CHAPTER 6

Collaboration Management Services

Revised: May 21, 2021

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 Webex Cloud-Connected UC for Webex cloud-based monitoring and management of on-premise collaboration applications.

The collaboration management services include:

- Cisco Prime Collaboration Deployment
- Cisco Smart Software Manager
- Webex Cloud-Connected UC

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.
- Single pane of glass for both cloud and on-premises UC management, simplifies and augments monitoring and reporting features across a deployment.

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
Webex Cloud-Connected UC	Webex Cloud-Connected UC	May 21, 2021
Cisco Meeting Server and Cisco Expressway applications add support for Cisco Smart Licensing with Cisco Smart Software Manager (SSM)	Cisco Smarttt Softeware Manager	May 21, 2021
Removed Cisco Prime Collaboration Provisioning		May 21, 2021

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

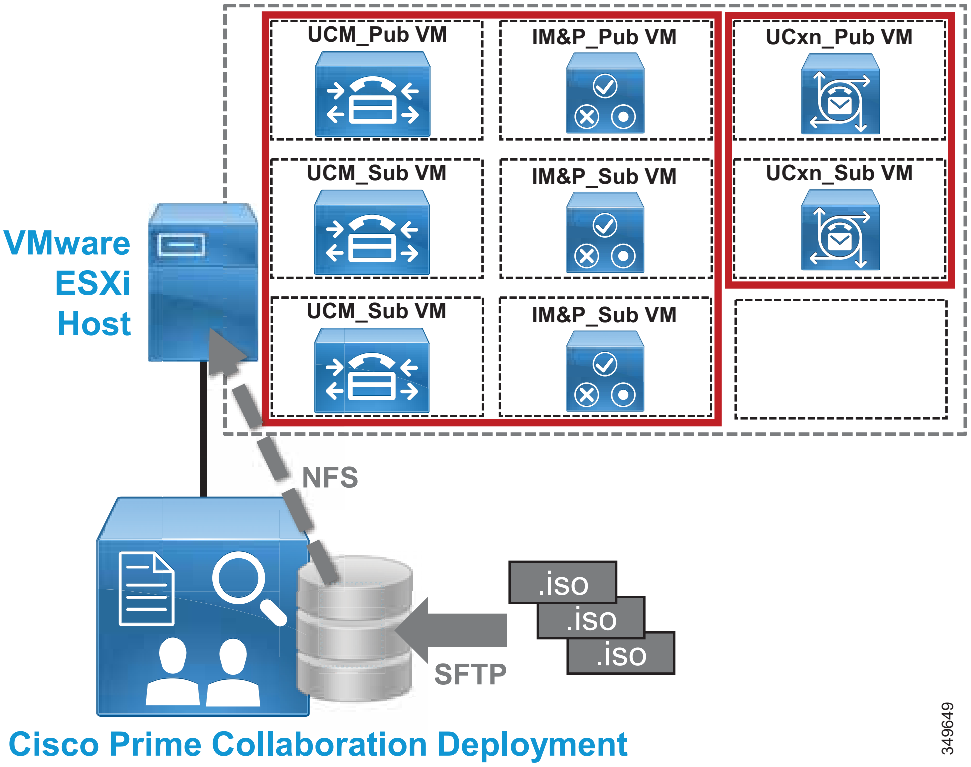
Using Cisco Prime Collaboration Deployment to deploy the Enterprise Collaboration Preferred Architecture call control and voice messaging application nodes provides the following benefits:

- 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 Webex Cloud-Connected UC.

Cisco Smart Software Manager

Cisco Smart Software Manager provides a centralized method for applying, tracking, and managing licenses on Cisco Unified CM, Cisco Unity Connection, Cisco Meeting Server (CMS), and Cisco Expressway 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, Unity Connection, CMS, and Expressway clusters within the enterprise deployment.

