouted.
RSVP Over SIP	Specifies the method that Cisco Unified Communications Manager uses to configure RSVP over SIP trunks.
Fall back to local RSVP	Allows failed end-to-end RSVP calls to fall back to local RSVP to establish the call.
SIP Rel1XX Options	Configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) are sent reliably to the remote SIP endpoint.
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 box, select one of the following three options • Immersive—High-definition immersive video. • Desktop—Standard desktop video. • Mixed—A mix of immersive and desktop video. Cisco Unified Communications Manager Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, Video Bandwidth or Immersive Bandwidth, depending on the type of call determined by the Video Call Traffic Class. Please refer to the Call Admission Control chapter of the Cisco Unified Communications Manager System Guide for more information.
Calling Line Identification Presentation	Select Strict From URI presentation Only to select the network provided identity. Select Strict Identity Headers presentation Only to select the user provided identity.

Field	Description
Deliver Conference Bridge Identifier	Check this check box for the SIP trunk to pass the b-number that identifies the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require that this field be enabled. Checking this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Enabling this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference. Supported only for Cisco Unified Communications Manager 8.5 and above.
Early Offer support for voice and video calls (insert MTP if needed)	Check this check box if you want to create a trunk that supports early offer. Supported only for Cisco Unified Communications Manager 8.5 and above.
Send send-receive SDP in mid-call Invite	Check this check box to prevent Cisco Unified Communications Manager from sending an Invite a=inactive SDP message during call hold or media break during supplementary services. Supported only for Cisco Unified Communications Manager 8.5 and above.
Allow Presentation Sharing using BFCP	If the box is checked, Cisco Unified Communications Manager is configured to allow supported SIP endpoints to use the Binary Floor Control Protocol to enable presentation sharing.
Allow iX Application	Check this check box to enable support for iX media channel.
Allow Passthrough of Configured Line Device Caller Information	Check this box to allow passthrough of configured line device caller information from the SIP trunk.
Reject Anonymous Incoming Calls	Check this box to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Check this box to reject anonymous outgoing calls.
SIP Options Ping	

Field	Description
Enable Options Ping to monitor destination status for Trunks with service type “None (Default)”	Check this check box if you want to enable the SIP Options feature. Supported only for Cisco Unified Communications Manager 8.5 and above.
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. Supported only for Cisco Unified Communications Manager 8.5 and above versions.
Ping Interval for Out-of-service SIP 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. Supported only for Cisco Unified Communications Manager 8.5 and above versions.
Ping Retry Timer (milliseconds)	This field specifies the maximum waiting time before retransmitting the Options request. Supported only for Cisco Unified Communications Manager 8.5 and above versions.
Ping Retry Count	This field specifies the number of times that Cisco Unified Communications Manager resends the Options request to the remote peer. Supported only for Cisco Unified Communications Manager 8.5 and above versions.

SIP Realm Infrastructure Configuration Product Fields

Table 119: SIP Realm Infrastructure Configuration Product Fields

Field	Description
Realm	Enter the domain name of the realm that connects to the SIP trunk.
User	Enter the username of the SIP user agent in this realm.
Digest Credentials	Enter the password that the Cisco Unified CM uses to respond to a challenge from this realm and user.

Softkey Template Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 120: Softkey Template Infrastructure Configuration Product Fields

Field	Description
Softkey Template Information	
Name	Enter a unique name to identify the softkey template.
Description	Enter a description that describes the use of the template.
Base SoftKey Template Name	Select the base SoftKey template name from the drop-down list.
Is Default SoftKey Template	Check the **Is Default Softkey Template** check box to designate this softkey template as the standard softkey template,

SRST Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 121: SRST Infrastructure Configuration Product Fields

Field	Description
SRST Reference Information	
Name	Enter a name in the SRST Reference Name field.
Port	Enter the port number for this SRST reference.
IP Address	Enter the IP address of the gateway for devices in a device pool to use as an SRST reference.
SIP Network/IP Address	Enter the IP address of the server that the phones that are running SIP will use when in SRST mode.
SIP Port	Enter the SIP port of the SRST gateway.
SRST Certificate Provider Port	This port monitors requests for the Certificate Provider service on the SRST-enabled gateway.
Is SRST Secure?	After you verify that the SRSTenabled gateway contains a self-signed certificate, check this check box.

Transfer Rule Infrastructure Configuration Product Fields

Table 122: Transfer Rule Infrastructure Configuration Product Fields

Field	Description
Tell Me Who the Call Is For	Check this check box to have Unity Connection say “call for ” or “call for ” when the user answers the phone. Use this setting when users share a phone or a user takes calls from more than one dialed extension. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.
If Extension is Busy	Indicate how Unity Connection handles calls when the phone is busy. You may want to use holding options sparingly, because calls on hold can tie up ports. • Send Callers to Voicemail—Unity Connection plays the busy greeting and allows the caller to leave a voice message. • Put Callers on Hold Without Asking—Unity Connection puts callers on hold. • Ask Callers to Hold—Unity Connection gives the caller the option of holding. These options are unavailable when Release to Switch is selected or when Transfer Calls To is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly.

Field	Description
Rings to Wait For	Select the number of times the extension rings before Unity Connection plays the user or handler greeting. Set this value to at least three to give users a chance to answer. Avoid setting to more than four, especially if the call may be transferred to another extension, where the caller might have to wait for another set of rings. This value should be at least two rings fewer than the phone system setting for forwarding calls. This option is unavailable when Transfer Incoming Calls is set to the Greeting option or when Release to Switch is selected. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly.
Ask Me If I Want to Take the Call	Check this check box to have Unity Connection ask users whether they want to take a call before transferring the call. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.
Transfer Rule Type	The name of the transfer rule.Select the Rule Name to go to the specific page for the transfer rule. • Alternate • Closed • Standard

Field	Description
Ask for Caller's Name	Check this check box to have Unity Connection prompt callers to say their names. When answering the phone, the user hears "Call from..." before Unity Connection transfers the call. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.
Call Handler	Name of the Call Handler for which Transfer Rules needs to be updated.
Extension	Enter an extension or URI to which the call is forwarded.
Play the Wait While I Transfer Your Call Prompt	Check this check box to have Unity Connection play “Wait while I transfer your call” to callers while performing the transfer. This option is unavailable when Transfer Incoming Calls is set to the Greeting option. Default setting: Check box checked.
Tell Me When the Call Is Connected	Check this check box to have Unity Connection say "transferring call" when the user answers the phone. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.

Field	Description
Status	Indicate whether the transfer option is enabled and for how long: • Disabled—The transfer option is not in effect. • Enabled With No End Date and Time(Enabled Always)—The transfer option is enabled until you disable it. • Enabled Until—Unity Connection performs the selected transfer option until the specified date and time arrives. Select Enabled Until, and then select the month, day, year, and time at which Unity Connection will automatically disable the transfer option. **Note** By design, the standard transfer rule cannot be disabled.
Time Expire	Select Enabled Until, and then select the month, day, year, and time at which Unity Connection will automatically disable the transfer option.

Transfer Calls	Select one of the following settings:
	• Greeting-When this option is selected, the call is transferred as follows:
	  • For user settings-to the user greeting, without ringing the user phone.
	  • For call handler settings-to the call handler greeting.
	• Extension or URI-Enter an extension or URI to which the call is forwarded.

Field	Description
Transfer Type	Select how Unity Connection transfers calls. Use this setting with caution and only if you understand its implications on the phone and voice messaging systems. • Release to Switch—Unity Connection puts the caller on hold, dials the extension, and releases the call to the phone system. When the line is busy or is not answered, the phone system—not Unity Connection—forwards the call to the user or handler greeting. This transfer type allows Unity Connection to process incoming calls more quickly. Use Release to Switch only when call forwarding is enabled on the phone system. • Supervise Transfer—Unity Connection acts as a receptionist, handling the transfer. If the line is busy or the call is not answered, Unity Connection—not the phone system—forwards the call to the user or handler greeting. You can use supervised transfer whether or not the phone system forwards calls. The Transfer Type option is unavailable when Transfer Incoming Calls is set to the My Personal Greeting option. Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly.

Translation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 123: Translation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Translation Pattern	Translation pattern, including numbers and wildcards.
Partition	Available route partitions.
Description	Optional description.
Numbering Plan	Numbering plan.
Route Filter	Optional route filter.

