

Collaboration Management Services

Revised: February 19, 2019

This chapter describes the collaboration management services included in the Enterprise Collaboration Preferred Architecture. This chapter focuses on a subset of core applications that are necessary for most collaboration environments. This Preferred Architecture is built with all of the available applications in mind, to simplify the deployment of these applications and to avoid unnecessary configuration changes.

The first two sections of this chapter describe the tools for deployment of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM IM and Presence Service, and Cisco Unity Connection. Those tools are: Cisco Prime Collaboration Deployment and the web-based Cisco Smart Software Manager portal. The third section of this chapter explains the optional implementation of Cisco Prime Collaboration Provisioning used to configure Unified CM.

The collaboration management services include:

- Cisco Prime Collaboration Deployment
- Cisco Smart Software Manager
- Cisco Prime Collaboration Provisioning

Key Benefits of Collaboration Management Services

- Eases deployment of new infrastructure components.
- Provides a single, centralized web-based tool to manage licenses, software, and entitlement for various products.
- Simplifies and consolidates product deployment and management with automated provisioning, monitoring, and trend reporting.
- Boosts productivity and consistency with accelerated moves, adds, and changes under workflow policy control.

What's New in This Chapter

Table 6-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 6-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Smart licensing updates related to the validity period of registration token and Specific License Reservation as alternate licensing method	Cisco Smart Software Manager, page 6-6	January 23, 2019
Other minor corrections and updates	Various sections of this chapter	January 23, 2019
Cisco Smart Software Manager has replaced Cisco Prime License Manager	Cisco Smart Software Manager, page 6-6	August 30, 2017

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment provides a simplified solution for deploying collaboration application nodes, including Cisco Unified Communications Manager (Unified CM), Cisco Unified CM IM and Presence Service, and Cisco Unity Connection. Cisco Prime Collaboration Deployment assists the administrator by automating many of the steps necessary to install Unified CM, Unified CM IM and Presence Service, and Unity Connection clusters.

Core Components

The core components of the Cisco Prime Collaboration Deployment architecture are:

- Cisco Prime Collaboration Deployment for deploying collaboration application nodes on the VMware ESXi server using Cisco ISO installation files
- VMware ESXi server for hosting collaboration application node virtual machines (VMs), including Unified CM and Unity Connection

Benefits

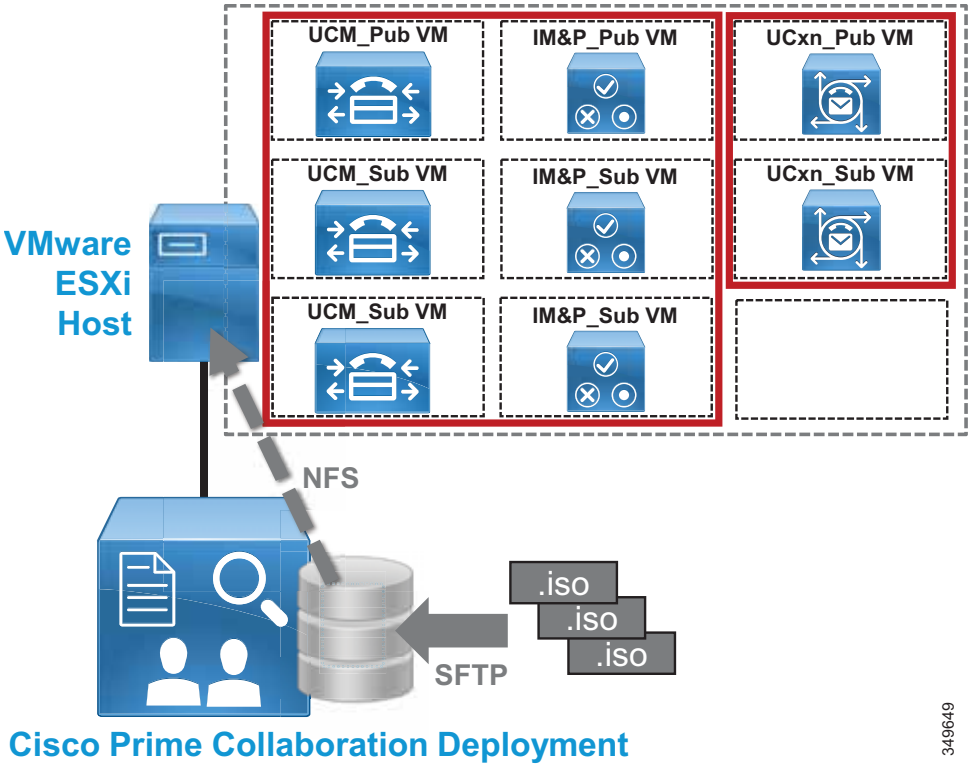
Using Cisco Prime Collaboration Deployment to deploy the Enterprise Collaboration Preferred Architecture call control and voice messaging application nodes provides the following benefits:

- Centralizes storage for collaboration application Cisco ISO files.
- Automates the installation of Unified CM, Unified CM IM and Presence Service, and Unity Connection collaboration applications.
- Applies an array of common settings across collaboration application server node VMs, including network components (NTP, DNS), administration accounts and passwords, and base certificate information.

