

Cisco Prime Collaboration Assurance/Analytics 9.5

Deployment Guide

September 2013

Contents

Scope	4
Introduction	4
Small, Medium, Large, and Very Large Enterprises	8
Voice and Video Infrastructure	8
Installation	10
Prerequisites	10
Server Requirement	11
Client Requirement	11
Preparing for Installation	11
Checking Port Availability	12
Upgrading Deployments	12
Licensing the Product	12
Preparing the Network	12
Required Device Protocols and Software Versions	12
Verifying Credentials	13
Preparing Call Scheduling and Calendaring for Cisco Prime Collaboration Assurance	14
Preparing Cisco TelePresence Management Suite	14
Enable HTTP	14
Enable SNMP	14
Preparing Cisco TelePresence Manager	16
Enable HTTP	17
Enable SNMP	17
Preparing Multipoint Bridges and Switches for Conferencing	17
Preparing MCUs for Cisco Prime Collaboration Assurance	17
Enable HTTP	18
Enable SNMP	18
Preparing Cisco TelePresence Multipoint Switch for Cisco Prime Collaboration	18
Enable HTTP	18
Enable SNMP	18
Preparing the Cisco TelePresence Server (Appliance and Blade)	19
Enable HTTP	19
Enable SNMP	19
Preparing Call Controllers and Processors for Cisco Prime Collaboration Assurance	19
Preparing Cisco Unified Communications Manager	19
Enable HTTP	19
Enable SNMP	20
Enable JTAPI	21
Configuring Syslog on Cisco Unified Communications Manager	23
Configure Cisco Unified Communications Manager to Send Call Records to Cisco Prime Collaboration	25
Preparing Cisco TelePresence Video Communication Server	26
Enable HTTP	26
Enable SNMP	27
Preparing Video Endpoints	27
Cisco TelePresence Server Video Endpoints	27
Enable HTTP	27
Enable SNMP	27
Enable CLI Access	28
Cisco TelePresence C and EX Series Video Endpoints	28
Enable HTTP	28
Enable SNMP	29
Enable CLI Access	29
Preparing Network Devices	30
Nonmedianet Routers and Switches	30
Medianet-Capable Routers and Switches	30

Discovering the Network	32
Logical Discovery	32
Discovery Using Cisco TelePresence Manager or Cisco TelePresence Management Suite	32
Diagnostic Tests	33
Synthetic Tests	33
Synthetic Test Descriptions and Expected Results	33
Creating Synthetic IP Phones in Cisco Unified Communications Manager	35
Node-to-Node Tests	35
Preparing Devices for Node-to-Node Tests	35
Node-to-Node Test Events	36
Batch Tests	36
Understanding Phone Tests	36
Resolving Batch Test Failure	38
Troubleshooting Tips for Initial Deployment	39
Appendix	40

Scope

This document provides a step-by-step guide for successful deployment of Cisco Prime™ Collaboration 9.5. Cisco Prime Collaboration 9.0 converged the siloed management products, that is, Cisco Prime Operations Manager, Cisco Prime Service Monitor, Cisco Prime Collaboration Manager, and Cisco Prime Provisioning Manager, into one product, and the 9.5 version is the next minor release. This document will detail the deployment considerations for Cisco Prime Collaboration Assurance and Analytics. The Cisco Prime Collaboration Provisioning deployment will be detailed in a separate document. Note that with the 9.5 release onwards, Cisco Prime Collaboration Assurance installation automatically installs the Cisco Prime Collaboration Analytics option module, which can be enabled with a purchased license.

Introduction

Cisco Prime Collaboration 9.5 allows voice and video network operations centers (NOCs) to visualize, monitor, and troubleshoot Cisco TelePresence® and voice and video infrastructure applications. This guide examines the details of all the aspects of deploying Cisco Prime Collaboration Assurance/Analytics 9.5. Cisco Prime Collaboration is a converged application. There are two separate applications, Cisco Prime Collaboration Assurance/Analytics, and Cisco Prime Collaboration Provisioning, which are installed on separate virtual machines (VMs), but you can operate the converged application in a single pane of glass. You can run these applications either as:

- A converged application with single sign-on, which provides a converged user interface with menu items for both Cisco Prime Collaboration Assurance/Analytics and Cisco Prime Collaboration Provisioning (Figure 1), or
- Standalone applications with separate logins. This mode provides a separate user interface for the Assurance/Analytics and Provisioning features (Figures 2 and 3).

Figure 1. Converged Cisco Prime Collaboration Screen

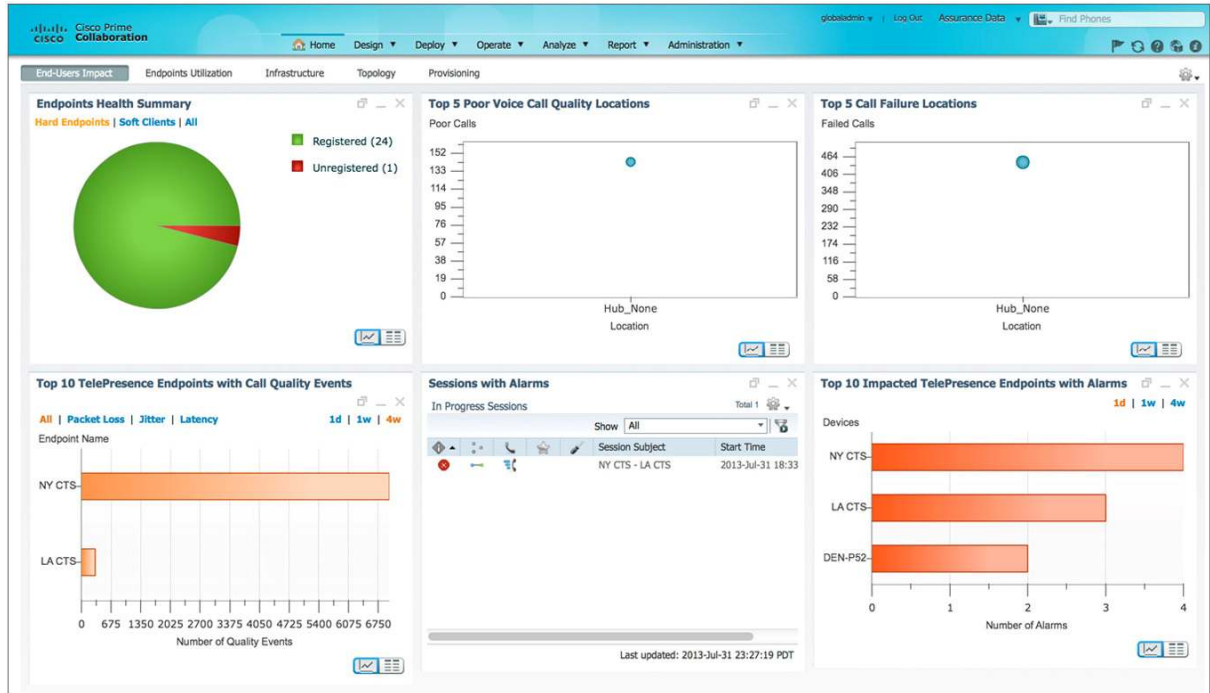


Figure 2. Standalone Cisco Prime Collaboration Assurance Screen without Cisco Prime Collaboration Analytics