Field	Description
MLPP Precedence	Multilevel Precedence and Preemption (MLPP) precedence settings.
Resource Priority Namespace Network Domain	Configured Resource-Priority Namespace Network Domain.
Route Class	Route class setting for the translation pattern.
Use Originator's Calling Search Space	To use the originator's calling search space for routing a call.
External Call Control Profile	External call profile that you want to assign to the translation pattern.
Call Search Space	Available calling search spaces.
Block Enabled	Enables or disables block.
Provide Outside Dial Tone	For each translation pattern that you consider to be off network.
Urgent Priority	Interrupts interdigit timing when the system must route a call immediately.
Do Not Wait For Interdigit Timeout On Subsequent Hops	When the Urgent Priority check box is checked and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), the system does not start the interdigit timer after it matches any of the subsequent patterns.
Route Next Hop By Calling Party Number	Enables routing based on the calling party number, which is required for call screening based on caller ID information to work between clusters.
Release Cause	Dependent on the Block Enabled field. If a release cause is selected, then Block Enabled must be set to True.
Is an Emergency Service Number	Check this check box, if you are configuring an emergency service number. **Note** This setting is applicable only if the Emergency Location Service is enabled in the call manager.
Calling Party Transformations	
Use Calling Party’s External Phone Number Mask	Determines whether to use the calling party’s external phone number mask.
Calling Party Transform Mask	Transformation mask value.

Field	Description
Prefix Digits (Outgoing Calls)	Prefix digits.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern.
Calling Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's name on the called party's phone display for this translation pattern.
Calling Party Number Type	The format for the number type in calling party directory numbers.
Calling Party Numbering Plan	The format for the numbering plan in calling party directory numbers.
Connected Party Transformations	
Connected Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this translation pattern.
Connected Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's name on the calling party's phone display for this translation pattern.
Called Party Transformations	
Discard Digits	The discard digits instructions that you want to be associated with this translation pattern.
Called Party Transform Mask	Transformation mask value.
Prefix Digits (Outgoing Calls)	Prefix digits.
Called Party Number Type	The format for the number type in called party directory numbers.
Called Party Numbering Plan	The format for the numbering plan in called party directory numbers.

Translation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and earlier

Table 124: Translation Pattern Infrastructure Configuration Product Fields

Field	Description
Translation Pattern	Translation pattern, including numbers and wildcards.
Route Partition	Available route partitions.
Description	Optional description.
Dial Plan	Numbering plan.
Route Filter	Optional route filter.
MLPP Precedence	Multilevel Precedence and Preemption (MLPP) precedence settings.
Call Search Space	Available calling search spaces.
Block Enabled	Enables or disables block.
Release Cause	Dependent on the Block Enabled field. If a release cause is selected, then Block Enabled must be set to True.
Is an Emergency Service Number	Check this check box, if you are configuring an emergency service number. **Note** This setting is applicable only if the Emergency Location Service is enabled in the call manager.
Use Calling Party's External Phone Number Mask	Determines whether or not to use the calling party's external phone number mask.
Calling Party Transform Mask	Transformation mask value.
Calling Party Prefix Digits (Outgoing Calls)	Prefix digits.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern.
Calling Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's name on the called party's phone display for this translation pattern.

Field	Description
Connected Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this translation pattern.
Connected Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's name on the calling party's phone display for this translation pattern.
Called Party Discard Digits	The discard digits instructions that you want to be associated with this translation pattern.
Called Party Transform Mask	Transformation mask value.

Unified Call Manager Group Infrastructure Configuration Product Fields

Table 125: Unified Call Manager Group Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Unified CMs	List of available Cisco Unified Communications Managers.
Auto-Registration Unified CM Group	Select Yes if you want this Cisco Unified Communications Manager group to be the default Cisco Unified Communications Manager group when auto-registration is enabled.

UC Service Infrastructure Configuration Product Fields

Table 126: UC Service Infrastructure Configuration Product Fields

Field	Description
Voicemail	
Product Type	Select a product type. Available options are Unity and Unity Connection. Default setting: Unity.
Name	Enter the name of the voicemail service. Ideally, the voicemail service name should be descriptive enough for you to instantly recognize it.

Field	Description
Description	(Optional) Enter a description that helps you to distinguish between voicemail services. You can change the description if required. Maximum characters: 100.
Hostname/IP Address	Enter the address of the voicemail service in one of the following forms: • Hostname • IP address • Fully qualified domain name (FQDN) This field value must exactly match the hostname, IP address, or FQDN of the associated voicemail service. If the hostname or IP address of the voicemail service changes, change this field value accordingly.
Port	Enter the port to connect with the voicemail service. Default port: 443 This field value must match the available port on the voicemail service. Change the port number only if it conflicts with other services.
Protocol	Select the protocol to route voicemail messages securely. Available options: HTTP, HTTPS We recommend that you use HTTPS as the voicemail transport protocol for Cisco Unity Connection servers. Only change to HTTP if your network configuration does not support HTTPS.
Conferencing	
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required.

Field	Description
Hostname/IP Address	Enter the address of the conferencing service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the conferencing service so that users can contact the service when they sign in to web conferences. Default Port: 80 Allowed Values: 1- 65535 **Note** Use port 80 for HTTP and port 443 for HTTPS communications. **Note** This value must match the available port on the conferencing service. Change the port number only if it conflicts with other services.

Field	Description
Protocol	Select the protocol to route web conference communications. Available Options: HTTP, HTTPS Default Setting: HTTP. Change this setting to suit your network configuration, IM and Presence settings and security needs as follows: HTTP— Selects Hypertext Transfer Protocol as the standard method for transferring data between the server, Cisco Jabber, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express server does not have SSL enabled. HTTPS— Selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server, Cisco Jabber, and the browser. Select this option if the Unified MeetingPlace or the Unified MeetingPlace Express server has SSL enabled.
Mailstore	
UC Service Type	Specifies the UC service type as Mailstore.
Product Type	Specifies the product type as Exchange.
Name	Enter the name of the mailstore service. Ideally the mailstore service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between mailstore services. You can change the description if required.

Field	Description
Hostname/IP Address	Enter the address of the mailstore service in one of the following forms: • Hostname • IP address • FQDN This field value must exactly match the hostname, IP address, or FQDN of the associated mailstore service. If the address of the mailstore service changes, change this field value accordingly. Cisco Unity creates subscriber mailboxes for message storage on the Microsoft Exchange server. **Note** Cisco Unity Connection usually provides a mailstore service, and hosts themailstore service on the same server.
Port	Specify the port number configured for the service. Default Port: 143 Allowed Values: 1 - 65535 **Note** For secure voice messaging with Cisco Unity Connection, use port 7993. **Note** This value must match the available port on the mailstore service. Change the port number only if it conflicts with other services.
Protocol	Select the corresponding protocol to use when Cisco Jabber clients contact this service. Available Options: TCP, SSL, TLS, UDP Default Setting: TCP, which is the most commonly used networkconfiguration. Change this setting to suit your deployment, Unified CM settings, and security needs. **Note** For secure voice messaging with Cisco Unity Connection, use TLS.
Directory	
Service Type	Specifies directory as the UC service type.

Field	Description
Product Type	Select a supported directory product type from this list that applies to your network configuration. Available Options: Directory, Enhanced Directory Default Setting: Directory
Name	Enter the name of the directory service. Ideally the directory service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only). Allowed values: All characters allowed except quotes (''), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required. Allowed values: All characters allowed except quotes (''), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Hostname/IP Address	Enter the address of the directory service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the directory service. Default Port: 389 Allowed Values: 1- 65535 This value must match the available port on the directory service. **Note** Change the port number only if it conflicts with other services.