Architecture

The Cisco Prime Collaboration Deployment architecture consists of the Cisco Prime Collaboration Deployment server node, where collaboration application Cisco ISO files are stored for installation. These files are placed on Cisco Prime Collaboration Deployment using secure FTP (SFTP). A network file system (NFS) mount is created to the ESXi host once the ESXi host is configured in Cisco Prime Collaboration Deployment. This NFS mount enables the appropriate collaboration application Cisco ISO files to be installed on the ESXi host server node VMs (Figure 6-1).

Figure 6-1 Cisco Prime Collaboration Deployment Architecture



Cisco Prime Collaboration Deployment may be deployed with multiple ESXi hosts as required for larger deployments that span multiple ESXi host servers.

Role of Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment serves as the collaboration application Cisco ISO store as well as the administrative interface for deploying and configuring collaboration application nodes on the VMware ESXi host or hosts.

Role of ESXi Host

The ESXi host server or servers contain the application node VMs for Unified CM, Unified CM IM and Presence Service, and Unity Connection clusters installed by Cisco Prime Collaboration Deployment.

High Availability for Cisco Prime Collaboration Deployment

The Cisco Prime Collaboration Deployment application does not support high availability; however, because Cisco Prime Collaboration Deployment is used for initial deployment and base configuration, redundancy is not a requirement. In order to deploy and perform base configuration for collaboration application nodes, the Cisco Prime Collaboration Deployment application node must be in service and able to reach the ESXi server host or hosts where collaboration application server nodes will be deployed. In cases where Cisco Prime Collaboration Deployment is not operational, it must be returned to service so that the network connectivity is available and the NFS mount to the ESXi server is up.

As with other collaboration and management applications, the Cisco Prime Collaboration Deployment application server should be backed up regularly using the Disaster Recovery System (DRS). DRS device configuration, backup scheduling, and backup and restore operations are managed through the Cisco Prime Collaboration Deployment application server command line interface (CLI).

Scaling Cisco Prime Collaboration Deployment

Given that there is only a single Cisco Prime Collaboration Deployment OVA template file for each release, capacity considerations for Cisco Prime Collaboration Deployment are limited to the amount of disc storage capacity of the Cisco Prime Collaboration Deployment VM. Because the Cisco ISO files for the various deployed collaboration applications are stored on Cisco Prime Collaboration Deployment, disc capacity is important. For this reason, management of Cisco ISO files is critical. Cisco ISO files that are no longer needed should be removed to make room for newer Cisco ISO files.

Cisco Prime Collaboration Deployment Process

There are two deployment aspects to consider with Cisco Prime Collaboration Deployment:

- Deploying the Cisco Prime Collaboration Deployment Application Server
- Deploying Cisco Collaboration Application Server Clusters with Cisco Prime Collaboration Deployment

Deploying the Cisco Prime Collaboration Deployment Application Server

The Cisco Prime Collaboration Deployment application is deployed as a single standalone node. Deploy the Cisco-provided Cisco Prime Collaboration Deployment OVA template file on your compute infrastructure.

Once the OVA has been deployed, mount the Cisco Prime Collaboration Deployment Cisco ISO file and power on the Cisco Prime Collaboration Deployment VM to install Cisco Prime Collaboration Deployment. After you enter the appropriate information, including account information (administrator account name and password), network information (IP address, hostname, DNS, NTP, and so forth), and web security information (self-signed certificate information including location, organization, and so forth), the installation will complete.

For information on how to obtain the OVA template and Cisco ISO files, refer to the documentation at

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-prime-collaboration-deployment.html

Once the OVA template is deployed and the Cisco Prime Collaboration Deployment Cisco ISO file is installed, you manage Cisco Prime Collaboration Deployment and deploy collaboration application server nodes and clusters using the web-based graphical user interface (GUI). Upgrades and backups of the Cisco Prime Collaboration Deployment system are performed using the CLI.

Deploying Cisco Collaboration Application Server Clusters with Cisco Prime Collaboration Deployment

To deploy collaboration application nodes and clusters with Cisco Prime Collaboration Deployment, perform these required steps:

1. Prepare for Collaboration application deployment.

   Download the necessary OVA templates and bootable Cisco ISO images for the target collaboration application(s): Unified CM, Unified CM IM and Presence Service, and Unity Connection. Next, SFTP the Collaboration application install .iso images to the '/fresh_install' directory on Cisco Prime Collaboration Deployment.

   Note Cisco Prime Collaboration Deployment does not support the deployment of other PA collaboration applications such as Cisco Expressway, Cisco Meeting Server, and Cisco TelePresence Management Suite.

2. Deploy OVA templates and virtual machines (VMs) on the compute infrastructure ESXi host(s).

   Create one VM for each required collaboration application node using the appropriate application OVA template based on the deployment size. For example, create VMs for the Unified CM publisher, dedicated Unified CM TFTP subscribers, and Unified CM call processing subscriber nodes. Repeat this process for Unified CM IM and Presence Service nodes and Unity Connection nodes. Leave all VMs powered off.

3. Add compute infrastructure ESXi host(s) to Cisco Prime Collaboration Deployment inventory.

   Use the Cisco Prime Collaboration Deployment administrative GUI to add the ESXi host (or hosts) where your collaboration application VMs are deployed. Enter the appropriate ESXi hostname, username, and password for each host.