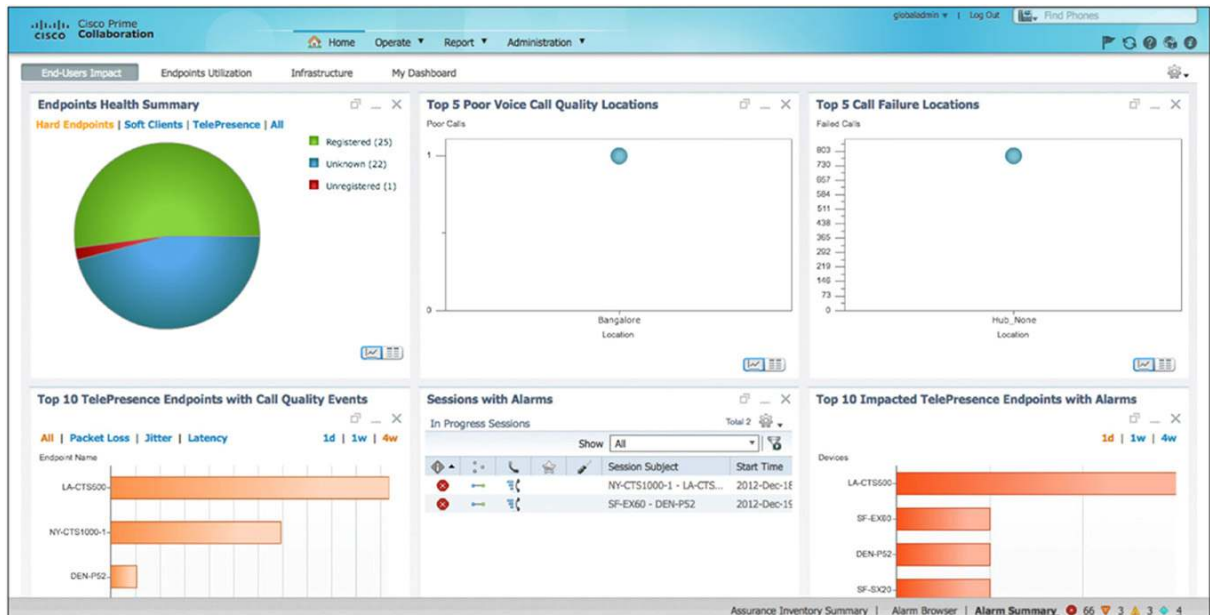
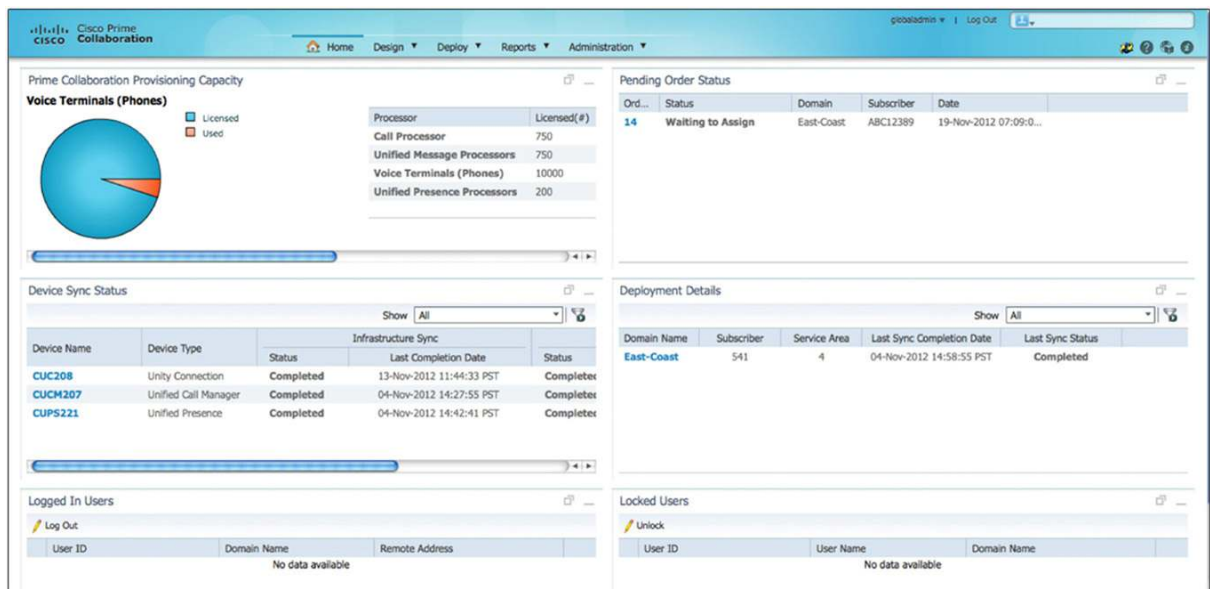


Figure 3. Standalone Cisco Prime Collaboration Provisioning Screen



Cisco Prime Collaboration Provisioning allows administrators to provision users and their unified communication services such as phones, lines, voicemail, and presence using a single user interface. It has a powerful auditing feature that allows you to track all the changes. It also has a self-care feature that allows administrators to empower end users to provision services, such as speed dialing and call forwarding, on their devices and change Cisco® Unified Communications (UC) Manager and voicemail passwords and pins. It also has configuration templates that allow you to automatically configure the Cisco Unified Communications voice infrastructure in a consistent way.

Cisco Prime Collaboration Assurance allows network operators to monitor and troubleshoot their voice and video networks. It provides tools to troubleshoot video sessions and diagnostic tests to proactively find issues in the network before users experience them. It also has comprehensive reporting and notification capabilities.

Cisco Prime Collaboration Assurance continuously monitors the current operational status of different IP communications elements such as Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Unity® systems, Cisco Unity Express, Cisco Unity Connection, Cisco Unified Contact Center, Cisco Unified Contact Center Express, Cisco Unified Presence Server, Cisco Emergency Responder, and Cisco Unified MeetingPlace® Express, as well as Cisco gateways, routers, switches, and IP phones. It also provides diagnostic capabilities for faster trouble isolation and resolution.

Cisco Prime Collaboration Assurance monitors and evaluates the current status of both the IP communications infrastructure and the underlying transport infrastructure in the network. It uses Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), and Windows Management Instrumentation (WMI) to remotely poll data from different devices in your IP communications deployment. Since Cisco Prime Collaboration Assurance does not deploy any agent software on the devices being monitored, it is nondisruptive to your system operations.

In addition, Cisco Prime Collaboration Assurance does the following:

-
- Presents the current operational status of your IP communications deployment and provides visualization using service-level views of the network.
 - Provides quick, at-a-glance real-time status of all the faults in the Unified Communications network.
 - Increases productivity of the network managers and helps enable faster trouble identification and isolation by providing contextual diagnostic tools to facilitate troubleshooting. This is done through:
 - Diagnostic tests, performance, and connectivity details about different elements of the converged IP communications infrastructure.
 - Use of synthetic tests that replicate end-user activity and verify gateway availability as well as other configuration aspects of the Cisco Unified Communications infrastructure. Tests may be run on synthetic phones or real IP phones (both Session Initiation Protocol [SIP]-based and Skinny Client Control Protocol [SCCP]-based phones) deployed in the network.
 - IP service-level agreement (SLA)-based diagnostic tests that can measure the performance of WAN links and measure node-to-node network quality.
 - Information provided in notification messages that contain context-sensitive links to more detailed information about service outages.
 - Use of context-sensitive links to other Cisco Prime tools and Cisco tools for managing IP communications implementations.
 - Discovers and reports on the status of different video-enabled IP endpoints (for both SIP- and SCCP-based phones) in the Cisco Unified Communications system and provides additional contextual information to facilitate the location and identification of the IP phones. Cisco Prime Collaboration Assurance can also track the status of these endpoints.
 - Provides a very powerful set of dynamic phone-testing capabilities that facilitate the use of IP phones (both SIP- and SCCP-based phones) in the Cisco Unified Communications system as test probes to run dial-plan tests, acceptance tests, phone-feature tests, and so on. Such phone-testing capabilities may be used to rapidly troubleshoot issues related to connectivity (signaling/media stream) and voice quality as well as call processing/dial-plan management issues.
 - Provides visibility into key performance metrics of different Cisco Unified Communications elements, such as resource usage (CPU, memory, Media Termination Point [MTP] resources, transcoder resources), call statistics (active calls), trunk statistics (trunk usage, port usage, gateway statistics), and so on, that aid in different tasks such as troubleshooting and capacity planning.
 - Correlates and presents service-quality alerts by using the information. It displays Mean Opinion Scores (MOSs) associated with voice quality between pairs of endpoints (IP phones, Cisco Unity messaging systems, or voice gateways) at specified times in the monitored call segment and other associated details about the voice-quality data.
 - Provides current information about connectivity-related and registration-related outages affecting different IP phones in the network and provides additional contextual information to help enable the location and identification of the IP phones.
 - Facilitates tracking of IP communications devices and IP phone inventory, tracks IP phone status changes, and creates a variety of reports that document the move, add, and change operations on IP phones in the network.
 - Provides real-time notifications using SNMP traps, syslog notifications, and email, thus reporting the status of the network being monitored to a higher-level entity (typically a manager of managers [MoM]).