Field	Description
Protocol	Select the protocol to route communications between the directory service and Cisco Jabber clients. Available Options: TCP, UDP, TLS Default Setting: TCP. This is the most commonly used network configuration. Change this setting to suit your network configuration, Unified CM settings, and security needs.
Connection Type	Specifies the directory server type to connect to Global Catalog server that is optimized for searching or a Domain Controller (or any server running an Ldap service) which may not be optimized for searching. This is a required field. Default: Global Catalog server
Use Secure Connection	Define whether to send credentials in clear text (default is not to send in clear text i.e. use a secure connection). This is a required field. Default: True
Use Wildcards	Use wildcards when doing number lookups. This is a required field. Default: False
Disable Secondary Number Lookups	Disables queries using home, mobile and other numbers. This is a required field. Default: False
Uri Prefix	Specify the Uri scheme name e.g. 'im:' or 'sip:' Maximum length: 32
Phone Number Masks	Allows a mask to be defined which can be used when doing resolution by telephone number. E.g. the mask +353|+(###) ## ## #### could be used to resolve numbers in the format +35311221234 to +(353) 11 22 1234. Multiple masks can be defined by using the '|' operator. For example: +353|+(###) ## ## ####|+44|+44 (##)## #####) ## ## #### could be used to resolve numbers in the format +35311221234 to +(353) 11 22 1234. Maximum length: 1024
IM and Presence	

Field	Description
Service Type	Specifies IM and Presence as the UC service type.
Product Type	Select a supported IM and Presence product type from this list that applies to your network configuration. Available options: Unified CM (IM and Presence), WebEx (IM and Presence) Default setting: Unified CM (IM and Presence)
Name	Enter the name of the IM and Presence service. Ideally the IM and Presence service name should be descriptive enough for you to recognize it instantly. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between IM and Presence services. You can change the description if required.
Hostname/IP Address	Enter the address of the IM and Presence service in one of the following forms: • Hostname • IP address • DNS SRV Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore(_). **Note** This field value must exactly match the host name, IP address, or DNS SRV of the associated IM and Presence service. If the address of the IM and Presence service changes, change this field value accordingly. Cisco recommends DNS SRV to help the client find the correct IM and Presence service for the user
Conferencing	
UC Service Type	Specifies conferencing as the UC service type.
Product Type	Select a product type that applies to your network configuration. Available Options: MeetingPlace Classic, MeetingPlace Express, WebEx

Field	Description
Name	Enter the name of the coferencing service. Ideally the service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required.
Hostname/IP Address	Enter the address of the conferencing service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the conferencing service so that users can contact the service when they sign in to web conferences. Default Port: 80 Allowed Values: 1- 65535 **Note** Use port 80 for HTTP and port 443 for HTTPS communications. **Note** This value must match the available port on the conferencing service. Change the port number only if it conflicts with other services.

Field	Description
Protocol	Select the protocol to route web conference communications. Available Options: HTTP, HTTPS Default Setting: HTTP. Change this setting to suit your network configuration, IM and Presence settings and security needs as follows: HTTP— Selects Hypertext Transfer Protocol as the standard method for transferring data between the server, Cisco Jabber, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express server does not have SSL enabled. HTTPS— Selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server, Cisco Jabber, and the browser. Select this option if the Unified MeetingPlace or the Unified MeetingPlace Express server has SSL enabled.
CTI	
Service Type	Specifies CTI as the UC service type.
Product Type	Specifies CTI as the product type.
Name	Enter the name of the CTI service. Ideally the CTI service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between CTI services when you have more than one configured. You can change the description if required.

Field	Description
Hostname/IP Address	Enter the address of the CTI service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the, hostname, IP address, or FQDN of the associated CTI service. If the address of the CTI service changes, change this field value accordingly.
Port	Enter the port for the CTI service. Default port: 2748 Allowed ports: 1-65535 **Note** This value must match the available port on the CTI service. Change the port number only if it conflicts with other services.
Protocol	Specifies TCP as the default protocol.

Voice Region Infrastructure Configuration Product Fields

Table 127: Voice Region Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Audio Codec	Codec setting. For Cisco Unified Communications Manager higher versions (4.1 and above) , the Default Codec field is set to the option selected.

Voicemail Pilot Infrastructure Configuration Product Fields

Table 128: Voicemail Pilot Infrastructure Configuration Product Fields

Field	Description
Number	Voicemail pilot number.
Description	Optional description.

Field	Description
Calling Search Space	Available calling search spaces.
Is Default	Indicates whether this pilot number is the default Voice Mail Pilot for the system.

Voicemail Profile Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 129: Voicemail Profile Infrastructure Configuration Product Fields

Field	Description
Voice Mail Profile Name	Profile name.
Description	Optional description.
Voice mail Pilot	Available voicemail pilots.
Voice mail Box Mask	The mask that is used to format the voice mailbox number for autoregistered phones.
Is Default	Indicates whether this voicemail profile is the default for the system.

Voice Gateway Infrastructure Configuration Product Fields

Table 130: VG202, VG204, VG224, and VG350 Infrastructure Configuration Product Fields

Field	Description
Gateway Name	Name of the gateway.
Protocol	Protocol associated with the gateway.
MAC Address (Last 10 Characters)	MAC address of the selected device. Updating the MAC Address field will update all associated phones' MAC addresses. However, to update MAC addresses in the user records, you must perform a Domain synchronization.
Description	Description of the device.
Cisco Unified Communications Manager Group	The group of the Cisco Unified Communications Manager.
Module in Slot <Number>	Module that is in the slot number.
Subunit <Number>	Subunit's number.

Field	Description
Modem Passthrough	Enables or disables the modem passthrough.
Cisco Fax Relay	Enables and disables the Cisco fax relay.
T38 Fax Relay	Enables and disables the T-38 fax relay.
RTP Package Capability	Enables or disables RTP Package Capability.
MT Package Capability	Enables or disables MT Package Capability.
RES Package Capability	Enables or disables RES Package Capability.
PRE Package Capability	Enables or disables PRE Package Capability.
SST Package Capability	Enables or disables SST Package Capability.
RTP Unreachable OnOff	Enables or disables RTP unreachable timeout.
RTP Unreachable timeout (ms)	RTP unreachable timeout in milliseconds.
RTP Report Interval (secs)	RTP Report Interval in seconds.
Simple SDP	Enables or disables simple SDP.

VG450, VG310 and VG320 Infrastructure Configuration Product Fields

VG450, VG310 and VG320 infrastructure configuration product fields are almost similar to VG350. VG450, VG310 and VG320 infrastructure configuration products have the following additional fields that are not available in VG350:

Field	Description
Global ISDN Switch Type	Choose the ISDN switch type.
Switchback Timing	Choose the timing mechanism that is used to switch back to a primary Cisco Unified Communications Manager.
Switchback Uptime-Delay	Choose the delay, in minutes, that applies when delayed switchback is used. You must make an entry in this field if you chose “Delayed” in the Switchback Timing field.
Switchback Schedule	Specify the schedule, in hours and minutes, that applies when scheduled switchback is used. You must make an entry in this field if you chose “Scheduled” in the Switchback Timing field.
Type of DTMF Relay	Choose the type of DTMF (Dual-tone multifrequency) that you want to use.

For VG450, VG310 and VG320, Prime Collaboration Provisioning supports only FXS model cards for provisioning analog phones. Cisco Unified Communications Manager supports both FXS and BRI cards for VG310 and VG320. You cannot provision ISDN BRI phones using Prime Collaboration Provisioning.

For Cisco Prime Collaboration Release 12.6SU1 and later

VG450 supports MGCP protocol. You can select MGCP protocol in **Gateway Details** from the **Protocol** drop-down list. For MGCP, you need to provide the domain name instead of MAC address.

Application User Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.6 and later

Table 131: Application User Infrastructure Configuration Product Fields

Field	Description
Application User Information	
UserId	Enter a unique application user identification name.
Password	Enter alphanumeric or special characters for the application user password.
BLF Presence Group	Choose a Presence group for the application user.
Accept Presence Subscription	Configure this field with the Presence feature for presence authorization.
Accept Out-of-dialog REFER	Check this box to authorize the system Cisco Unified Communications Manager to accept Out-of-Dialog REFER requests that come from this SIP trunk application user.
Accept Unsolicited Notification	Check this box to authorize the system to accept unsolicited notifications that come from this SIP trunk application user.
Accept Replaces Header	Check this box to authorize Cisco Unified CM to accept header replacements in messages from this SIP trunk application user.
Device Information	
Associated Devices	Displays the list of devices that are associated with the application user. Click **Add**, to add a new controlled device. You can also edit and delete the associated devices. **Note** If a user has more than 50 associated devices, and Prime Collaboration Provisioning displays performance issues, restrict the number of associated devices to 50 per user by splitting the devices between multiple users.
CTI Controlled Device Profiles	This field lists the devices that are associated with the application user.

Field	Description
Associated Groups	Displays the groups to which the application user belongs. Click **Add**, to associate a group. You can also edit and delete the associated groups.