4. Define new Unified Communications clusters in the Cisco Prime Collaboration Deployment inventory.

   Use the Cisco Prime Collaboration Deployment administrative GUI to define Unified Communications clusters for each Unified CM, IM and Presence Service, and Unity Connection cluster. Each cluster must have a unique name. Next, add the appropriate collaboration application node VMs (previously created in step 1) to the respective clusters. Finally, configure cluster-wide settings, including credentials and passwords, certificate information, DNS, NTP, and time zones for each cluster.

5. Add an installation task for each cluster.

   From the Cisco Prime Collaboration Deployment administrative GUI, select one of the Unified Communications clusters for installation and select the appropriate installation file (Cisco ISO file) for the cluster nodes. Next, specify a start time (immediately or sometime in the future). Repeat these steps for each cluster. If manual start is selected, manually start each installation task. Finally, monitor the installation tasks and confirm that each installation completes successfully.

6. Configure the installed clusters using the application server GUI.

   Once the Cisco Prime Collaboration Deployment installation tasks have completed successfully, the base configuration of all cluster nodes will be in place. Next configure the clusters manually using information contained in the Call Control chapter (for Unified CM and IM and Presence Service clusters) and the Voice Messaging chapter (for Unity Connection clusters). Once you have configured the clusters, use Cisco Prime Collaboration Provisioning for subsequent moves, adds, changes, and deletions (MACDs) as described in the section on Cisco Prime Collaboration Provisioning.

Cisco Smart Software Manager

Cisco Smart Software Manager provides a centralized method for applying, tracking, and managing licenses on Cisco Unified CM, IM and Presence Service, and Unity Connection as well as other Cisco products. Cisco Smart Software Manager assists the administrator by automating many of the steps necessary to license users on the application servers.

Core Components

The core component of the Smart Software Manager architecture is the web-hosted Cisco Smart Software Manager portal. This portal is used to acquire, apply, and track user licenses across Unified CM and Unity Connection clusters within the enterprise deployment.

Benefits

You must use Cisco Smart Software Manager to license the Enterprise Collaboration Preferred Architecture call control and voice messaging clusters. Cisco Smart Software licensing provides the following benefits:

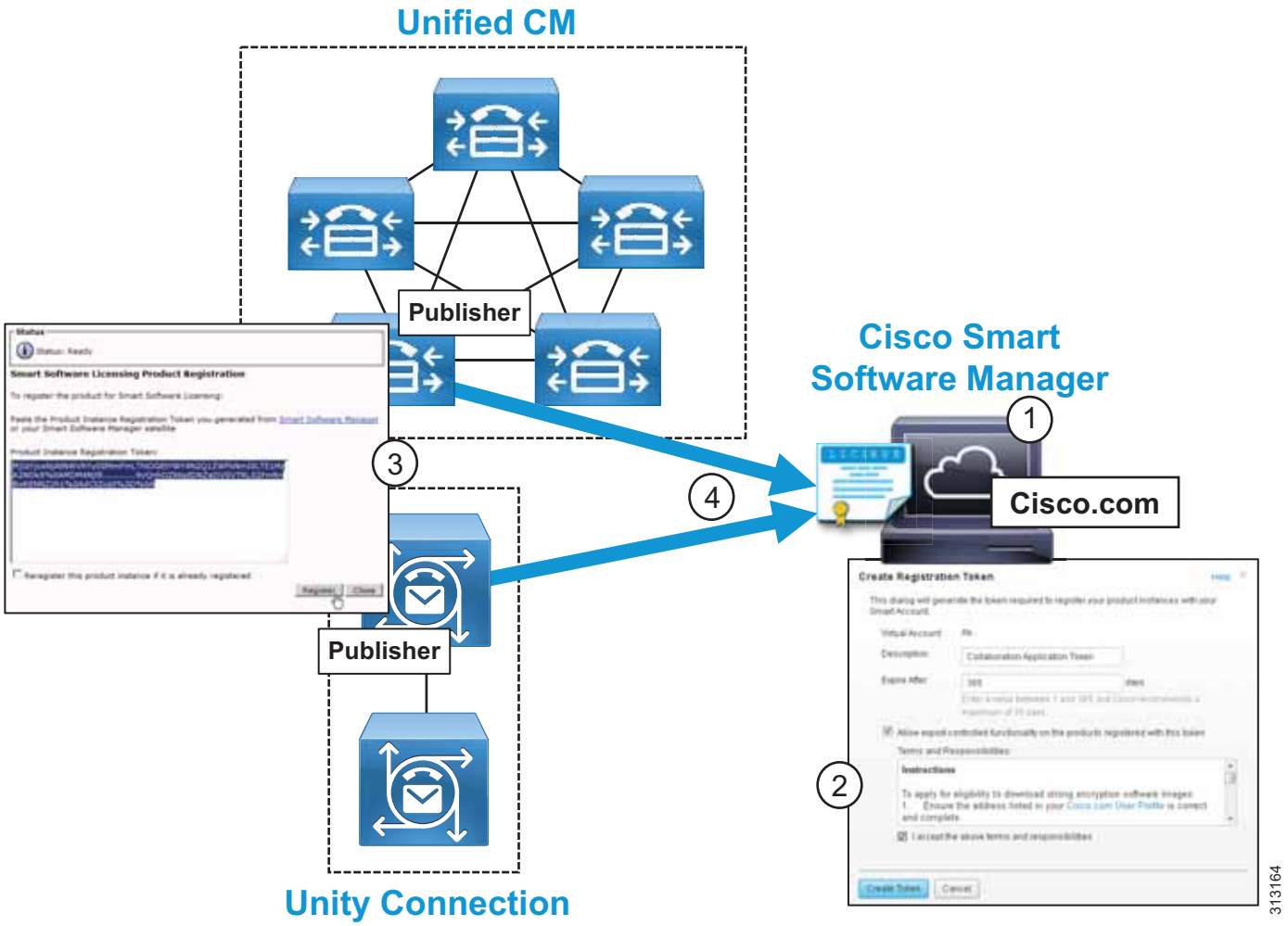
- Centralizes user and feature license management, allocation, entitlement, and reconciliation for Unified CM, Unified CM IM and Presence Service, and Unity Connection.
- Provides shared license pooling across all enterprise clusters.
- Provides enterprise-level reporting of usage and entitlement.
- Simplifies future license planning and procurement of additional licenses as the number of users within a deployment grows.