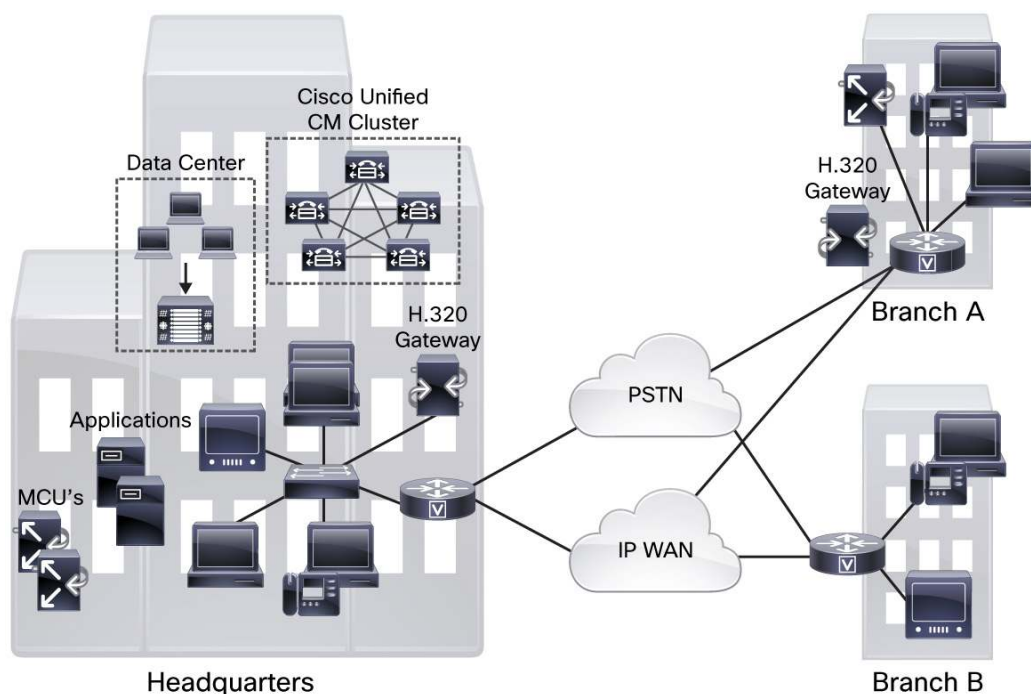
- Provides a single view to visualize and monitor Unified Communications component status, performance, and test results by logical and physical groupings, and provides the status of the key components on a single screen to make diagnosis of problems much quicker than the previous individual-feature navigation approach.
- Provides troubleshooting tools for ongoing video sessions using medianet. You can trace the path of the video call and see the topology of all the devices in between the two video endpoints. If medianet-enabled devices are present, it can also display more detailed impairment information on each device thus helping to troubleshoot the exact point where the session is having an issue.
- Provides utilization reports for all Cisco TelePresence endpoints and sessions.

Cisco Prime Collaboration Analytics helps you identify traffic trends, technology adoption trends, and over- and underutilized resources in your network. You can also track intermittent and recurring network issues and address service quality issues. The data is persisted for a year and helps the operator in trending various statistics over an entire year. The ability to track collaboration deployments, usage trends, and adoption over time closes the loop on a complete planning cycle that measures the effective absorption of collaboration technology into the business.

Small, Medium, Large, and Very Large Enterprises

Small business are organizations with fewer than 1000 phones, medium businesses have fewer than 10,000 phones, and large enterprises are organizations with more than 10,000 phones and up to 100,000 phones (Figure 4). The Cisco Prime Collaboration software is now provided as Open Virtualization Archives (OVAs) specific to each deployment, so there are OVAs for small, medium, large, and very large deployments. These OVAs for each instance of Cisco Prime Collaboration Assurance can manage multisite and multicluster IP communications environments. Cisco Prime Collaboration Assurance provides real-time notifications, using SNMP traps, syslog notifications, and email, that help enable Cisco Prime Collaboration Assurance to report the status of the network being monitored to a higher-level entity (typically a MoM).

Figure 4. Deployment Model for Large Enterprises



Voice and Video Infrastructure

Video infrastructure can be loosely termed as layers of network and applications that are needed to successfully create an end-to-end video Cisco TelePresence session. Figure 5 shows a typical video infrastructure. Now let's consider each of the layers:

- **Network:** The network is the foundation of all the layers. You need a reliable and efficient network for any video calls to go through it.
- **Endpoints:** Endpoints are the video devices such as the personal Cisco TelePresence System EX90, the Cisco TelePresence Movi (Movi) Camera, or maybe the Cisco TelePresence System 1300 Series Server that is used to actually send and receive live video.
- **Call controllers and processors:** Endpoints register themselves at call controllers and processors. These applications (for example, Cisco Unified Communications Manager or Cisco TelePresence Video Communication Server [Cisco VCS]) stipulate how the endpoints should be making the calls and the quality associated with them.
- **Multipoint bridges and switches:** We can think of these bridges and switches as multipoint video switches, which facilitate more than one endpoint to talk to each other in real time.
- **Call scheduling and calendaring:** This application allows the video calls to be scheduled just like Microsoft Outlook meetings. They can be tied to an existing corporate Lightweight Directory Access Protocol (LDAP) or Microsoft Exchange server to make it easier to deploy.