Benefits

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

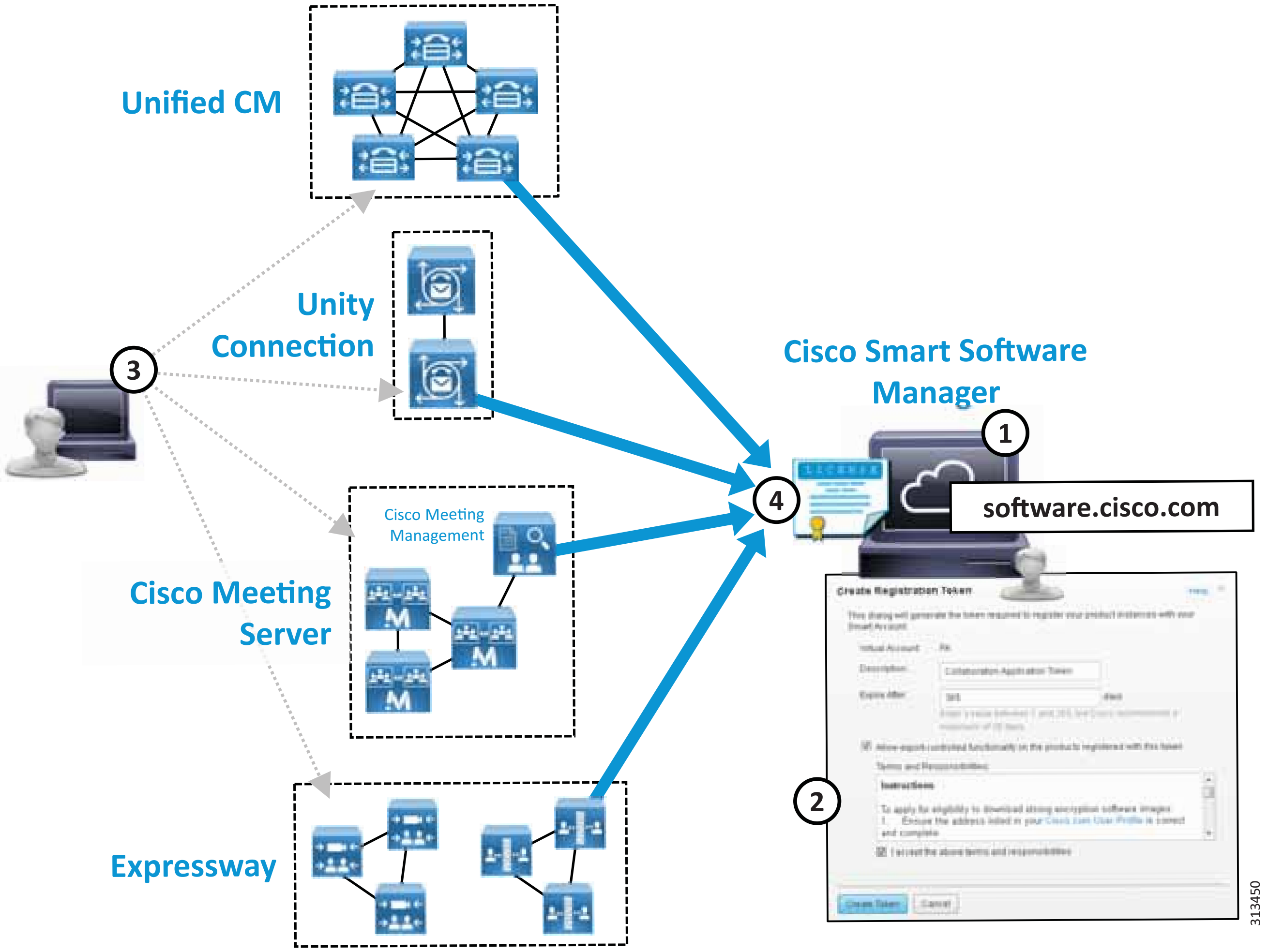
- Centralizes user and feature license management, allocation, entitlement, and reconciliation for Unified CM, Unity Connection, CMS, and Expressway.
- Provides shared license pooling across all enterprise clusters.
- Provides enterprise-level reporting of usage and entitlement.
- Simplifies future license 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, conferencing, and edge components. Cisco Smart Software Manager manages and monitors user and/or feature licensing for Cisco Unified CM, Unity Connection, CMS, and Expressway.

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 product instances (Unified CM, Unity Connection, CMS, and Expressway) 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/or feature licensing entitlement information (step 4).

Figure 6-2 Cisco Smart Software Manager Architecture



Create Registration Token

Help

This dialog will generate the token required to register your product instances with your Smart Account

Virtual Account: PA

Description: Collaboration Application Token

Expire After: 365 days

Enter a value between 1 and 365, but Cisco recommends a maximum of 30 days.