Port Group Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 132: Port Group Infrastructure Configuration Product Fields

Field	Description
Authentication Username	User name that Unity Connection uses to authenticate with the SIP server.
Call Process IP Address	IP Address for the Call Process.
Retry Interval After Successful Attempt	Wait time, in milliseconds, between MWI retries that occur after success is reported.
Delay between Requests	Minimum length of wait time, in milliseconds, between subsequent MWI requests.
Maximum Concurrent Requests	Maximum number of messaging waiting indicator (MWI) requests that are attempted at the same time so that a spike in MWI requests does not demand a large portion of Unity Connection resources.
Register with SIP Server	This is a checkbox. Check this check box so that Unity Connection registers with the SIP server.
SIP Transport Protocol	Lists the SIP transport protocols. Select the SIP transport protocol that Unity Connection uses .
Authenticate with SIP Server	This is a checkbox. Check this check box so that Unity Connection authenticates with the SIP server.
MWI On Extension	Extension specified in Cisco Unified CM Administration for turning MWIs on.
Enable Message Waiting Indicators	This is a checkbox that is checked by default. If checked, voice messaging ports in the port group are enabled to turn message waiting indicators (MWIs) on and off. If unchecked, turning message waiting indicators (MWIs) on and off is disabled for all voice messaging ports in the port group.
Display Name	Port Group Name.

Field	Description
SIP Contact Line Name	Voice messaging line name (or pilot number) that users use to contact Unity Connection and that further register with the SIP server.
Retries After Successful Attempt	Number of times an MWI request is retried after success is reported so that MWI success is assured.
Device Name Prefix	Prefix that Cisco Unified Communications Manager adds to the device name for voice ports. This prefix must match the prefix used by Cisco Unified CM.
Authentication Password	Password that Unity Connection uses to authenticate with the SIP server.
MWI Off Extension	Extension that you specified in Cisco Unified CM Administration for turning MWIs off.
Port Group Type	Type of the port group. Unity Connection creates the new port group based on the type that is selected from the list. The new port group has default settings as specified in the port group type.

Unified Communications Manager Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 133: Unified Communications Manager Server Infrastructure Configuration Product Fields

Field	Description
Password	The password used by the Expressway to access the Unified CM publisher. Range: 1 to 1024 characters.
Username	The username used by the Expressway to access the Unified CM publisher. The user must have the Standard AXL API Access role. Range: 1 to 1024 characters.
Unified CM publisher address	The FQDN or IP address of a Unified CM publisher. Range: 1 to 1024 characters.
CucmServer setting URL to Expressway Server	The Unified Communications Manager Server setting URL for the Expressway Server.

Field	Description
TLS verify mode	State of the TLS verify mode. If TLS verify mode is enabled, the Unified CM system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.

IMP Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 134: IMP Server Infrastructure Configuration Product Fields

Field	Description
IM and Presence Service database publisher node	The FQDN or IP address of the IM and Presence Service database publisher node.
Password	IP Address for the Call ProcessIP Address for the Call Process.
TLS verify mode	State of the TLS verify mode. If TLS verify mode is enabled, the IM and Presence Service node's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.
Username	The username used by the Expressway to access the IM and Presence publisher. The user must have the Standard AXL API Access role.
IMPServer setting URL to Expressway Server	The IMP Server setting URL for the Expressway Server.

DNS Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 135: DNS Infrastructure Configuration Product Fields

Field	Description
Domain name	The name to be appended to an unqualified host name before querying the DNS server. Used when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers. Can also be used along with the local System host name to identify references to this system in SIP messaging .
DNS requests port range	Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure.
DNS requests port range start	The lower source port in the range used for sending DNS queries. Requests choose a random port from this range. **Warning** Setting a small source port range increases your vulnerability to DNS spoofing attacks.
System host name	Defines the DNS hostname that this system is known by. The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit. **Note** This is not the fully-qualified domain name, just the host label portion.
DNS requests port range end	The upper source port in the range used for sending DNS queries. Requests choose a random port from this range. **Warning** Setting a small source port range increases your vulnerability to DNS spoofing attacks.
DNS setting URL to Expressway Server	The DNS setting URL for the Expressway Server.

DNS per Domain Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 136: DNS per Domain Server Infrastructure Configuration Product Fields

Field	Description
Address1	The Address 1 of the Domain Server.
Address2	The Address 2 of the Domain Server.
Address3	The Address 3 of the Domain Server.

Field	Description
Address4	The Address 4 of the Domain Server.
Address5	The Address 5 of the Domain Server.
DNSPerDomainServer setting URL to Expressway Server	The DNS per Domain Server setting URL for the Expressway Server.

DNS Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 137: DNS Server Infrastructure Configuration Product Fields

Field	Description
Address1	The Address 1 of the DNS Server.
Address2	The Address 2 of the DNS Server.
Address3	The Address 3 of the DNS Server.
Address4	The Address 4 of the DNS Server.
Address5	The Address 5 of the DNS Server.
DNSServer setting URL to Expressway Server	The DNS Server setting URL for the Expressway Server.

DNS Zone Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 138: DNS Zone Infrastructure Configuration Product Fields

Field	Description
Automatically respond to SIP searches	Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. • **Off:** a SIP OPTIONS message is sent to the zone. • **On:** Searches are responded to automatically, without being forwarded to the zone.

Field	Description
SIP UDP/IX filter mode	Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. • **On:** any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. • **Off:** INVITE requests are not modified.
SIP record route address type	Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway.
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including inter-worked calls) to and from this zone.
TLS verify inbound mapping	Switch Inbound TLS mapping On to map inbound TLS connections to this zone if the peer certificate contains the TLS verify subject name. If the received certificate does not contain the TLS verify subject name (as CN or SAN), then the connection is not mapped to this zone. Switch Inbound TLS mapping Off to prevent the Expressway from attempting to map inbound TLS connections to this zone.
Fallback transport protocol	Determines which transport type is used for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. RFC 3263 suggests that UDP should be used.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.
Modify DNS request	Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. This option is primarily intended for use with Cisco Spark Call Service. See www.cisco.com/go/hybrid-services.

Field	Description
Send empty INVITE for inter-worked calls	Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. • **On:** SIP INVITEs with no SDP are generated and sent to this neighbor. • **Off:** SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor.
Preloaded SIP routes support	Enable this zone to to process or reject SIP INVITE requests that contain Route header.
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified.
H323 Mode	Determines whether H.323 calls will be allowed to and from this zone.
Zone profile	Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.
SIP parameter preservation	Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. • **On:** preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. • **Off:** allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.
Name	Name of the zone.

Field	Description
SIP UDP/BFCP filter mode	Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. • **On:** any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled • **Off:** INVITE requests are not modified.
DnsZone setting URL to Expressway Server	The DNS Zone setting URL for the Expressway Server.
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or sub-zone. When there is a mismatch of settings i.e. • **On:** 'On' on one side and 'Off' on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. • **Off:**Off by default.
NewName	The new name of zone.
TLS verify subject name	The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).
Include address record	Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS records. • **On:** the Expressway will query for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones. • **Off:** the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

Field	Description
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
Domain to search for	Enter a FQDN to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected. • **On:** SIP requests sent out via this zone that are received again by this Expressway will be rejected. • **Off:** SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.

MRA Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 139: MRA Infrastructure Configuration Product Fields

Field	Description
SSODefaulted	Default SSO availablity.

Field	Description
Enabled	Enable or disable Mobile and Remote Access (MRA). MRA allows endpoints such as Cisco Jabber to have their registration, call control, messaging and provisioning services provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.
SSO	Controls SSO access.
IOSSafariPlugin	IOS Jabber client using safari plugin.
MRA setting URL to Expressway Server	The MRA setting URL for the Expressway Server.

Domain In Expressway Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 140: Domain In Expressway Infrastructure Configuration Product Fields

Field	Description
XMPP federation	Indicates that XMPP federated services will be provided for this local domain. **Note** If static routes for federated foreign domains are required, these are configured on Expressway-E.
IM and Presence Service	Instant messaging and presence services for this SIP domain are provided by Cisco Unified Communications Manager IM and Presence Service.
Domain setting URL to Expressway Server	The Domain setting URL to Expressway Server.
SIP registrations and provisioning on Unified CM	Endpoint registration, call control and provisioning for this SIP domain is serviced by Cisco Unified Communications Manager. The Expressway acts as a Cisco Unified Communications Manager gateway to provide secure firewall traversal and line-side support for Cisco Unified Communications Manager registrations.