Figure 5. Typical Video Infrastructure

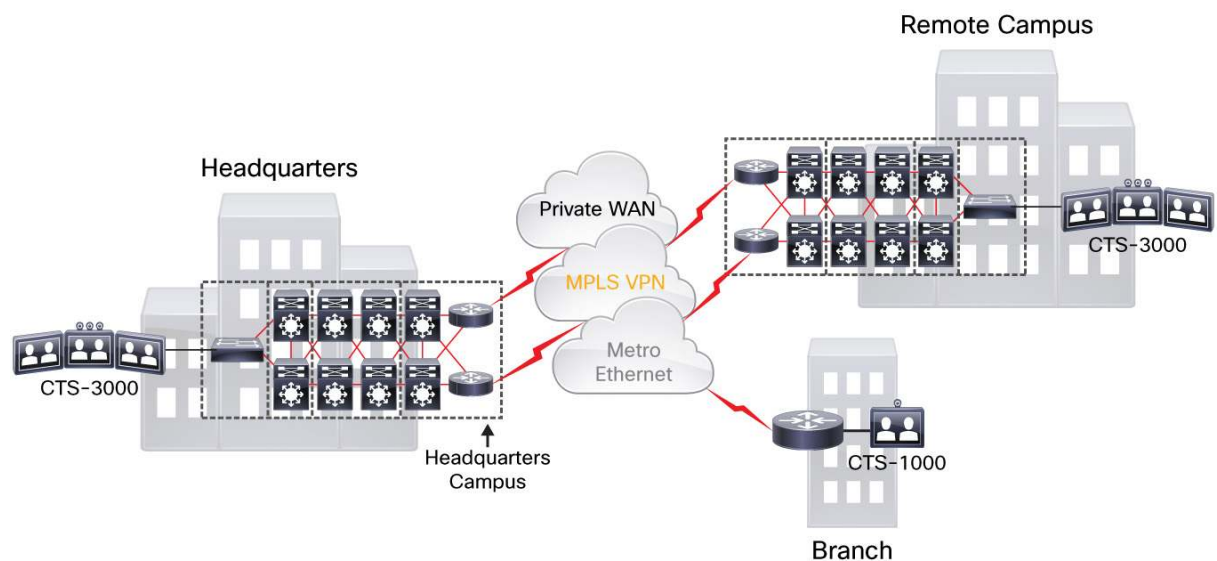
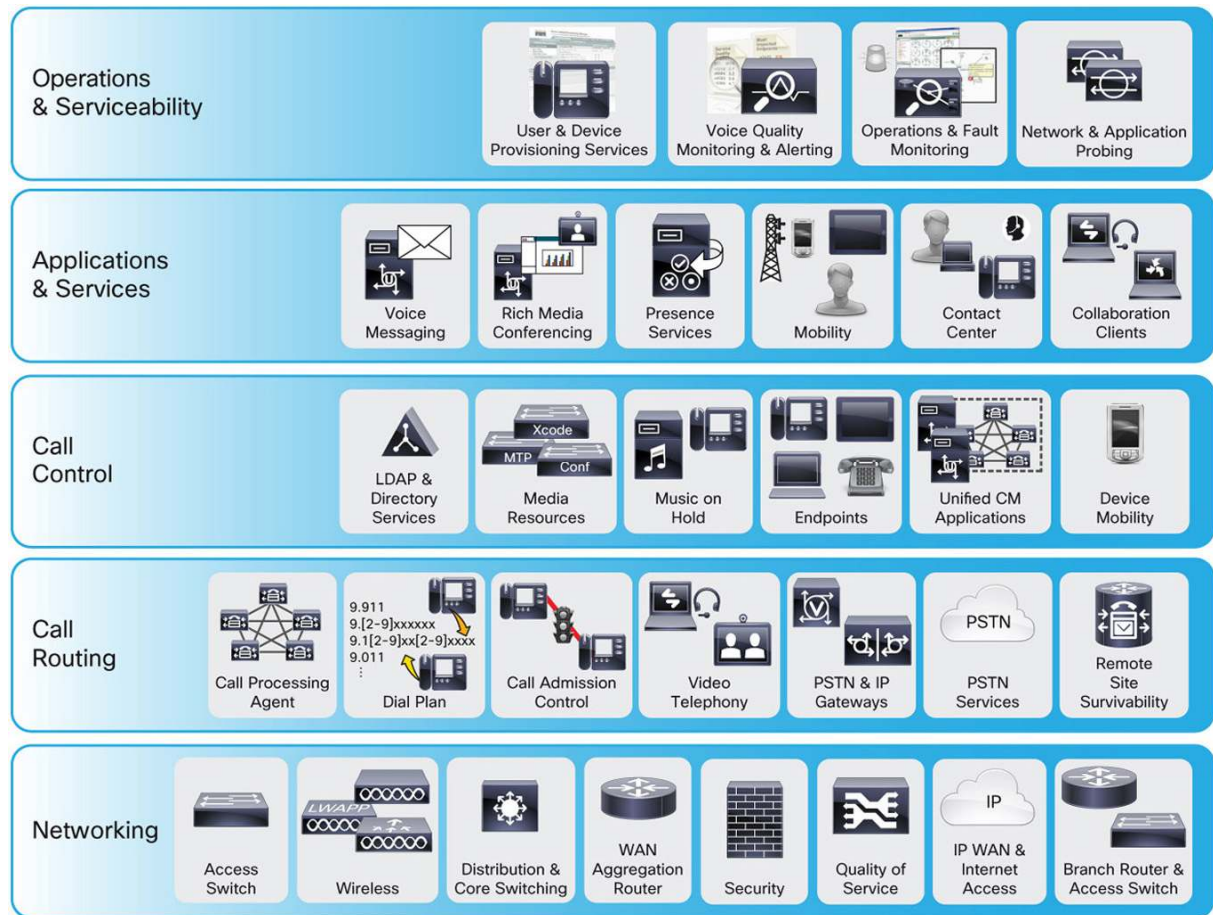


Figure 6 shows the components in the voice infrastructure.

Figure 6. Voice Infrastructure



Installation

The Cisco Prime Collaboration Assurance/Analytics and Cisco Prime Collaboration Provisioning OVA's must be installed on separate virtual machines. For Cisco Prime Collaboration Provisioning, if you have more than 10,000 phones, you need to install the application and database on separate virtual machines. The same Cisco Prime Collaboration Provisioning OVA is used to install both. The options are given at install time to install the application, the database, or both.

Prerequisites

You can install Cisco Prime Collaboration as a VMware Virtual Appliance only (as an OVA) file that you can import into your VMware Virtual Infrastructure (ESXi 4.1/5.0). Cisco Prime Collaboration runs on any VMware certified hardware with ESXi 4.1 or 5.0 installed. Large (more than 10,000 endpoints) or very large (more than 100,000 endpoints) deployments require ESXi 5.0.

Note: Hyperthreading must be disabled in the server (BIOS level) for better performance of Cisco Prime Collaboration. See your hardware documentation for information about disabling hyperthreading.

Server Requirement

Please refer to the Quick Start Guide at

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration/9.5/quick/start/guide/Cisco_Prime_Collaboration_Quick_Start_Guide_9_5.html#wp117957 for the exact VMware reservation requirements.

Client Requirement

Please refer to the Quick Start Guide at

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration/9.5/quick/start/guide/Cisco_Prime_Collaboration_Quick_Start_Guide_9_5.html#wp117078.

Preparing for Installation

You need to download the OVA images for Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Provisioning and install them on separate VMs. If you need only one or the other, then download just the required OVA and deploy that. OVAs are available for each deployment, small, medium, large, and very large. Note that there is no separate OVA for analytics. The Cisco Prime Collaboration Assurance OVA contains the Analytics component, which can be enabled if appropriate optional licensing is applied.

Please refer to the Quick Start Guide at

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration/9.5/quick/start/guide/Cisco_Prime_Collaboration_Quick_Start_Guide_9_5.html for the OVA details.

It is recommended that you know the values beforehand for the following parameters as you are required to specify them at the console prompts while configuring the virtual appliance:

- IP Address: The IP address of the virtual appliance
- IP default netmask: The default subnet mask for the IP address
- IP default gateway: The IP address of the default gateway
- Default DNS domain: The default Domain Name System (DNS) name
- Primary nameserver: The primary name server. You may add the name server. To configure several name servers, enter **y**
- Primary NTP server[time.nist.gov]: The primary Network Time Protocol (NTP) server

To enter a secondary NTP server, enter **y** at the next prompt.

- Timezone: The time zone set for Cisco Prime Collaboration. When you are prompted to enter the system time zone, specify the default time zone - UTC. You can use Secure Shell (SSH) Protocol to change the time zone after you install the Cisco Prime Collaboration Assurance or Cisco Prime Collaboration Provisioning server; the time stamp that is displayed on the UI is the server time. You must use the same time zone for Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Provisioning servers in converged mode. For a list of supported time zones, see "[Supported Timezones for Cisco Prime Collaboration](#)."
- Username: The command-line interface (CLI) admin user name. The user name is admin by default. However, you can specify the user name of your choice.
- Password: CLI admin password. This password is used to log in to the CLI to check the application status and perform backup and restore.
- Root user: Superuser who has all privileges in CLI.

- Root password: Specify a password for the root user.
- globaladmin: Superuser who can access both the Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Provisioning UI.
- globaladmin password: Specify a password for the globaladmin.

With Cisco Prime Collaboration 9.5 Assurance, we now have two different modes of deployment for video endpoint management: Enterprise and Managed Service Provider. Select E for Enterprise deployment and M for Managed Service Provider deployment when prompted. To know more about the differences between MSP mode and Enterprise mode, please refer to the Assurance Guide at http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration/9.5/assurance/guide/intro.pdf.

Checking Port Availability

Make sure the firewall is opened for the required ports to manage the voice and video infrastructure from the Cisco Prime Collaboration server. Refer to http://docwiki.cisco.com/wiki/Required_Ports_for_Prime_Collaboration for the list of ports. This lists the ports required for both the Cisco Prime Collaboration Assurance server and the Cisco Prime Collaboration Provisioning server.