Architecture

The Cisco Smart Software Manager architecture consists of the Cisco hosted Cisco Smart Software Manager web portal, where an organization's collaboration application entitlements and licenses are tracked and synchronized to call control and voice messaging components. Cisco Smart Software Manager manages and monitors user and feature licensing for Cisco Unified CM and Unity Connection.

As shown in Figure 6-2, appropriate licenses must first be acquired and applied to the Cisco Smart Account for managing software and entitlement using the Cisco Smart Software Manager portal (step 1). Next, the administrator generates a product instance registration token on the Cisco Smart Software Manager portal at https://software.cisco.com (step 2). The administrator then registers the collaboration application publisher product instances (Unified CM and Unity Connection) using the registration token copied from the Cisco Smart Software Manager portal (step 3). Once registered, the publishers will synchronize with Cisco Smart Software Manager and receive user and feature licensing entitlement information (step 4).

Figure 6-2 Cisco Smart Software Manager Architecture



The Cisco Smart Licensing Manager service is enabled automatically on the publisher node of Cisco Unified CM and Unity Connection clusters during initial installation. Registration and synchronization between Unified CM and Unity Connection publishers and Cisco Smart Software Manager happens directly using an outbound HTTPS connection from the publisher to the Internet hosted Cisco.com Cisco Smart Software Manager service.

For more information about Cisco Smart Software Manager, see

https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html

Role of Cisco Smart Software Manager

Cisco Smart Software Manager centralizes management of user-based call control and voice messaging licenses and entitlement across enterprise collaboration application deployments. Cisco Smart Software Manager enables license planning, license entitlement and distribution, and usage tracking. Because the Cisco Smart Software Manager is hosted on the Internet, administration and management of licenses and software entitlement is done using a web browser.

Alternative Architectures for Cisco Smart Software Manager

If your organization has network availability considerations or security policies in place that prevent direct Internet access from the Cisco Unified CM and Unity Connection cluster publisher nodes, there are some additional options:

- HTTPS proxy

  If an HTTPS proxy has already been deployed within the organization, it can be used for communication with the Cisco Smart Software Manager.

- On-premises Cisco Smart Software Manager satellite system

  Cisco Unified CM and Unity Connection publishers register with and report license consumption to the Cisco Smart Software Manager satellite on-premises server instead of the online Cisco Smart Software Manager service. The satellite system must periodically connect to the online Cisco Smart Software Manager to synchronize (connected), or a report file from the system must be manually uploaded to the online service (disconnected).

  For more information on Cisco Smart Software Manager satellite, refer to

  https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

- Specific License Reservation

  Cisco Unified CM and Unity Connection are licensed by an initial manual exchange of information (cut and paste) with the Cisco Smart Software Manager service. Once the product configuration and authorization is complete, no further interaction with Cisco Smart Software Manager service is required. With this configuration, the license reservations are permanently allocated to the systems within Cisco Smart Software Manager unless or until the reservation is updated or removed. Any update to the reservation requires another manual exchange of information between the Cisco Smart Software Manager service and the Unified CM and Unity Connection systems.

High Availability for Cisco Smart Software Manager

The online Cisco Smart Software Manager application is highly available; however, in the case of an Internet connection issue, the collaboration application systems will continue to operate for 90 days. User and device provisioning is not possible once the systems reach full non-compliance. In order to maintain system operation, the online Cisco Smart Software Manager must be reachable consistently.

Scaling Cisco Smart Software Manager

Because Cisco Smart Software Manager is an Internet-hosted online service, there are few or no scalability considerations. The primary sizing considerations from an enterprise prospective are Internet connection bandwidth and network availability.

Cisco Smart Software Manager Deployment Process

There are two deployment aspects to consider with Cisco Smart Software Manager:

- Managing Licenses and Entitlement with the Cisco Smart Account and Smart Software Manager
- Authorizing and Registering Collaboration Product Instances and Applying Licenses

Managing Licenses and Entitlement with the Cisco Smart Account and Smart Software Manager

In order to license the collaboration applications, you first need to procure appropriate collaboration user and feature licensing before you can authorize the collaboration application systems. Once you have purchased the appropriate licenses, you can apply those licenses to your Cisco Smart Account.