Field	Description
Domain name	The name of the domain managed by this Expressway. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot).A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters
NewDomain name	The name of the new domain. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters

NTP Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 141: NTP Server Infrastructure Configuration Product Fields

Field	Description
Address1	The Address 1 of the NTP Server.
Address2	The Address 2 of the NTP Server.
Address3	The Address 3 of the NTP Server.
Address4	The Address 4 of the NTP Server.
Address5	The Address 5 of the NTP Server.
NTPServer setting URL to Expressway Server	The NTP Server setting URL for the Expressway Server.

Neighbor Zone Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 142: Neighbor Zone Infrastructure Configuration Product Fields

Field	Description
Peer address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or host names are therefore not recommended. If the traversal server is a cluster of Expressway-Es, this is the FQDN of one of the peers in that cluster.
NewName	The new name of zone.
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted.
Send empty INVITE for interworked calls	Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. • **On:** SIP INVITEs with no SDP are generated and sent to this neighbor. • **Off:** SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor.

Field	Description
SIP authentication trust mode	Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Expressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials.
H.323 call signaling port	Specifies the port on the neighbor to be used for H.323 calls to and from this Expressway.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Zone profile	Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.
Automatically respond to SIP searches	Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. • **Off:** a SIP OPTIONS message is sent to the zone. • **On:** searches are responded to automatically, without being forwarded to the zone.
SIP poison mode	Determines whether SIP requests sent out to this zone will be poisoned such that if they are received by the local Expressway again they will be rejected.
Interworking SIP search strategy	Determines how the Expressway searches for SIP endpoints when interworking an H.323 call. • **Options:** the Expressway sends an OPTIONS request. • **Info:** the Expressway sends an INFO request.

Field	Description
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
Call signaling routed mode	Specifies how the Expressway handles the signaling for calls to and from this neighbor. Auto: signaling is taken as determined by the Call routed mode configuration. Always: signaling is always taken for calls to or from this neighbor, regardless of the Call routed mode configuration.
Transport	The transport protocol to use for SIP calls to and from the traversal client.
SIP Proxy-Require header strip list	A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified.
SIP encryption mode	Determines whether or not the Expressway allows encrypted SIP calls on this zone. • **Auto:** SIP calls are encrypted if a secure SIP transport (TLS) is used. • **Microsoft:** SIP calls are encrypted using MS-SRTP. • **Off:** SIP calls are never encrypted.
SIP UPDATE strip mode	Determines whether or not the Expressway strips the UPDATE method from the Allow header of all requests and responses received from, and sent to, this zone.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.

Field	Description
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
Automatically respond to H.323 searches	Determines what happens when the Expressway receives an H.323 search, destined for this zone. • **Off:** an LRQ message is sent to the zone. • **On:** searches are responded to automatically, without being forwarded to the zone.
Preloaded SIP routes support	Enable this zone to to process or reject SIP INVITE requests that contain Route header.
H323 Mode	Determines whether H.323 calls will be allowed to and from this zone.
Name	Name of the zone.
Neighborzone setting URL to Expressway Server	The Neighbor zone setting URL for the Expressway Server.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.
SIP multipart MIME strip mode	Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007.
SIP record route address type	Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway.
SIP REFER mode	Determines how SIP REFER requests are handled. Forward: SIP REFER requests are forwarded to the target. Terminate: SIP REFER requests are terminated by the Expressway.
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone. • **On:** allow Multistream. • **Off:** disallow Multistream.

Field	Description
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings. For example, On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off
SIP parameter preservation	Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone.
SIP UDP/IX filter mode	Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. • **On:** any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. • **Off:** INVITE requests are not modified.
Monitor peer status	Specifies whether the Expressway monitors the status of the zones peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive.
SIP UDP/BFCP filter mode	Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. • **On:** any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. • **Off:** INVITE requests are not modified.

Search Rule Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 143: Search Rule Infrastructure Configuration Product Fields

Field	Description
Source	The sources of the requests for which this rule applies. Any: locally registered devices, neighbor or traversal zones, and any non-registered devices. • **AllZones:** locally registered devices plus neighbor or traversal zones. • **LocalZone:** locally registered devices only. Named: a specific zone or subzone.
SearchRule setting URL to Expressway Server	Search Rule setting URL for the Expressway Server.
State	Indicates if the search rule is enabled or disabled. Disabled search rules are ignored.
Replace string	The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only.)
Pattern type	How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) • **Exact:** The entire string must exactly match the alias character for character. • **Prefix:** the string must appear at the beginning of the alias. • **Suffix:** the string must appear at the end of the alias. • **Regex:** the string is treated as a regular expression.
Protocol	The source protocol for which this rule applies.
On successful match	Specifies the ongoing search behavior if the alias matches all of the search rule's conditions. Continue: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. Stop: any remaining search rules with a lower priority are not applied, even if the endpoint identified by the alias is ultimately not found.
Description	A free-form description of the search rule.

Field	Description
Priority	The order in the search process that this rule is applied, when compared to the priority of the other search rules. All priority 1 search rules are applied first, followed by all priority 2 search rules, and so on.
NewRule name	The name of the SearchRule.
Pattern string	The pattern against which the alias is compared. (Applies to Alias pattern match mode only.) Note: if the pattern string is a Regex, you can refer to the regular expressions reference table in the online help.
Target	The zone name or policy service name to query if the alias matches the search rule.
Request must be authenticated	Specifies whether this search rule applies only to authenticated search requests.
SIP variant	Select which type of SIP messages this search rule will process. Choose MicrosoftAny if you want the search rule to route MicrosoftSIP and MicrosoftIMP. Choose Standard to ignore Microsoft types and route standards-compliant SIP, or choose Any to route all types.
Mode	The type of alias for which this search rule applies. • **AliasPatternMatch:** the alias must match the specified pattern type and string. • **AnyAlias:** any alias (providing it is not an IP address) is allowed. • **AnyIPAddress:** the alias must be an IP address.
Source Name	The specific source zone or subzone for which this rule applies. Choose from the Default Zone, Default Subzone or any other configured zone or subzone.
Pattern behavior	Determines whether the matched part of the alias is modified before being sent to the target zone or policy service. (Applies to Alias Pattern Match mode only.) • **Leave:** the alias is not modified. • **Strip:** the matching prefix or suffix is removed from the alias. • **Replace:** the matching part of the alias is substituted with the text in the replace string.
Rule name	The name of the SearchRule.

Time Zone Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 144: Time Zone Infrastructure Configuration Product Fields

Field	Description
TimeZone setting URL to Expressway Server	The Time Zone setting URL for the Expressway Server.
Time Zone	The Time Zone.

Transform Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 145: Transform Infrastructure Configuration Product Fields

Field	Description
Pattern string	The pattern against which the alias is compared.
Priority	Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform.
Description	A free-form description of the transform.
NewPriority	Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform.
State	Indicates if the transform is enabled or disabled. Disabled transforms are ignored.
Pattern behavior	How the alias is modified. Strip: removes the matching prefix or suffix from the alias. Replace: substitutes the matching part of the alias with the text in the replace string. • AddPrefix: Prepends the Additional text to the alias. • AddSuffix: Appends the Additional text to the alias.
Transform setting URL to Expressway Server	The Transform setting URL for the Expressway Server.

Field	Description
Pattern type	How the pattern string must match the alias for the transform to be applied. • **Exact:** the entire string must exactly match the alias character for character. • **Prefix:** the string must appear at the beginning of the alias. • **Suffix:** the string must appear at the end of the alias. • **Regex:** the string is treated as a regular expression.
Replace string	The text string to use in conjunction with the selected Pattern behavior.

Traversal Client Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 146: Traversal Client Infrastructure Configuration Product Fields

Field	Description
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings. That is, 'On' on one side and 'Off' on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone. • **On:** allow Multistream. • **Off:** disallow Multistream.

Field	Description
Peer address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Expressway-Es, this is the FQDN of one of the peers in that cluster.
Password	The Password used by the Expressway when connecting to the traversal server.
SIP parameter preservation	Determines whether the Expressways B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. • **On:** Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. • **Off:** Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.
NewName	The new name of zone.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected. • **On:** SIP requests sent out through this zone that are received again by this Expressway will be rejected. • **Off:** SIP requests sent out through this zone that are received by this Expressway again will be processed as normal.