Upgrading Deployments

If you need to upgrade your deployment model to medium, large, or very large, you must first upgrade your hardware resources, such as vRAM, vCPU, and vDisk. Increase the virtual disk size by adding a new vDisk if your vDisk already has four partitions. (Refer to VMware documentation to upgrade the hardware resources).

Log in as the root user. Then run the following script:

```
# /opt/emms/emsam/bin/cpcmtuning.sh
```

From the options displayed, choose the deployment model (excluding option 1) that you wish to upgrade to, and then select Y to proceed with upgrading or N to reselect the deployment model.

Licensing the Product

Please refer to the Quick Start Guide at

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration/9.5/quick/start/guide/Cisco_Prime_Collaboration_Quick_Start_Guide_9_5.html for information about licensing.

Preparing the Network

This part is the most important part in successfully deploying Cisco Prime Collaboration Assurance. You must make sure all the credentials are in place and are correctly entered in the application.

Required Device Protocols and Software Versions

The following link has all the information that you need to enter in Cisco Prime Collaboration Assurance in order to successfully manage the Cisco voice and video infrastructure:

http://docwiki.cisco.com/wiki/Setting_up_Devices_for_Prime_Collaboration_Assurance.

For Cisco Prime Collaboration Provisioning refer to:

http://docwiki.cisco.com/wiki/Supported_Devices_for_Prime_Collaboration_Provisioning.

Verifying Credentials

You can verify the credentials entered in Cisco Prime Collaboration Assurance for the devices being managed.

Cisco Prime Collaboration has a very good utility that allows you to do this verification in real time as the credentials are created. After a new credential profile is created, navigate to Operate > Device Work Center > Manage Credentials. Then select the credential set that contains the device/appliance/server and click Verify (Figure 7).

Figure 7. Credential Profiles

The screenshot shows the 'Discover Devices' page. At the top, there are two tabs: 'Manage Credentials' and 'Device Discovery'. The 'Device Discovery' tab is active. Below the tabs, there are four buttons: 'Add', 'Delete', 'Clone', and 'Verify'. The 'Verify' button is highlighted. Below the buttons is a table with the following data:

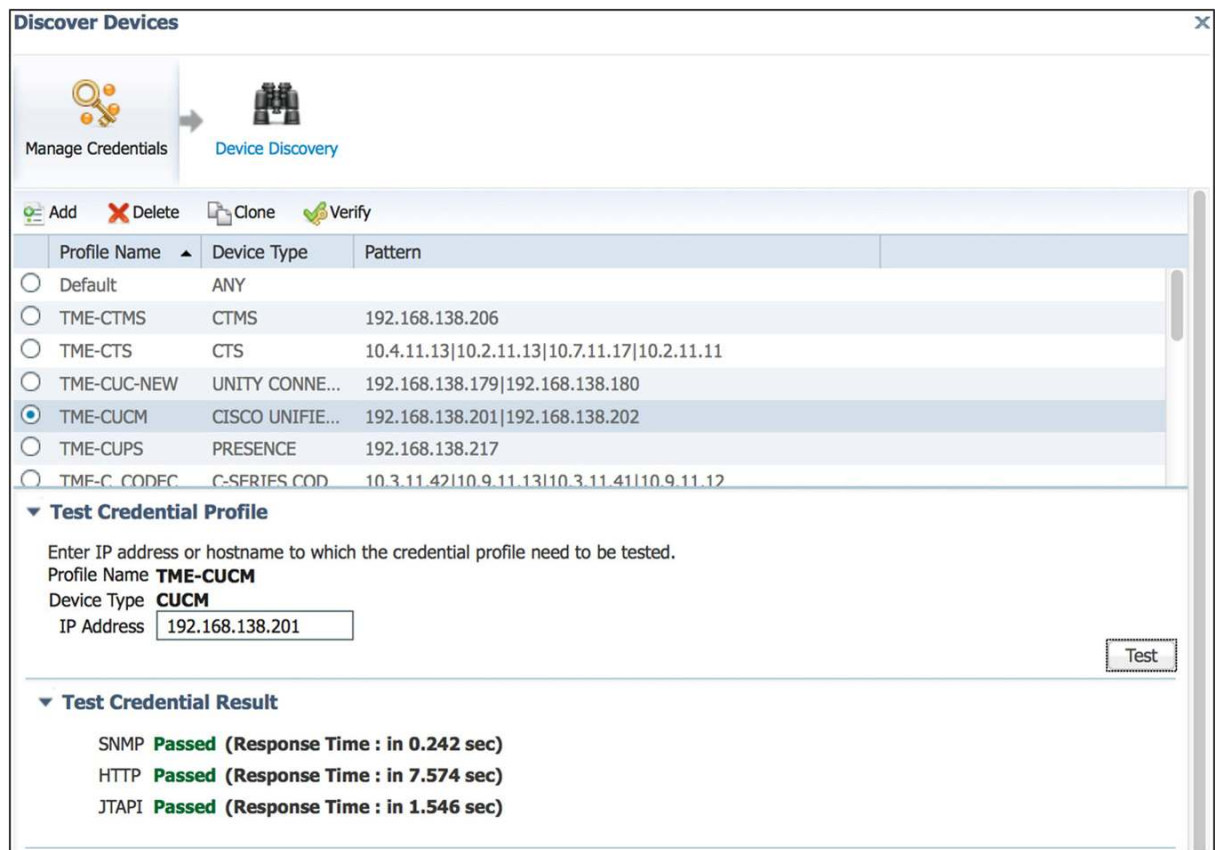
Profile Name	Device Type	Pattern
<input type="radio"/> Default	ANY	
<input type="radio"/> TME-CTMS	CTMS	192.168.138.206
<input checked="" type="radio"/> TME-CTS	CTS	10.4.11.13 10.2.11.13 10.7.11.17 10.2.11.11
<input type="radio"/> TME-CUC-NEW	UNITY CONNE...	192.168.138.179 192.168.138.180
<input type="radio"/> TME-CUCM	CISCO UNIFIE...	192.168.138.201 192.168.138.202
<input type="radio"/> TME-CUPS	PRESENCE	192.168.138.217
<input type="radio"/> TME-C.CODEC	C-SERIES.COD	10.3.11.42 10.9.11.13 10.3.11.41 10.9.11.12

* Indicates required field

Enter one of the IP addresses from the range or one of the IP addresses mentioned in the credential profile that needs to be verified. Click Test. Within 10 to 30 seconds, depending on the type of profile, you should see the results (Figure 8).

Click another profile to get back to editing the profile.

Figure 8. Verifying Credentials



Preparing Call Scheduling and Calendaring for Cisco Prime Collaboration Assurance

Preparing Cisco TelePresence Management Suite

Enable HTTP

The Cisco TelePresence Management Suite is accessed through a web browser (<http://<serveraddress>/TMS>), where <serveraddress> is the IP address or hostname of your server. The default password for the administrator user, admin, is TANDBERG. If you cannot log in to the web GUI, Cisco Prime Collaboration will not be able to log in either. Unless this problem is fixed, Cisco Prime Collaboration will not be able to successfully monitor the Cisco TelePresence Management Suite. Refer to the "Installation and Getting Started Guide" for Cisco TelePresence Management Suite 13.0 for detailed instructions about how to change the admin password.