Next, access the Cisco Smart Software Manager (https://software.cisco.com) using your Cisco Smart Account. Once logged into the Cisco Smart Software Manager, select (or create) the relevant virtual account (organization dependent). Under the virtual account you can manage collaboration licenses, view licenses and license usage, and register product instances.

For information on Cisco Smart Accounts, see:

https://www.cisco.com/c/en/us/buy/smart-accounts.html

Authorizing and Registering Collaboration Product Instances and Applying Licenses

Smart Licensing is automatically enabled by default on the Cisco Unified CM and Unity Connection publishers. However, until your products are registered to the Cisco Smart Software Manager and licenses have been applied to the system, your system will be out of compliance and after the grace period will have severely reduced capabilities and functionality.

In order to manage user licensing for call control and voice messaging clusters with Cisco Smart Software Manager, perform the following required steps:

1. Create a product instance registration token

   To set up Smart Licensing, go to the Smart Software Manager and under your virtual account create a new product instance registration token by clicking the **New Token…** button. In the subsequent dialog box specify a small number of days that the registration token will be valid (**Expires After:**), check the **Allow export-controlled functionality...** check box along with the **I accept the above terms and responsibilities** check box, and then click **Create Token**.



Note The registration token validity length (in days) should be set to a small value (for example, 3). The token needs to be valid only during the initial Smart License registration process. After that, the token may be revoked and/or removed so that it cannot be used again.

2. Register product instances

   Next register the Unified CM and Unity Connection publishers by copying the product instance registration token from the Smart Software Manager portal and entering it in the device/product license window. On the Unified CM and Unity Connection license pages, click the **Register** button. In the resulting pop-up window, enter the product instance registration token in the Smart Software Licensing Product Registration window and click the **Register** button to complete registration.

Once the Unified CM and Unity Connections publishers are registered, they synchronize with Cisco Smart Software Manager to receive licensing and authorization for current users and features.

The above registration and authorization operations require a valid Smart Account for managing your Cisco software and licensing and appropriate product licensing entitlement.

Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration Provisioning provides a scalable web-based solution to help administrators manage the provisioning needs of an integrated IP telephony, video, voicemail, and unified messaging environment. Cisco Prime Collaboration Provisioning can be used for day-to-day configuration updates such as moves, adds, changes, and deletions (MACD).

For the Enterprise Collaboration Preferred Architecture, we recommend performing the initial configuration manually using information contained in the Call Control chapter (for Unified CM and IM and Presence Service clusters) and the Voice Messaging chapter (for Unity Connection clusters). Once you have configured the clusters, you can then use Cisco Prime Collaboration Provisioning to perform subsequent operational configuration updates (MACDs) for Unified CM, the IM and Presence Service, and Unity Connection as needed.

Benefits

Using Cisco Prime Collaboration Provisioning to perform moves, adds, changes, and deletions (MACDs) provides the following features and benefits:

- Cisco Prime Collaboration Provisioning allows for a single, consolidated view of users across the organization and across clusters.
- MACDs can be tracked and audited by means of an order number assigned to each MACD request.
- MACDs can be executed as a batch file rather than one at a time manually.
- Service Templates help speed up MACDs and reduce configuration errors that can often occur with manual configuration.
- The batch file can be executed during non-peak hours to avoid potential interruptions to user services.