Field	Description
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
TraversalClient setting URL to Expressway Server	The Traversal Client setting URL for the Expressway Server.
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
Username	The user name used by the Expressway when connecting to the traversal server.
H323 Protocol	Determines which of the two firewall traversal protocols will be used for H323 calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. will be used for H323 calls to and from the traversal client.
Retry interval	Specifies the interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. establish a connection to the traversal server should be retried.
Name	Name of the zone.
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified.
Transport	The transport protocol to use for SIP calls to and from the traversal client.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.

Field	Description
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. • **Best effort:** Use encryption if available, otherwise fall back to unencrypted media. • **ForceEncrypted (Force encrypted):** all media must be encrypted. • **ForceunEncrypted (Force unencrypted):** ForceunEncrypted (Force unencrypted): all media must be unencrypted
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.

Traversal Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 147: Traversal Server Infrastructure Configuration Product Fields

Field	Description
H.460.19 demultiplexing mode	Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client
TLS verify subject name	The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).
Name	Name of the zone.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected.

Field	Description
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone.
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off.
Transport	The transport protocol to use for SIP calls to and from the traversal client.
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
NewName	The new name of zone.
SIP parameter preservation	Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed through this zone.
H323 Protocol	Determines which of the two firewall traversal protocols will be used for H323 calls to and from the traversal client.
UDP retry count	Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway.
UDP keep alive interval	Set the frequency until which the UDP probe is sent to the Expressway.

Field	Description
UDP retry interval	Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway.
TLS verify mode	Controls X.509 certificate checking and mutual authenticationbetween this Expressway and the traversal client. If enabled, aTLS verify subject name must be specified.
Username	The user name used by the Expressway when connecting to the traversal server.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.
TCP Retry interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
TraversalServer setting URL to Expressway Server	The Traversal Server setting URL for the Expressway Server.
TCP retry count	Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway.
TCP keep alive interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
H323 Mode	Determines whether H.323 calls will be allowed to and from this zone.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.

XMPP Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 148: XMPP Infrastructure Configuration Product Fields

Field	Description
Privacy mode	Controls whether restrictions are applied to the set of federated domains.
Use static routes	Indicates whether a controlled list of static routes, rather than DNS lookup, are used to locate federation XMPP addresses.
XMPP federation support	Enable or disable support for XMPP federation.
Require client-side security certificates	Controls whether the certificate presented by the client is verified against Expressway's current trusted CA list and the revocation list if loaded.
Dialback secret	The dialback secret used for identity verification with federated XMPP servers.
XMPP setting URL to Expressway Server	The XMPP setting URL for the Expressway Server.
Security mode	Indicates if a TLS connection to servers is required, preferred, or not required.

Unified Communications Traversal Core Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 149: Unified Communications Traversal Core Infrastructure Configuration Product Fields

Field	Description
Username	The user name used by the Expressway when connecting to the traversal server.
Password	The Password used by the Expressway when connecting to the traversal server.
SIP parameter preservation	Determines whether the Expressways B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. • **On:** Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. • **Off:** Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.

Field	Description
UnifiedCommunications Traversal Core setting URL to Expressway Server	The Unified Communications Traversal Core setting URL for the Expressway Server.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone. • **On:** Allow Multistream. • **Off:** Disallow Multistream.
Peer Address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Expressway-Es, this is the FQDN of one of the peers in that cluster.
Name	Name of the zone.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.
NewName	The new name of zone.
Retry interval	Specifies the interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. establish a connection to the traversal server should be retried.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.

Field	Description
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected. • On: SIP requests sent out through this zone that are received again by this Expressway will be rejected. • Off: SIP requests sent out through this zone that are received by this Expressway again will be processed as normal.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.

Unified Communications Traversal Edge Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 150: Unified Communications Traversal Edge Infrastructure Configuration Product Fields

Field	Description
TCP retry interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Username	The user name used by the Expressway when connecting to the traversal server.

Field	Description
TCP keep alive interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
TLS verify subject name	The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone.
UDP retry count	Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected.
UnifiedCommunications Traversal Edge setting URL to Expressway Server	The Unified Communications Traversal Edge setting URL for the Expressway Server.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected.
UDP retry interval	Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway.
UDP keep alive interval	Set the frequency until which the UDP probe is sent to the Expressway.

Field	Description
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
Name	Name of the zone.
NewName	The new name of zone.
SIP parameter preservation	Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed through this zone.
TCP retry count	Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway.

Restart Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 151: Restart Infrastructure Configuration Product Fields

Field	Description
Restarting the Expressway Server	Restarting the Expressway Server.
Message	Message on restarting the Server.

Credential Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 152: Credential Infrastructure Configuration Product Fields

Field	Description
Credential setting URL to Expressway Server	The Credential setting URL for the Expressway Server.
NewName	Change the existing credential name to another name.
Password	The password required for this entry in the local authentication database.The maximum plaintext length is 128 characters, which will then be encrypted.
Name	The name required for entry in the local authentication database.

APPENDIX C

Provisioning Default Values for Maximum Calls and Busy Trigger Attributes

Provisioning Default Values for Maximum Calls and Busy Trigger Attributes

Maximum Calls and Busy Trigger are Line provisioning attributes that Cisco Prime Collaboration Provisioning sets with default values based on the endpoint type. The following table lists the default values that Cisco Prime Collaboration Provisioning sets for each endpoint type.

Table 153: Default Settings for Maximum Calls and Busy Trigger Provisioning Attributes

Product	Maximum Calls	Busy Trigger
Analog Phones	1	1
Cisco Jabber for BlackBerry	2	2
CTI Port	4	2
Cisco 3905	2	2
Cisco 6901	2	2
Cisco 6911	2	2
Cisco 6921	2	1
Cisco 6941	2	1
Cisco 6945	2	1
Cisco 6961	2	1
Cisco 7902	2	2
Cisco 7905	4	2

Provisioning Default Values for Maximum Calls and Busy Trigger Attributes

Product	Maximum Calls	Busy Trigger
Cisco 7905 (SIP)	2	2
Cisco 7906	4	2
Cisco 7906 (SIP)	4	2
Cisco 7910	2	2
Cisco 7911	4	2
Cisco 7911 (SIP)	4	2
Cisco 7912	4	2
Cisco 7912 (SIP)	2	2
Cisco 7920	2	2
Cisco 7921	4	2
Cisco 7925	4	2
Cisco 7926 G	4	2
Cisco 7931	1	1
Cisco 7935	2	1
Cisco 7936	2	1
Cisco 7937	6	2
Cisco 7940	4	2
Cisco 7940 (SIP)	2	2
Cisco 7941	4	2
Cisco 7941 (SIP)	4	2
Cisco 7941G-GE	4	2
Cisco 7941G-GE (SIP)	4	2
Cisco 7942	4	2
Cisco 7942 (SIP)	4	2
Cisco 7945	4	2
Cisco 7945 (SIP)	4	2
Cisco 7960	4	2
Cisco 7960 (SIP)	2	2

Product	Maximum Calls	Busy Trigger
Cisco 7961	4	2
Cisco 7961 (SIP)	4	2
Cisco 7961G-GE	4	2
Cisco 7961G-GE (SIP)	4	2
Cisco 7962	4	2
Cisco 7962 (SIP)	4	2
Cisco 7965	4	2
Cisco 7965 (SIP)	4	2
Cisco 7970	4	2
Cisco 7970 (SIP)	4	2
Cisco 7971	4	2
Cisco 7971 (SIP)	4	2
Cisco 7975	4	2
Cisco 7975 (SIP)	4	2
Cisco 7985	4	2
Cisco 8941	3	2
Cisco 8945	3	2
Cisco 8961(SIP)	4	2
Cisco 9951(SIP)	4	2
Cisco 9971 (SIP)	4	2
Cisco IP Communicator	4	2
Cisco IP Communicator (SIP)	4	2
Cisco Unified Personal Communicator	6	2
Cisco ATA-186	2	2
Cisco ATA-187	2	2
Cisco Cius	4	2
Cisco DX70	4	2

Provisioning Default Values for Maximum Calls and Busy Trigger Attributes

Product	Maximum Calls	Busy Trigger
Cisco DX80	4	2
Cisco E20	5	2
Cisco EX60	4	4
Cisco EX90	4	4
Cisco Jabber for Android	3	2
Cisco Jabber for Desktop	6	2
Cisco Jabber for iPhone	3	2
Cisco Jabber for Tablet	3	2
Cisco TelePresence MX700	4	4
Cisco TelePresence MX800	4	4
Nokia S60[1]	3	2
Remote Destination Profile	2	2
Third-party SIP device (advanced)	2	2
Third-party SIP device (basic)	2	2

[1] After upgrade new phones like Nokia and iPhone cannot be ordered by default. You must associate these new phone types to the appropriate user types.