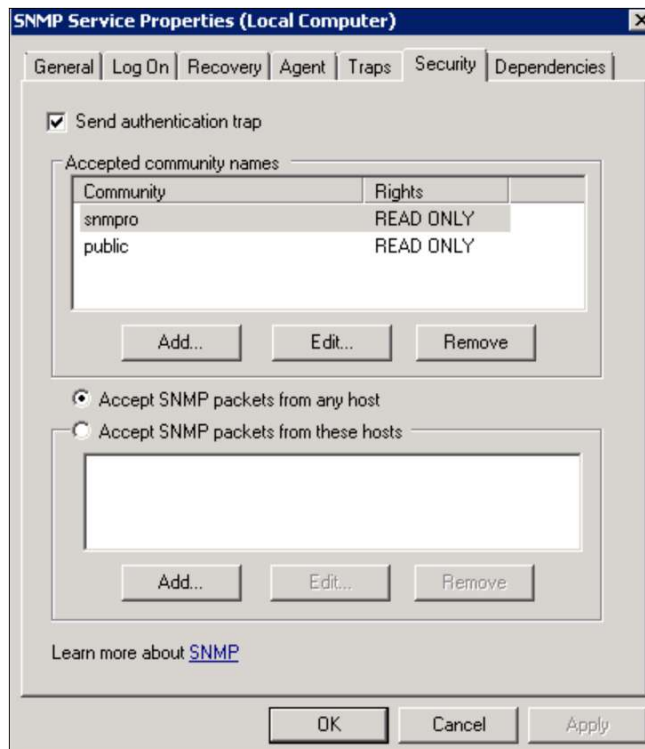
Enable SNMP

By default, "public" and "Public" are enabled as SNMP read only (RO) community strings for Cisco TelePresence Management Suite. This string is what the Cisco TelePresence Management Suite uses to poll other devices. If you need to add or change these strings, you can go to the web GUI and navigate to Administrative Tools > Configuration > Network Settings and then change the SNMP settings.

In addition to the web GUI, SNMP service on the Cisco TelePresence Management Suite server also needs to be enabled. Go to Start on the server console. Then click Run and type in **services.msc**. A service window will pop open on the server console. Look for a service called SNMP Service, right-click that service, and go to Properties.

Click the Security tab and choose Add (Figure 9). Unless you want only specific hosts polling SNMP from Cisco TelePresence Management Suite, you can leave the default setting of “Accept SNMP packets from any host”.

Figure 9. SNMP Service Properties



You can also click the Traps tab next to Security and add the IP address of Cisco Prime Collaboration and a community string. (This address will be used within the SNMP traps).

You can optionally click Agent to specify SNMP contact and location for Cisco TelePresence Management Suite. Cisco Prime Collaboration Assurance will use this information to show where Cisco TelePresence Management Suite is located in the inventory.

Restart the SNMP Service after the changes are made.

Booking API for Cisco TelePresence Management Suite

The Cisco TelePresence Management Suite 3rd Party Booking API is an API that gives developers access to the booking functionality in Cisco TelePresence Management Suite.

To create the Booking API user:

Step 1. From the Cisco TelePresence Management Suite server, go to <http://localhost/tms/external/booking/remotesetup/remotesetupservice.asmx>.

The RemoteSetupService page appears.

Note: You may replace “localhost” in the URL with the IP address of the Cisco TelePresence Management Suite server.

Step 2. Choose GenerateConferenceAPIUser.

Step 3. Enter the values for the following parameters:

- **userNameBase:** The base portion of the username; for example, SI 17233 root emsam_fault 7-22:30:00
- **encPassword:** A base64 encoded password that is used for the newly created user; to encode the password to base64, we recommend that you use the web utility available at <http://www.motobit.com/util/base64-decoder-encoder.asp>.
- **emailAddress:** The user's email address; do not enter a value in this field.
- **sendNotifications:** If you want the user to receive scheduling notifications; you must enter False in this field because Cisco Prime Collaboration Assurance will be polling from Cisco TelePresence Management Suite.

Step 4. Click Invoke.

For more information about the Cisco TelePresence Management Suite, refer to the documents available for Cisco TelePresence Management Suite at <http://www.cisco.com/go/telepresence>.

Preparing Cisco TelePresence Manager

Only HTTP and SNMP access is needed to successfully manage Cisco TelePresence Manager. For the Cisco Prime Collaboration Assurance server to retrieve data from Cisco TelePresence Manager 1.7, you must have a valid Metrics Dashboard (room and endpoint) and Reporting API license in Cisco TelePresence Manager. You can refer to "Getting Started with Cisco TelePresence Reporting API," available at <http://developer.cisco.com/web/tra/start>, for a detailed overview of the Reporting API.

Requirements for the Cisco TelePresence Manager and LDAP and Exchange

On the Cisco TelePresence Manager side:

1. You can either dedicate an HTTP account (user) on Cisco TelePresence Manager for Cisco Prime Collaboration Assurance or use an existing user from LDAP. An LDAP user with permissions for the Livedesk and Reporting API is required to be managed by Cisco Prime Collaboration Assurance. A new user can be created through the Cisco TelePresence Manager CLI only.

```
admin:set account name cpcm-http

Privilege Levels are:
  ordinary - Level 0
  Advanced - Level 1

Please enter the privilege level :1
      Please enter the password :*****
      re-enter to confirm :*****
Account successfully created
admin:█
```

You can use the following command to create a new user: set account name, where name is the name of the user. This command sets up a new account on the operating system. After you enter the username, the system prompts you to enter the privilege level and password for the new account:

2. A proper license is required for the Cisco TelePresence Manager; that is, "Room" (number of endpoints or rooms - count-based) and "Metrics Dashboard and Reporting API." The part number for the Metrics Dashboard and Reporting API feature is LIC-CTS-MAN-RPT.

Now on the LDAP and Exchange side:

3. Create two groups (although one group can be used for both): Live Desk group (have accounts but less privilege) and Reporting API group.
4. Create a dedicated user account to be used for Reporting API in LDAP and Exchange for Cisco Prime Collaboration.
 - a. This user needs to have a mailbox.
 - b. This user must be used as an HTTP user in Cisco Prime Collaboration.

Back on the Cisco TelePresence Manager side:

5. The user group created in step 3 in LDAP and Exchange must have privileges for Reporting API as well as Live Desk in Cisco TelePresence Manager. To set these privileges, from the main menu navigate to Configuration > Access Mgmt > Add Role and add privileges for Live Desk and for Reporting API.

Enable HTTP

Cisco TelePresence Manager can be accessed through a web browser by pointing the browser to `https://<serveraddress>/adminui/loginAction.do`, where <serveraddress> is the IP address or hostname of the Cisco TelePresence Manager.

Enable SNMP

SNMP community strings can be viewed only through the web interface, but they can be configured and enabled only through the CLI with SSH into the Cisco TelePresence Manager. (Refer to the Cisco TelePresence Manager 1.7 CLI reference guide for more details.) Here is the quick guide to the command for enabling SNMP read only, where `snmpro` is the community string: “set snmp user add 2c snmpro r”. The following shows the complete syntax for this command:

```
Syntax:
set snmp user add [options]
version      mandatory    SNMP version as either 3 or 2c
usr_comm     mandatory    SNMP username (v3) or community string (v2c)
access       mandatory    values can be r, w, or rw (r = read, w = write)
level        optional     v3 only; values can be authNoPriv, authPriv,
                           noauthNoPriv (default authNoPriv)
pw           optional     Required for version 3, passphrase for
                           user (8 characters min)
```

For version 3, hash will always be MD5 and encryption will be DES.

```
admin:set snmp user add 2c snmpro r
Successfully added user
admin:█
```

Preparing Multipoint Bridges and Switches for Conferencing

The main products that are normally deployed for conferencing needs are Multipoint Control Units (MCUs) for Cisco VCS-based devices or the Cisco TelePresence Multipoint Switch for Cisco Unified Communications Manager-based video endpoints. This section describes how to configure and prepare each of these conferencing components for manageability.

Preparing MCUs for Cisco Prime Collaboration Assurance

A Cisco TelePresence MCU MSE 8510 cluster consists of a Cisco TelePresence MCU MSE 8050 Supervisor Blade and an MCU MSE 8510 blade. After the basic information is configured, HTTP access is enabled by default.

Enable HTTP

The supervisor web interface can be accessed by pointing the browser to `http://<MCU_Address>`, where `<MCU_Address>` is the IP address or hostname of your server. The default password for the admin user is blank (no password). If you cannot log in to the web GUI, Cisco Prime Collaboration will not be able to log in either. Unless this problem is fixed, Cisco Prime Collaboration will not be able to successfully manage the MCU MSE Supervisor. To log in to the web interface of the MCU MSE 8510 blade:

1. Log in to the supervisor web interface.
2. Go to Hardware > Blades and click the IP address of the MCU MSE 8510 blade.
3. Click Log in, and enter the username "admin" with no password.