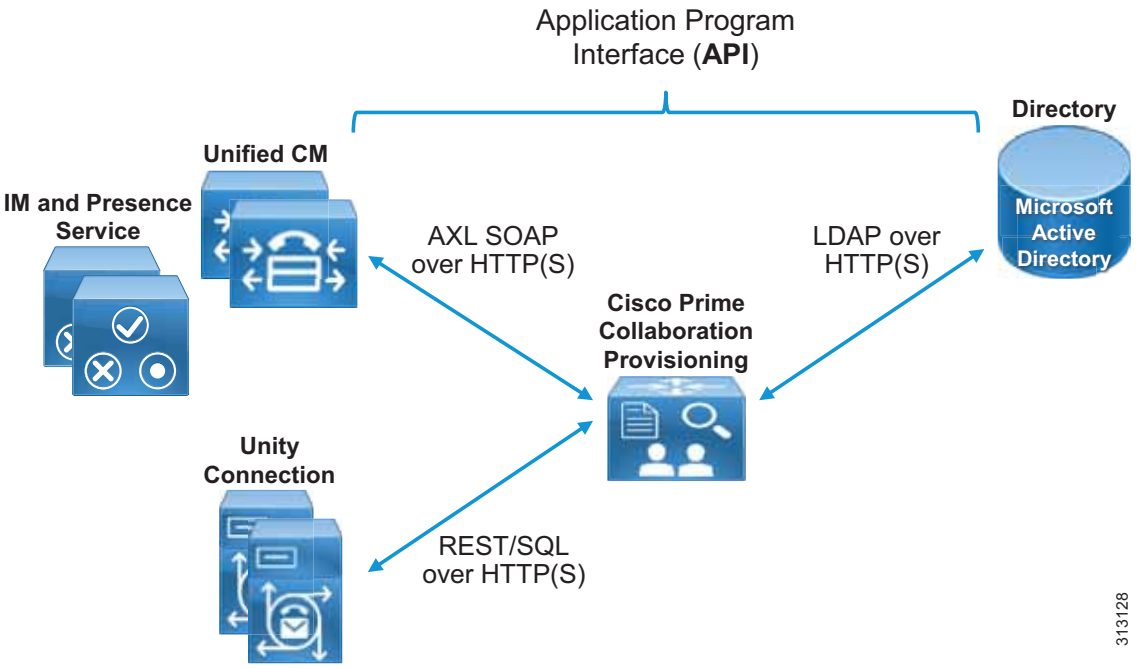
Architecture

The architecture for Cisco Prime Collaboration Provisioning consists of the Cisco Prime Collaboration Provisioning server node, Cisco Unified CM, the IM and Presence Service, and Unity Connection. Cisco Prime Collaboration Provisioning uses various APIs to connect with and configure the collaboration application servers.

Role of Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration Provisioning manages configuration changes for IP communication endpoints and services in an integrated IP telephony, video, voicemail, and unified messaging environment that includes Cisco Unified Communications Manager and Cisco Unity Connection. Figure 6-3 shows the components and APIs.

Figure 6-3 Cisco Prime Collaboration Provisioning Architecture



Protocols Used to Communicate with Unified Communications Applications

Cisco Prime Collaboration Provisioning uses the following protocols to communicate with its managed applications (see Table 6-2):

- Cisco Unified CM and Cisco Unified CM IM and Presence Service

  Cisco Prime Collaboration Provisioning communicates with Unified CM and the IM and Presence Service via AXL SOAP over an HTTPS API that enables remote provisioning of Unified CM and the IM and Presence Service.

- Cisco Unity Connection

  Cisco Prime Collaboration Provisioning uses REST and SQL over HTTPS to provision Cisco Unity Connection.

- Directory servers (Microsoft Active Directory)

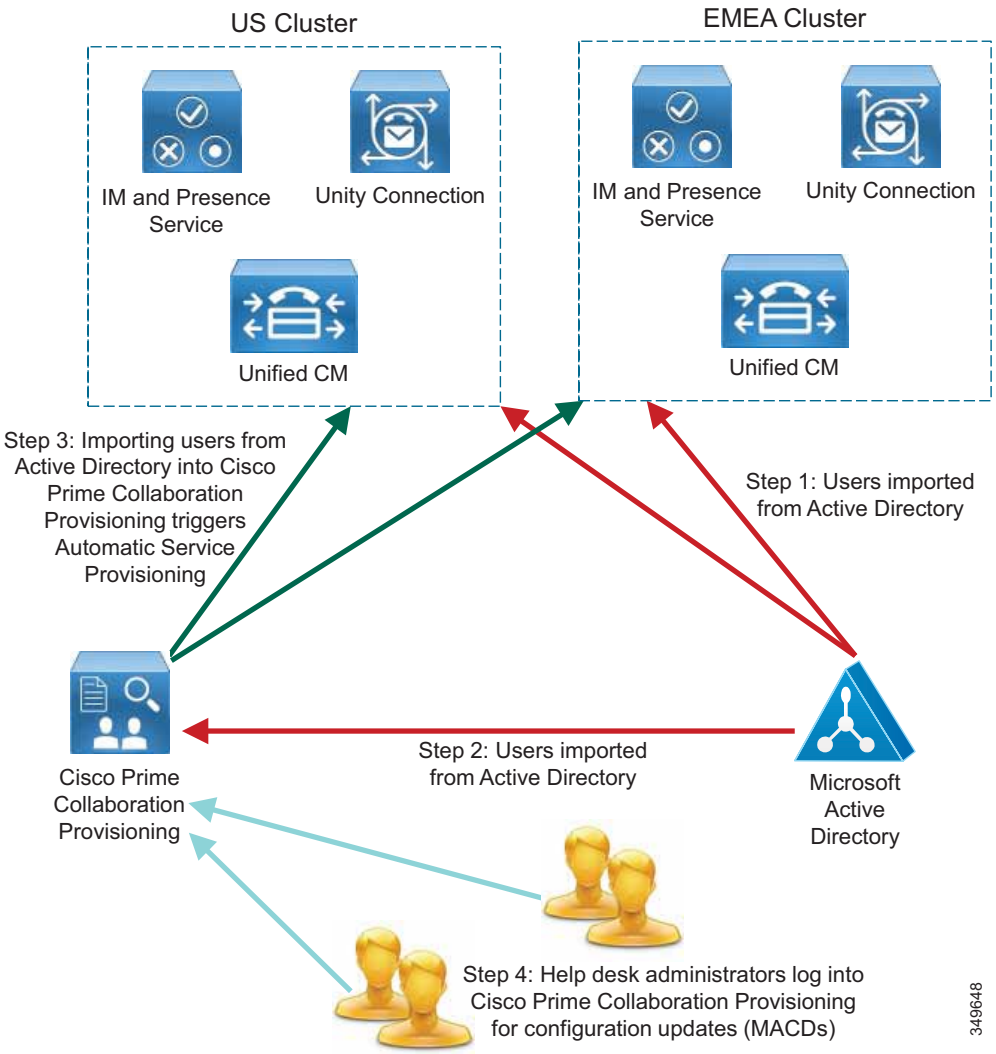
  Cisco Prime Collaboration Provisioning uses LDAP to communicate with the Microsoft Active Directory server. We recommend enabling SSL, so that the communication is LDAP over HTTPS; otherwise Cisco Prime Collaboration Provisioning uses LDAP over HTTP.