☑ Allow export-controlled functionality on the products registered with this token

Terms and Responsibilities

Instructions

To apply for eligibility to download strong encryption software images:
1. Ensure the address listed in your Cisco.com User Profile is correct and complete.

☑ I accept the above terms and responsibilities

Create Token | Cancel

Note CMS licensing is managed by Cisco Meeting Management (CMM) which handles communication with Cisco Smart Software Manager.

The Cisco Smart Licensing Manager service is enabled on appropriate application cluster nodes during initial installation or configuration. Registration and synchronization between collaboration applications and Cisco Smart Software Manager happens directly using an outbound HTTPS connection from the node(s) to the Internet hosted 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 collaboration application clusters, 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.

- Cisco Smart Software Manager On-Prem (formerly Smart Software Manager satellite).

  Application cluster nodes register with and report license consumption to the Cisco Smart Software Manager On-Prem 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 On-Prem, refer to

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

- Specific License Reservation

  Applications 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 process 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 collaboration systems. Specific License Reservation is not supported with CMS/CMM or Expressway.

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 without impacting administrator or user experience for 90 days. Limitations to configuration and provisioning as well as intrusive warning notifications occur 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 perspective 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 available by default on the appropriate application nodes. 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, capacity, and user experience.

In order to manage user licensing for collaboration applications 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 **Allow export-controlled functionality** option is not shown for Smart Accounts that are not authorized to use export-controlled functionality.

2. Register product instances

   Next register the collaboration applications by copying the product instance registration token from the Smart Software Manager portal and entering it in the device/product license window. On the application server license page, 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 collaboration applications 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.

Webex Cloud-Connected UC

Webex Cloud-Connected UC is a set of cloud services delivered by Webex and managed through Webex Control Hub that provides centralized and simplified on-premises collaboration application management and visibility.

Webex Cloud-Connected UC (CCUC) is designed for customers with on-premises collaboration deployments with Unified CM that want to move some of administrative workloads to the Webex cloud while still maintaining their on-premises calling workload.

Core Components

The core component of the Webex Cloud-Connected UC architecture is the web-hosted Webex Control Hub portal. This portal is used to access CCUC services for on-premises collaboration applications within the enterprise deployment.

Benefits

You should use Webex Cloud-Connected UC for analytics with the Enterprise Collaboration Preferred Architecture call control and other application clusters. Webex CCUC provides the following benefits:

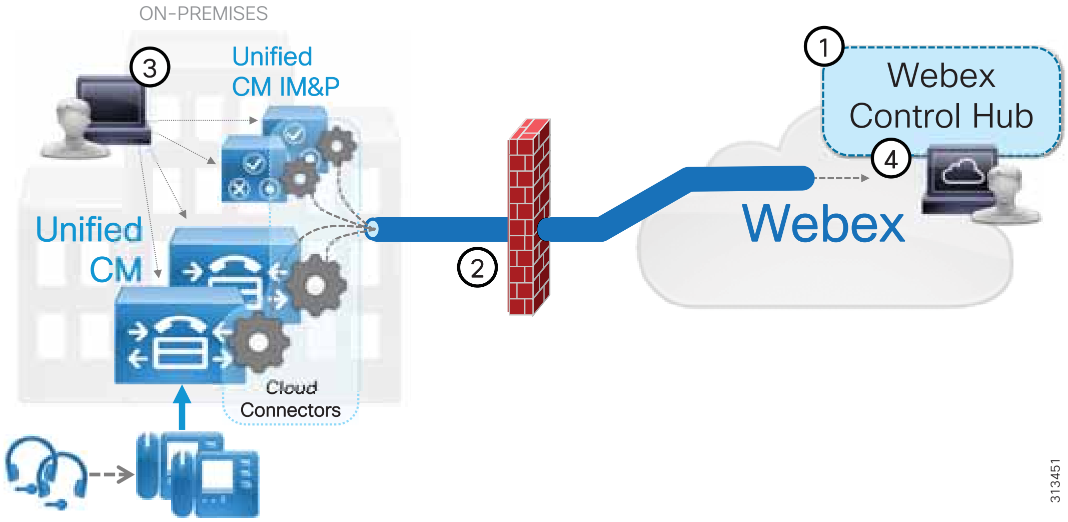
- Webex Control Hub provides a single pane of glass for both cloud and on-premises UC management.
- Solution enabled by cloud connectors running on infrastructure collaboration application nodes.
- Lower total cost of ownership (TCO) as customer gains cost optimized insights and increased administrative productivity through automated workflows.
- Delivers analytics for broad business and operations actionable insights for collaboration products.
- Enables customer to maintain business-critical calling and media on-premises.
- Simplifies and augments monitoring and reporting features and workflows for Cisco on-premises UC collaboration deployments.
- Industry leading Webex security and privacy with disaster recovery and redundancy.
  - All data is encrypted at rest and in transit.
  - Cisco Webex Identity Services infrastructure is used to authenticate and authorize cloud connectors to a specific Webex Control Hub organization.
  - All the data sent by CCUC is outlined in the privacy data sheet maintained at the Trust Portal (https://trustportal.cisco.com).