APPENDIX D

Prebuilt IOS Templates

Prebuilt IOS Templates

For Cisco Prime Collaboration Release 11.6 and later

From Cisco Prime Collaboration Release 11.6, Pre-Built IOS templates enables you to:

- Create batch actions for the existing Pre-Built IOS templates.
- Migrate existing configuration templates to batch projects.
- Migrate the existing keyword list from Configuration Templates to the keyword management user interface.
- Support 32,000 character for configurations, replacing the existing 1000K character support so as to allow large iOS configurations in batch actions of infrastructure configuration objects.

On migration, existing Configuration Templates are created as batch projects in Batch Provisioning. The configurations in each template is created as respective batch actions. While migrating, the inputs for Domain, Service Area and Processor are replaced as keywords in the migrated batch actions as ${DOMAIN}, ${SERVICEAREA} and ${PROCESSOR}, respectively. While migrating the IOS Generic router, the '@' symbol in the command field representing the keywords, for example '@PARAM', is replaced with '${PARAM}' to maintain uniformity throughout the application.

Post migration, privilege for Batch Provisioning is given for the users who had access to Configuration Templates privilege before migration. For access control groups which had access to both Configuration Templates and Batch Provisioning before migration, privilege for Configuration Template is removed.

In Batch Provisioning user interface, the user has to choose the list of keywords in the batch project to apply keywords to the migrated batch actions.

The following Pre-Built IOS templates from Configuration Templates contains the sample batch action files in Batch Provisioning:

- Analog Voice Gateway Configurations
    - IOSConfigureSetAvgSccpCcm.txt
- Sample

- IOSConfigureCUBESipTrunk.txt
- IOSConfigureTelephonyServiceMessage.txt

In addition to Pre-Built IOS templates, the following IOS templates from Configuration Templates contains the sample batch action files in Batch Provisioning:

- Unified CME
  - Unified CME IOS Template
- Unity Express
  - CUE IOS Template

Creating sample batch action files of Pre-built IOS templates

For Cisco Prime Collaboration Release 11.6 and later

1. Go to the Batch Provisioning (**Advanced Provisioning > Batch Provisioning**) page.
2. Create a new batch project and upload a sample batch action file, IOSConfigureSetAvgSccpCcm.txt from the list of batch action files with the required configurations.
3. Select the keywords list from the keyword drop-down where values for Domain, Service Area and Processor name are chosen for the batch action. (The Generic IOS Router device for the above template selection should be created already in **Device Setup** page).
4. Give the configurations for the keywords in the Configuration command which is denoted by ${<<param name>>}.
5. Run the batch action.
6. The Router Device configuration(s) is provisioned through the newly created batch action template.

Copying Prebuilt Cisco IOS Templates to Cisco Prime Collaboration Provisioning

The generic Prebuilt Cisco IOS templates are available for download from cisco.com.

To copy files:

Procedure

Step 1 Access your Provisioning system and go to the subdirectory ${CUPM-INSTALLED}\sep\ipt\ios-pre-built.

Step 2 Copy the downloaded files into your Provisioning platform's subdirectory. There you will find a directory called Sample.

Step 3 Create a new directory and give a descriptive name for the type of generic Cisco IOS prebuilt templates.

Step 4 Copy the *Name*-swconfig.txt and Config-UserGuide-*Name*.txt for your prebuilt template into one of the subdirectories you have created under ios-pre-built.

Generate Console Account using Troubleshooting User

Follow these steps to generate a console account using troubleshooting user

1. In PCP micro service page under Console Account, we generate a console account user by providing username and password.
2. From console account, you can access CLI of PCP server.

Note

- In PCP 12.1, there is no access to CLI/SSH as root, so the user created through console account can access this privilege.
- If troubleshooting user is created using trouble shooting UI, and the Cisco Prime Collaboration Provisioning database is not up and running, then the user will be available only through the troubleshooting UI and not through the Cisco Prime Collaboration Provisioning UI.

APPENDIX E

Troubleshooting

Changing the SSL Port

To change the port used by Cisco Prime Collaboration Provisioning for SSL:

Procedure

Step 1 In the Cisco Prime Collaboration Provisioning system, open the ssl.conf file located at /opt/cupm/httpd/conf.

Step 2 Change the port number in the following lines:

```
Listen 443

VirtualHost_default_:443

ServerName www.example.com:443

RewriteRule ^/?(.*) https://%{SERVER_NAME}:443/$1 [R,L]
```

Note After you change the port number, you must enter the new port number when you access Cisco Prime Collaboration Provisioning.

Step 3 Save the changes and close the file.

Step 4 Open the httpd.conf file located at /opt/cupm/httpd/conf.

Step 5 Change the port number in the following line:

```
RewriteRule ^/?(.*) https://%{SERVER_NAME}:443/$1 [R,L]
```

Step 6 Save the changes and close the file.

Step 7 Restart the Apache server by using the following commands:

```
/opt/cupm/httpd/bin# ./apachectl -k stop
```

```
/opt/cupm/httpd/bin# ./apachectl -k start -DSSL
```

Configuring Cisco Prime Collaboration Provisioning Server Time Zone

You can provide Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT), updated with leap seconds.

To change the time zone in the Provisioning server:

Procedure

Step 1 Log into the Cisco Prime Collaboration Provisioning server with the Console User Login account.

Step 2 Enter the following command to check the configured timezone:

```
user $ timedatectl
```

Step 3 Enter the following command to see the list of supported time zones:

```
user $ timedatectl list-timezones
```

Step 4 Enter the following commands to set the time zone for the Cisco Prime Collaboration Provisioning server:

```
user $ timedatectl set-timezone Asia/Kolkata
```

Step 5 Navigate to **cd /opt/cupm/sep**.

Step 6 Update the following property in the dfc.properties file to update the offset:

```
dfc.gui.utc_offset=<applicable offset for your geographic location>
```

For example, if you are in IST time zone, you must enter: `dfc.gui.utc_offset=+0530`

Step 7 Restart the services

```
sudo /opt/cupm/bin/cpcmcontrol.sh stop
sudo /opt/cupm/bin/cpcmcontrol.sh start
```

Note You can also restart the services from Cisco Prime Collaboration Provisioning >Process Management Page.

Synchronizing Special Directory Numbers

Prior to the Cisco Prime Collaboration Provisioning 9.5 release, Cisco Prime Collaboration Provisioning only synchronizes those Directory Numbers (DN) whose endpoints are managed by Cisco Prime Collaboration Provisioning and will not have a complete knowledge of the DNs configured by Cisco Unified Communications Manager. There might be instances of few special DNs configured on Cisco Unified Communications Manager.

Special Directory Numbers:

- The DN features which are present in Cisco Unified Communications Manager but not managed by Cisco Prime Collaboration Provisioning. For example, Intercom DN.
- The DN attached to endpoints which are not managed by Cisco Prime Collaboration Provisioning.

Note Provisioning has a limited support of endpoints and does not support all the endpoints available in Cisco Unified Communications Manager.

From Cisco Prime Collaboration Provisioning 10.0 and above versions, you can synchronize all special DNs as part of user synchronization. This feature will be disabled by default. To enable this feature, you must add the following property to /opt/cupm/sep/ipt.properties file:

```
dfc.ipt.cisco.ccm.sync.orphanDN=true
```

By enabling this property, Cisco Prime Collaboration Provisioning synchronizes more DN's and takes additional time to complete the user synchronization process. Time taken depends on the number of special DN's configured in Cisco Unified CM.

Note After updating the ipt.properties file, you must restart the cupm services for the changes to take effect.

When this feature is enabled, the provisioning orders are validated from Provisioning, rather than submitting it to Cisco Unified Communications Manager which results in failure.

Provisioning and Special DN conditions:

Any provisioning activity carried out from Cisco Prime Collaboration Provisioning, which tries to re-use such special DNs, can result in provisioning failure.

- When the provisioning line is auto-assigned, line will not be provisioned if the DN is already used.
- When the provisioning line is chosen manually, Cisco Prime Collaboration Provisioning will throw an error during provisioning.