Enable SNMP

You can edit SNMP settings by logging in to the Codian MCU web interface. Navigate to Network > SNMP and go to the bottom portion of the page, which has the SNMP read only and read/write strings. Change or edit them as needed, and click Update SNMP Settings to apply the changes.

Preparing Cisco TelePresence Multipoint Switch for Cisco Prime Collaboration

Enable HTTP

A dedicated user with minimum role of diagnostic technician is required for managing the Multipoint Switch within Cisco Prime Collaboration. This user can be configured in the Multipoint Switch web user interface when logged in as admin. An admin user is not required by Cisco Prime Collaboration Assurance to manage the Multipoint Switch.

You can access the Multipoint Switch through a web browser (preferably using Internet Explorer, if possible) by pointing the browser to `https://<ctms_serveraddress>`, where `<ctms_serveraddress>` is the IP address or hostname of the Multipoint Switch.

Enable SNMP

SNMP is enabled by default, and it monitors the Multipoint Switch system status (go to Troubleshoot > System Resources for system status details). You can designate a particular server where SNMP trap messages are gathered and stored. You configure all SNMP settings through the Multipoint Switch CLI commands. Configuration requires username and password authentication.

The following default SNMP settings are also enabled by default:

- SNMPv3 username set to "mrtg": This name is for internal use of the system and should not be deleted.
- SNMPv2c username set to "public": This name is for internal use of the system and should not be deleted.
- No trap receiver is configured. Use Multipoint Switch CLI commands to configure SNMP trap receiver information.

Use SSH in the Multipoint Switch to configure SNMP using the CLI. The CLI commands to configure SNMP read only and read/write are as follows:

```
set snmp user add 2c snmpro r
set snmp user add 2c snmprw rw
```

Note: Replace snmpro and snmprw with your own SNMP read and read/write community strings.

Some of the other commands that might be useful when dealing with SNMP on the Multipoint Switch are as follows:

- `utils service snmp restart`: This command restarts the SNMP daemon on the Multipoint Switch appliance.
- `utils service snmp status`: This command displays the current SNMP daemon state.
- `show process search snmp`: This command shows more information about the SNMP daemon in general.

Preparing the Cisco TelePresence Server (Appliance and Blade)

Enable HTTP

A user with API access should be sufficient for Cisco Prime Collaboration to manage the Cisco TelePresence Server. This user can be configured by logging in to the Cisco TelePresence Server web user interface as admin.

You can access the Cisco TelePresence Server web interface by pointing the browser to `http://<TS_Address>`, where `<TS_Address>` is the IP address or hostname of your Cisco TelePresence Server.

Enable SNMP

SNMP is not required for Cisco TelePresence Server.

Preparing Call Controllers and Processors for Cisco Prime Collaboration Assurance

Preparing Cisco Unified Communications Manager

Enable HTTP

It is not necessary to create a new user if you want to allow Cisco Prime Collaboration to use admin credentials to log in. If that is not the case, and you only want to allow Cisco Prime Collaboration to use just the right credentials to log in to Cisco Unified Communications Manager, you must create a new HTTP user group and a corresponding user that Cisco Prime Collaboration can use to communicate. The steps for creating such a user follow:

Create a user group with sufficient privileges. Log in to the Cisco Unified Communications Manager administration web interface using the administrator role. Go to **User Management > User Groups** and create a new group with a suitable name, “CPCM_HTTP_Users” in this case. A new row will now be added to the existing default groups. This group will be the only group with a check box indicating that it is a user-defined group.

Figure 10. User Group Configuration

The screenshot shows the 'User Group Configuration' web interface. At the top, there is a 'Save' button. Below it is a 'Status' section with an information icon and the text 'Status: Ready'. The 'User Group Information' section contains a text field for 'Name*' with the value 'CPCM_HTTP_Users'. The 'Role Assignment' section features a list box with three roles: 'Standard AXL API Access', 'Standard CCM Admin Users', and 'Standard SERVICEABILITY Administration'. To the right of the list box are two buttons: 'Assign Role to Group' and 'Delete Role Assignment'. At the bottom left, there is another 'Save' button.

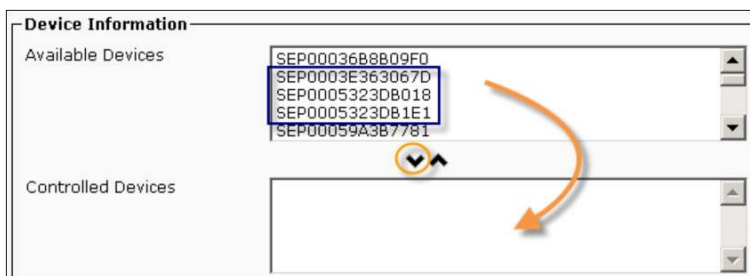
Step 5. Click the ⓘ (Roles) icon. A new window will open. Click the Assign Role to Group button and select the following roles:

- Standard AXL API Access
- Standard CCM Admin Users
- Standard SERVICEABILITY Administration

You should get a screen that looks something like Figure 10. Now click the Save button to save the configuration.

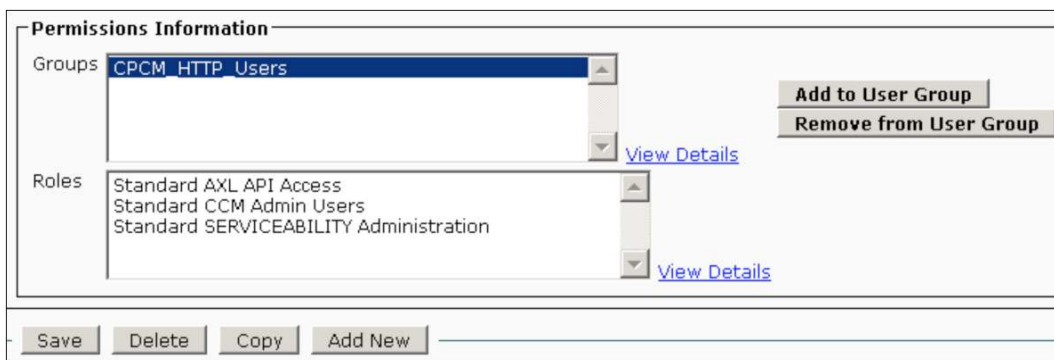
Step 6. From the main menu, navigate to User Management > Application Users > Create a new user. Call it "ccpm-http", for example. Give a suitable password on the Application User Configuration page. Now from the Available Devices text area, you can either select specific devices, or if you want to allow Cisco Prime Collaboration to monitor all devices (recommended), click the first device, scroll down, hold the Shift key, and select the end device. Using the middle down arrow, move those devices to the controlled devices as shown in Figure 11.

Figure 11. Device Information



Step 7. Scroll down to the Permissions Information section. Click the Add to User Group button and select the group that was created in step 1. In our case, we will select "CPCM_HTTP_Users". Click Save. The page should refresh and automatically fill in the appropriate privileges as shown in Figure 12.

Figure 12. Permissions Information



Enable SNMP

SNMP is not enabled in Cisco Unified Communications Manager by default. You must enable it using the following steps:

Step 1. Log in to the Cisco Unified Serviceability view by choosing this option in the top-right pull-down menu of the Cisco Unified Communications Manager web GUI.

Step 2. From the main menu in the Cisco Unified Serviceability view, navigate to SNMP > v1/v2c > community string. Then select a server and click Find (Figure 13).

Figure 13. Search Options

Step 3. If the community string is already defined, you will see the result with the link on the community string as shown in Figure 14.

Figure 14. Search Results

Search Results		
<input type="checkbox"/>	Community String Name	Access Privileges
<input type="checkbox"/>	snmppro	ReadOnly

Step 4. If there are no results, you need to add a new string by clicking the Add New button toward the bottom of the screen. Fill in the necessary SNMP-related information as shown in Figure 15 and save the configurations.