Architecture

The Webex Cloud-Connected UC architecture includes on-premises collaboration applications like Unified CM and the Webex Control Hub web portal, where an organization's collaboration application analytics are collected, and other management and monitoring tasks are conducted.

As shown in Figure 6-3, a Webex organization with Webex Control Hub access and UC Management enablement is required in order to enable Webex CCUC and access analytics (step 1). Next, the on-premises network firewalls must be configured to allow outbound communication to Webex (step 2). The administrator then onboards on-premises application nodes to activate CCUC (step 3). Once on-premises application cluster nodes are onboarded, the administrator must verify application nodes with Webex Control Hub to complete onboarding and begin collecting information about on-premises systems (step 4).

Figure 6-3 Webex Cloud-Connected UC Deployment Architecture



A cloud connector is enabled on appropriate application cluster nodes during initial configuration and onboarding. The connector manages the synchronization between collaboration applications and Webex Control Hub which happens directly using outbound HTTPS connections from the node(s) to the Internet-hosted Webex cloud services on TLS port 443.

For more information about Webex Cloud-Connected UC, see

https://help.webex.com/en-us/jv0u1db/Cisco-Webex-Cloud-Connected-UC-Overview

Role of Webex Control Hub

Webex Control Hub centralizes monitoring and analytics across enterprise collaboration deployments by extending cloud management services to on-premises applications. Webex Control Hub enables single pane of glass management and monitoring providing administrators a central location to view and analyze applications and services operations and utilization. Because the Webex Control Hub is hosted on the Internet, administration of management and analytics is done using a web browser.

High Availability for Webex Cloud-Connected UC

The online Webex Control Hub is highly available; however, in the case of an Internet connection issue, the collaboration application systems will continue to collect analytics and other information to send to Webex. However, without a network connection to Webex this information cannot be sent and as such cloud-based monitoring and analytics capabilities will not be available until access to Webex Control Hub has been restored. In the meantime, traditional on-premises collaboration application management and monitoring tools may be used. In order to maintain Webex Control Hub analytics and monitoring of on-premises systems, access to Webex over the Internet must be maintained consistently.

Scaling Webex Cloud-Connected UC

Because Webex Control Hub is an Internet-hosted online service, there are few or no scalability considerations. The primary sizing considerations from an enterprise perspective are Internet connection bandwidth and network availability.

Webex Cloud-Connected UC Deployment Process

There are two deployment aspects to consider with Webex Cloud-Connected UC:

- Managing Analytics, Reporting, and Monitoring with Webex Control Hub
- Configuring Webex Cloud-Connected UC and Onboarding On-Premises Applications

Managing Analytics, Reporting, and Monitoring with Webex Control Hub

In order to manage collaboration applications analytics, reporting, and monitoring with Webex Cloud-Connected UC (CCUC), you must first procure a Webex organization with CCUC entitlement in order to access the Webex Control Hub and Connected UC services.

Next, access the Webex Control Hub (https://admin.webex.com) using your Webex administrator account. Once logged into Webex Control Hub, to configure and manage CCUC, select **Connected UC** under the *Services* section of the left-hand navigation pane. You will see on-premises application node and cluster inventory information here as you onboard application server nodes.

Within Webex Control Hub, analytics for CCUC-enabled on-premises applications is available via the Connected UC Analytics page (select Analytics under the Monitoring section of the navigation pane).