Table 6-2 Summary of Protocols Used by Cisco Prime Collaboration Provisioning

Unified Communications Application	Protocols Used by Cisco Prime Collaboration Provisioning
Cisco Unified CM and IM and Presence Service	AXL SOAP over HTTPS API
Cisco Unity Connection	REST and SQL over HTTPS
Directory servers (Microsoft Active Directory)	LDAP over HTTPS (recommended) or LDAP over HTTP

For the day-to-day operational provisioning of moves, adds, changes and deletions (MACD), the administrator must create user accounts on Cisco Prime Collaboration Provisioning, and this can be done by integrating it with the Microsoft Active Directory server or by synchronizing users from Cisco Unified CM (see Figure 6-4). Users can also be added manually into Cisco Prime Collaboration Provisioning via batch or from the graphical user interface. For the Enterprise Collaboration Preferred Architecture, we recommend having LDAP synchronization enabled in both Unified CM and Cisco Prime Collaboration Provisioning to support Automatic Service Provisioning for user on-boarding (automatically provisioning services when the user is added to the directory server) and off-boarding (deleting all the services for a user when the user is removed from the directory server). Because Cisco Prime Collaboration Provisioning and all the Unified Communications applications synchronize with the directory server, this raises the question of which applications synchronizes first with the directory server. If Cisco Prime Collaboration Provisioning syncs first and downloads a new user, and if that user is not found on the Unified Communications applications, Cisco Prime Collaboration Provisioning has to wait until that user shows up in the Unified Communications applications and then it triggers Automatic Service Provisioning (ASP) if ASP is enabled for that user role. Therefore, we recommend using Active Directory server synchronization and scheduling the synchronization so that the Unified Communications applications synchronize before Cisco Prime Collaboration Provisioning does. The rest of this chapter assumes that this recommendation is followed.

Figure 6-4 Cisco Prime Collaboration Provisioning Synchronization with Microsoft Active Directory



Cisco Prime Collaboration Provisioning Terminology

This section explains the terminology used to describe the most important concepts and main features of Cisco Prime Collaboration Provisioning. This terminology is used throughout this chapter:

- Domain — Domains are groupings of users managed by one or more administrators. A domain administrator handles moves, adds, changes, and deletions (MACD) for all users in that domain.
- Service Area — Service Areas are groupings within a Domain that typically represent locations or sites, and they provide a template mechanism that determines provisioning attribute values used during configuration update (MACD) operations.

- User Role — User Roles provide policy enforcement by controlling which Unified Communications features are allowed for various classes of users, 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 Template — Service Templates allow small or large amounts of settings to be collected into a single template that can be applied to endpoints or services. This saves time compared to setting many individual attributes, and it 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.
- Business Rule — Business Rules or policies may be set on a Domain, and these rules and policies apply to services for users in that Domain.
- Infrastructure Synchronization — This is a download process from Cisco Unified CM and Cisco Unity Connection into Cisco Prime Collaboration Provisioning that downloads only objects not specific to individual users.
- User Synchronization — This is a download process from Cisco Unified CM and Cisco Unity Connection into Cisco Prime Collaboration Provisioning that discovers all user accounts and all objects related to individual users.
- Domain Synchronization — This is a process that associates existing users, discovered from all Unified Communications clusters during user synchronization, into their respective Domains.
- Batch Engine — The Cisco Prime Collaboration Provisioning batch engine can be used to perform bulk operations on a large number of users and their services. Unlike Cisco Unified CM BAT files that run only on Cisco Unified Communications Manager (Unified CM), Cisco Prime Collaboration Provisioning batch files can execute commands on multiple Unified Communications applications.

Cisco Prime Collaboration Provisioning Deployment Process

To install Cisco Prime Collaboration Provisioning, download the Cisco Prime Collaboration Provisioning Medium OVA template (for up to 20,000 endpoints). This is the template used for the Enterprise Collaboration Preferred Architecture.

The format for the OVA template file name is: **cpc-provisioning-**<*version number*>**-**<*build number*>**-**<*deployment size*>**.ova**, where the version number is the Cisco Prime Collaboration Provisioning release number. For the Enterprise Collaboration Preferred Architecture, download the OVA template file named:

cpc-provisioning-12.2.0.659-medium_SIGNED.ova

Once the OVA template installation is complete, you can power on the system and configure the network details (IP address, Netmask, Gateway, DNS, NTP). For detailed instructions on the installation process, refer to the latest version of the *Cisco Prime Collaboration Provisioning Install and Upgrade Guide*, available at

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html

Configuration Updates Using Cisco Prime Collaboration Provisioning

This section describes how to use Cisco Prime Collaboration Provisioning to make configuration updates (moves, adds, changes, and deletions) for the Unified Communications applications in the Enterprise Collaboration Preferred Architecture.

Perform the following steps to deploy Cisco Prime Collaboration Provisioning and use it for configuration updates (MACDs) of your Unified Communications applications. Following these steps in order will minimize the impact of dependencies and will deploy Cisco Prime Collaboration Provisioning in the most efficient way.