Restore the Single-Machine Provisioning Database

Before you begin

If you are restoring to a new installation, have the system with the new installation up and running before beginning this procedure. This procedure requires that you have administrator level access to the Provisioning database (the PostgreSQL database).

If you are restoring the database on a new system, you must verifying that the following ports are not being used by another application:

- dfc.jboss.port=46008
- dfc.postgres.port=5432

- dfc.nice.rmi.registry.internal.port=46001
- dfc.webport=80

If a port is being used by another application, you must change the port number to a vacant port. These settings are defined in the /opt/cupm/sep/dfc.properties file. If you accepted the default location during installation, the installation directory is /opt/cupm.

Procedure

Step 1 Login as troubleshooting user using SSH with port 22.

Step 2 Navigate to the **/opt/cupm** folder and enter the following command to stop the application services like Apache, JBoss and NICE:

```
sudo ./cupm-app-service.sh stop
```

Step 3 Ensure whether the application services are stopped by using the following command:

```
ps -aef | grep startcupm
ps -aef | grep nice
kill -9 <startcupm process-id>
kill -9 <nice process-id>
```

a) To check whether the nice process is still holding on the postgres connection, enter the following command:

```
ps -aef
```

b) Look for the process: /opt/cupm/jvm/bin/java -server -classpath /opt/cupm/sep/lib/dom.jar:/opt/cupm/sep/lib/jaxbapi.jar:/opt/cupm/sep/lib/jaxb-impl.jar

If the process is running then enter the following command:

```
kill -9 <Process-Id found earlier>
```

Step 4 If you are restoring to the same installation, then proceed to the next step, if you are restoring to a new installation, paste the backed-up file (bak) into /mnt folder

Step 5 Go to the directory using the command:

```
cd /opt/postgres/pghome/bin
```

Step 6 Run the following command to restore the database:

```
sudo ./CUPM-restore.sh <username> <password> <backup_file_name with Absolute Path>
```

where, username is the username of the PostgreSQL administrator. The default administrator username is pmadmin; the password is same as you entered for globaladmin.

If you are getting the following error:

```
"dropdb: database removal failed: ERROR:  database "cupm" is being accessed by other users"
```

Do the following:

a) Check whether the nice process is still holding on the postgres connection by using the following command:

```
ps -aef
```

b) Look for the process: /opt/cupm/jvm/bin/java -server -classpath /opt/cupm/sep/lib/dom.jar:/opt/cupm/sep/lib/jaxbapi.jar:/opt/cupm/sep/lib/jaxb-impl.jar

If the process is running then enter the following command:

```
kill -9 <Process-Id found earlier>
```

c) Run the restore command again (./CUPM-restore.sh <username> <password> /mnt/<backup_file_name>).

Step 7 If you are restoring to the same installation, proceed to next step. If you are restoring to a new installation, copy back the following backed-up files. To copy the file using ssh, copy the files at **/home/<sudo user directory>** , and then copy using **sudo cp <file_name> <Absoulte_Patch_file_name_to _ be_copied>**. For example: If sudo user id is 'testuser', and file to be copied is 'dfc.properties' file at /home/testuser/, Using ssh, copy dfc.properties file at /home/testuser/ and then, copy the file again to mentioned directory using the command sudo cp /home/testuser/dfc.properties /opt/cupm/sep/dfc.properties

- /opt/cupm/sep/dfc.properties
- /opt/cupm/sep/ipt.properties
- /opt/cupm/sep/dfc.keystore
- /opt/cupm/jboss/server/cupm/conf/login-config.xml
- /opt/cupm/jboss/server/cupm/deploy/dfc-ds.xml
- /opt/cupm/sep/custom.properties
- /opt/cupm/sep/passwordpolicy.properties

Note To restore the random key, refer Restore the Single-Machine Provisioning Database, on page 517.

Step 8 Start Apache, JBoss, and NICE Services using the following commands:

```
cd /opt/cupm
sudo ./cupm-app-service.sh start
```

Restoring Random Key

The backup compressed file created by Backup Management (**Administration > Backup Management**) includes a copy of random key file.

Procedure

Step 1 Copy the backed up directory to the server. Navigate to /opt/cupm/sep/ipt/.

Step 2 Create a directory .system (if it does not exist) using the mkdir command, else move to step 3.

Step 3 Navigate to /opt/cupm/sep/ipt/.system.

Step 4 Copy the following from backed up directory:

```
cp <BACK UP DIR>/pcprandom.key .pcprandom.key
cp .pcprandom.key .pcprandom.key.bkp
touch .pcprandomconfigured
```

Restore the Database from the Provisioning User Interface

For Cisco Prime Collaboration Provisioning 12.2 and later

The user can restore the database from the PCP user interface.

Procedure

Step 1 Choose **Administration**>**Backup Management**.

Step 2 In the Backup Management page, click **Restore**.

Step 3 In Database Restore page, select the required restore options:

- **Automatic**: If you select **Automatic**, and click **Find Backups**. It displays the list of the available backups, select the required backup, and click **Restore**. A warning is displayed stating, Database backups, Backup yyyy-mm-dd hh:mm:ss, will now be restored. Current system data will be lost. The application will not be accessible. Do you wish to continue? click **Yes** to continue.
- **SFTP** or **FTP**

  If you select SFTP or FTP, provide the following details:

  - IP address of the server where the backup files is saved.
  - Provide the port details.
  - Path to the backup location.
  - Username and password information.
  - Click**Find Backups** . It displays the list of the available backups, select the required backup, and click **Restore**. A warning is displayed stating, Database backups, Backup yyyy-mm-dd hh:mm:ss, will now be restored. Current system data will be lost. The application will not be accessible. Do you wish to continue? click **Yes** to continue.
- **Local Disk**

  If you select Local, provide the following details:

  - Path to the backup location.
  - Click**Find Backups** . It displays the list of the available backups, select the required backup, and click **Restore**. A warning is displayed stating, Database backups, Backup yyyy-mm-dd hh:mm:ss, will now be restored. Current system data will be lost. The application will not be accessible. Do you wish to continue? click **Yes** to continue.

  Once the restore process begins in Cisco Prime Collaboration Provisioning, it directs you to a static page, where the logs can be viewed, and after the completion of restore process, you are directed to the Cisco Prime Collaboration Provisioning login screen.

Note In troubleshooting UI, once the restore process begins, it directs you the restore progress screen, where the logs can be viewed and the Start another DB Restore button is available. Click **Start another DB Restore** to start another restore process.

Note This functionality is also available in Troubleshooting UI, which can be used when the PCP/JBOSS are down.

Note Currently, restore from Cisco Prime Collaboration Provisioning user interface is not supported in case of backed up database having a different password than the server on which it is being restored. For such cases, the user needs to restore the database from CLI.

Self-Care User Migration Script

The SelfCareMigrationUtility can be invoked during the migration, or from the CLI, after migration. The tool processes all the users in the domains that have CreateSelfCareAccounts rule and DefaultCUPMPassword rule set.

This tool can be run through CLI from /opt/cupm/sep/ipt/bin. It can be run either globally (means for all domains) or for a single domain.

To run script:

Procedure

Step 1 Go to /opt/cupm/sep/ipt/bin.

Step 2 Run: `./SelfCareMigrationUtility.sh ALL ENABLE`

- ALL—Indicates all domains.
- ENABLE—Enables selfcare for all users in the domain specified.

  Tto disable selfcare option, run:

  ```
  ./SelfCareMigraionUtility.sh ALL DISABLE
  ```

  The script can be run at the domain level also. To do this, run:

  ./SelfCareMigrationUtility.sh *DOMAIN NAME* [ENABLE | DISABLE]

For more information on migration, see the Cisco Prime Collaboration Upgrade and Migration Guide.

Retaining User Information During System Reboot

For Cisco Prime Collaboration Release 11.5 and later

This method of creating new user helps to retain the user information that is lost during system reboot.

Procedure

Step 1 Log in to CLI as root.

Step 2 Navigate to the /opt/cupm folder and enter the following command:

```
useradd <username>
passwd <username>
```

Step 3 Enter the password.

Step 4 To retain the user data, enter the following command:

```
cp /etc/shadow /storedconfig/startup-config-*/etc/shadow
```

Step 5 Enter **Yes** to continue.

Step 6 Enter the following command:

```
cp /etc/passwd /storedconfig/startup-config-*/etc/passwd
```

Step 7 Enter **Yes** to continue.