For more information on Webex Control Hub, see:

https://help.webex.com/ld-nwespu1-CiscoWebexControlHub/Control-Hub

Configuring Webex Cloud-Connected UC and Onboarding On-Premises Applications

Note The following deployment steps rely on the use of CLI commands at the collaboration application nodes to onboard the server and activate CCUC. Although not discussed, an alternate method for onboarding the nodes and activating CCUC is available which relies on the installation of an agent install or COP (.cop) file. This file is downloaded from Webex Control Hub (**Connected UC > UC Management > Install Files**) and installed on each collaboration application node.

1. Prepare Webex Control Hub for on-premises node onboarding.

   To begin, login to Webex Control Hub with organization administrator account. Once logged in add a collaboration application cluster group by navigating to the UC Management Inventory page (under *Services*: Connected **UC > UC Management > Inventory**) and clicking the **Add Cluster Group** button. Enter the cluster group name (for example, ‘PA Unified CM Cluster’) and cluster group description (for example, ‘Primary Unified CM cluster’) and then click **Save**.

Note The above Webex Control Hub operations require a valid Webex organization with Connected UC entitlement.

2. Update on-premises firewalls and networks to allow communication with Webex cloud.

Next, prepare the on-premises firewall and any network access control lists to allow outbound communication from collaboration application server nodes to Internet-based Webex cloud services. Outbound HTTPS traffic on TLS port 443 should be allowed to the following URLs:

- *.ucmgmt.cisco.com
- *.webex.com

If your organization utilizes an HTTP proxy for connections to the Internet, you should configure the cloud connector to utilize this proxy for all external communications. On each collaboration application node use the CLI **utils ucmgmt proxy** set of commands to configure and manage proxy information.

For more information on preparing the enterprise network for CCUC, see:

https://help.webex.com/en-us/fg3qim/Network-Requirements-for-Cisco-Webex-Cloud-Connected-UC

For more information on configuring the on-premises proxy for CCUC, see:

https://help.webex.com/en-us/ty4jte/Add-a-Proxy

3. Onboard on-premises application nodes.

Once a cluster group has been configured on Webex Control Hub and the on- premises network and firewall allow outbound communication to Webex, you are ready to onboard your collaboration application server nodes.

To onboard an application node, first use the CLI **utils ucmgmt organization** command to associate the application node with your organization. You can find your organization ID in Webex Control Hub by navigating to the Account page (under *Management*: **Account**).

Once the organization ID is configured, use the **utils ucmgmt agent** CLI command set to enable and manage the cloud connector UC management agent.

Repeat these CLI commands at each collaboration application node you wish to onboard.

Note You must set the following global and per node CDR related service parameters values to enable call quality metrics for CCUC: **Call Diagnostics Enabled** set to ‘Enabled Only When CDR Enabled Flag is True’ (global), and **CDR Enabled Flag** and **CDR Log Calls with Zero Duration Flag** are set to ‘True’ (per node). These parameters were covered earlier in the Call Control chapter and should already be configured as above.

4. Complete node onboarding by verifying and assigning nodes to a cluster group.

To complete application node onboarding, return to Webex Control Hub and again navigate to the UC Management Inventory page (under Services: **Connected UC** > **UC Management** > **Inventory**). Once there, you should see a cluster and set of nodes requiring assignment to a cluster group. Begin by clicking **Resolve** next to the cluster and nodes requiring assignment.

On the next screen, click **Verify** next to each cluster node requiring verification. On the subsequent screen, compare the displayed verification code for each node with the verification code displayed at the node when using the CLI command **utils ucmgmt agent verification**. Ensure that the verification code displayed on Webex Control Hub matches the verification code displayed at the application CLI.

Finally, assign the node to a cluster group by selecting the cluster group that you created earlier from the dropdown menu (for example, ‘PA Unified CM Cluster’) and then clicking the checkmark next to each node to verify and assign to the cluster group.

As indicated previously, analytics information can be found on the Connected UC Analytics page (select **Analytics** under the *Monitoring* section of the navigation pane). It will be the next day before Connected UC analytics information begins to display.

For more information on deploying Webex Cloud-Connected UC, see:

> https://help.webex.com/en-us/nzt6c0b/Set-Up-Cisco-Webex-Cloud-Connected-UC-for-On-Premises-Devices