1. Connect Cisco Prime Collaboration Provisioning with the Unified Communications applications.

   The Unified Communications applications can be added to Cisco Prime Collaboration Provisioning by putting in the credentials required for Cisco Prime Collaboration Provisioning to connect to them. This can be done from the **Device Setup** menu. Note that only the publisher node of Unified CM and Unity Connection need to be added here.

2. Create domains. Domains are groupings of users and administrators who manage various sites.

   We recommend creating the domains based on the number of administrators in your organization. For example, for two clusters (US and EMEA) the number of domains could be two if there are two groups of administrators: one group to handle MACDs for US users and another group of administrators to handle MACDs for EMEA users. However, more domains could also be created if your organization wants to create smaller administrative groups with fewer users. For instance, you could create domains for the states in the US or the countries in EMEA.

3. Add and/or edit user roles.

   Once the domains are created, the user roles have to be created within each domain. Cisco Prime Collaboration Provisioning automatically creates a few default user roles that the administrator can change, and more roles can be created if required. Also, if necessary, Automatic Service Provisioning can be enabled on the user roles to enable user on-boarding (provisioning services automatically when the user is added to Active Directory and comes into Cisco Prime Collaboration Provisioning after Cisco Prime Collaboration Provisioning synchronizes with Active Directory) and off-boarding (deleting services automatically when the user is removed from Active Directory).

4. Synchronize the infrastructure components.

   Cisco Prime Collaboration Provisioning must be synchronized with the Unified Communications applications. During this step, Cisco Prime Collaboration Provisioning downloads the configuration from Unified CM, Unity Connection, and Unified CM IM and Presence Service. The device pools, locations, and partitions downloaded from Unified CM and the voicemail templates downloaded from Unity Connection are necessary in the next step, which is to create service areas.

5. Create service areas.

   Service areas contain a set of service parameters: mainly, the device pool, location, voicemail template, and directory number (DN) block. We recommend mapping a service area to a site or a physical location. These service areas are contained within a domain and apply only to the users in that domain. Because each service area is connected to a specific device pool and a location, the various combinations of the mandatory attributes could create a large number of service areas, so we recommend cleaning up unused device pools and/or not creating service areas for those unused device pools. If the number of service areas becomes too large to manage, then it might be a good idea to increase the number of domains in order to reduce the number of service areas within each domain.

6. Create service templates for the phones, lines, voicemail, and so forth.

   These service templates can be applied readily at order time to minimize human errors, thereby reducing configuration errors. We recommend creating service templates for the most popular endpoint models, lines, and voicemail services as well as for Extension Mobility and Remote Destination Profiles if required.

7. Configure LDAP, user, and domain synchronization.

   Once the templates are created and assigned to user roles and Service Areas in the Service Templates section, LDAP synchronization can be run to bring users into Cisco Prime Collaboration Provisioning from the Microsoft Active Directory server. Advanced queries can be written for Domain LDAP filter, Service Area LDAP filter, and User Role LDAP filter, and we highly recommend filtering out users based on specific attributes. Importing users from Active Directory will trigger Automatic Service Provisioning (ASP) and Cisco Prime Collaboration Provisioning will then configure the services specified in the ASP section under the default user role specified in the Business rules section. Make sure that the Active Directory server is synchronized to Unified CM and Unity Connection before Cisco Prime Collaboration Provisioning synchronizes with the Active Directory server. Because Unified CM and Unity Connection are integrated with the Active Directory server, both of these applications are marked as “LDAP integrated” under the Device Setup in Cisco Prime Collaboration Provisioning. Thus, Cisco Prime Collaboration Provisioning waits for the users to show up on those applications before provisioning services. A Domain Synchronization is necessary after the Infrastructure Synchronization and User Synchronization are completed.

8. Assign provisioning privileges, domain administrators, and other administrators from the Access Control menu.

9. Start taking orders for provisioning services.

10. Create batch files for frequently performed actions.

Using Cisco Prime Collaboration Provisioning to Troubleshoot Configuration Updates

Cisco Prime Collaboration Provisioning provides a convenient way to look at the trace messages and to collect log files. Cisco Prime Collaboration Provisioning writes application log files for the Service Enabling Platform (SEP) module (sep.log) and the Network Interface and Configuration Engine (NICE) service (nice.01.log). The log files are located in the /opt/cupm/sep/logs folder. These logs can also be accessed from the **Logging** and **ShowTech** menu options under **Administration**. The Application Level and the Nice Level logs can be set to DETAILED before troubleshooting, along with logging the messages that are exchanged with Unity Connection, Unified CM, and Unified CM IM and Presence Service. Use **Generate ShowTech** to collect the traces, and if the administrator chooses to view the logs in the user interface, then the **Browse Logs** > **Application and NICE logs** option can be selected. This allows the administrator to view the logs in the browser windows or to download them to the local computer. These logs contain a lot of messages that can be very helpful to troubleshoot any issues that could occur during the day-to-day configuration updates (MACDs).

Redundancy and Backup for Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration Provisioning supports backing up and restoring the configuration and data. We highly recommend having Cisco Prime Collaboration Provisioning back up the configuration and data to an external server via FTP or SFTP. Detailed instructions on performing the backup and restore can be found in the product documentation for Cisco Prime Collaboration Provisioning, available at

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