Figure 15. SNMP-Related Information

Enable JTAPI

Java Telephony API (JTAPI) is used to retrieve the session status information from the device. You must create a JTAPI user in the call processor with the required permission to receive JTAPI events on endpoints.

Cisco Prime Collaboration manages multiple call-processor clusters. It monitors both intra- and intercluster calls. It does not monitor sessions among clusters. You must ensure that the cluster IDs are unique. You must create this user on the cluster publisher to provide clusterwide information. The following steps will help ensure that you can create a new JTAPI user to help Cisco Prime Collaboration get all the needed information.

Step 1. Create a user group with sufficient privileges. Log in to the Cisco Unified Communications Manager's administration web interface. Go to User Management > User Groups > Create a New Group. Give the new group a suitable name, "CPCM_JTAPI_Users" in this case. A new row will be now added to the existing default groups. This group will be the only group with a check box, indicating that it is a user-defined group.

Step 2. Click the ⓘ (Roles) icon. A new window will open. Click the Assign Role to Group button and select the following roles:

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled

You should get a screen that looks something like Figure 16.

Figure 16. User Group Information

User Group Information

Name * CPCM_JTAPI_Users

Role Assignment

Role

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled

Assign Role to Group

Delete Role Assignment

Now click the Save button to save the configuration.

Step 3. From the main menu, navigate to User Management > Application Users > Create a New User.

Call the new user "cpcm-jtapi", for example. Enter a suitable password on the Application User Configuration page. Now from the Available Devices text area, you can either select a few devices, or if you want to allow Cisco Prime Collaboration to monitor all devices (recommended), click the first device, scroll down, hold the Shift key, and select the end device. Using the middle down arrow, move those devices to the controlled devices as shown in Figure 17.

Figure 17. Device Information

Device Information

Available Devices

- SEP00036B8B09F0
- SEP0003E363067D
- SEP0005323DB018
- SEP0005323DB1E1
- SEP00059A3B7781

Controlled Devices

Step 4. Scroll down to the Permissions Information section. Click the Add to User Group button, and select the group that was created in step 1. In our case, we will select “CPCM_JTAPI_Users”. Click Save. The page should refresh and automatically fill in the appropriate privileges as shown in Figure 18.

Figure 18. Permissions Information

The screenshot displays the 'Permissions Information' section of a web application. It features two main sections: 'Groups' and 'Roles'. The 'Groups' section has a dropdown menu with 'CPCM_JTAPI_Users' selected. To the right of this section are two buttons: 'Add to User Group' and 'Remove from User Group'. The 'Roles' section lists two roles: 'Standard CTI Allow Call Monitoring' and 'Standard CTI Enabled'. Each role has a 'View Details' link to its right. At the bottom of the interface, there is a row of four buttons: 'Save', 'Delete', 'Copy', and 'Add New'.

Device Profile Tips for Cisco Unified Communications Manager

Following are some tips to make sure video endpoints are successfully registered to the Cisco Unified Communications Manager:

- Bandwidth must be enough for the call in the default profile or custom profile to handle the desired video call. Lack of bandwidth can even prevent video calls from being established. Also make sure the device pool is mapped correctly to the one with appropriate bandwidth. You can access the device pool from Cisco Unified Communications Manager Administration: System > Device Pool. Click the region in which you have an interest from the list.
- In order to integrate the Multipoint Switch under Cisco Unified Communications Manager, please refer to the “Configuring Cisco Unified Communications Manager for Cisco TelePresence Management Suite” section under Administrator Guide for Cisco Unified Communications Manager at http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_7/administration/guide/cucm.html.
- If the passwords are expired on the Cisco TelePresence Server devices, it will not allow SSH access, and you will have problems trying to get information using the Cisco Prime Collaboration CLI. Configure the Cisco Unified Communications Manager device profile to help ensure that passwords never expire, especially for secure deployments.
- If you are using the same device profiles, make sure the correct SNMP string is defined in the original one. Cisco TelePresence Server devices will use this string when they boot up.

Configuring Syslog on Cisco Unified Communications Manager

Cisco Prime Collaboration uses syslogs from Cisco Unified Communications Manager to monitor the status of the phones and other endpoints such as gateways. It will monitor whether the phones or gateways are registered or unregistered based on the syslogs it gets from Cisco Unified Communications Manager on an ongoing basis. Hence you need to set up Cisco Unified Communications Manager to send syslogs to the Cisco Prime Collaboration server.

To configure syslog receiver on Cisco Unified Communications Manager:

Step 1. In Cisco Unified Communications Manager, select **Cisco Unified CM Administration** from the Navigation drop-down menu in the top-right corner of the device's home screen.

Step 2. Select **System > Enterprise Parameters**.

Step 3. Go to the Cisco Syslog Agent section and update the following required fields:


- **Remote Syslog Server Name** with the IP address of Cisco Prime Collaboration server
- Select **Informational** from the drop-down menu for **Syslog Severity For Remote Syslog Messages**

Step 4. Select **Cisco Unified Serviceability** from the Navigation drop-down menu in the top-right corner of the device's home screen.

Step 5. Select **Alarm > Alarm Configuration**.

Step 6. Select the correct alarm configuration elements (Server, Service Group, and Service) for your particular machine and then click **Go**. Enter the Cisco Prime Collaboration server IP address or DNS name in the server textbox. Select the service group and service options based on the information in Figure 19.

Figure 19. Service Group and Service Options

- 
- Service Group > CM Services > Service > Cisco CallManager
 - Service Group > CDR Service > Cisco CDR Agent and Cisco CDR Repository Manager
 - Service Group > Database and Admin Services > Cisco Database Layer Monitoring
 - Service Group > Performance and Monitoring Services > Cisco AMC Service
 - Service Group > Backup and Restore > Cisco DRF Client and Cisco DRF Master
 - Service Group > Remote Syslogs

Step 7. Select the **Enable Alarm** check box and select the proper Alarm Event Level.

See the Alarm Configuration Settings in **Cisco Unified Serviceability Administration Guide for Cisco Unified Communications Manager** on Cisco.com.

For example, for Local Syslogs, set the alarm event level to **Error** (Figure 20).

Step 8. Enter any necessary information based on your Unified Communications Manager. For device cluster discovery or remote syslog notification, set the alarm event level to **Informational**.

Step 9. Check **Apply to all nodes**.

Figure 20. Cisco Unified Communications Manager Serviceability Page

The screenshot shows the Cisco Unified Serviceability web interface. The top navigation bar includes 'Navigation', 'Cisco Unified Serviceability', and a 'Go' button. Below the navigation bar, there are tabs for 'Alarm', 'Trace', 'Tools', 'Snmp', and 'Help'. The main section is titled 'Alarm Configuration' and contains several configuration panels. The first panel, 'Select Server, Service Group and Service', has dropdown menus for 'Server*' (192.168.138.201), 'Service Group*' (CM Services), and 'Service*' (Cisco CallManager (Active)), each with a 'Go' button. Below this is a checkbox for 'Apply to All Nodes'. The second panel, 'Local Syslogs', has a checked 'Enable Alarm' checkbox and an 'Alarm Event Level' dropdown set to 'Error'. The third panel, 'Remote Syslogs', has a checked 'Enable Alarm' checkbox, an 'Alarm Event Level' dropdown set to 'Informational', and a 'Server Name*' field with the value '192.168.138.22'. Below this is a checkbox for 'Exclude End Point Alarms'. The fourth panel, 'SDI Trace', has a checked 'Enable Alarm' checkbox and an 'Alarm Event Level' dropdown set to 'Error'. The fifth panel, 'SDL Trace', has a checked 'Enable Alarm' checkbox and an 'Alarm Event Level' dropdown set to 'Error'. At the bottom of the page are 'Save' and 'Set to Default' buttons.

Configure Cisco Unified Communications Manager to Send Call Records to Cisco Prime Collaboration

Cisco Prime Collaboration uses call detail records (CDRs) and call management records (CMRs) from Cisco Unified Communications Manager to provide detailed CDR and voice quality reports including MOS and impairment details. It also uses CDRs to calculate trunk and route group utilization.

To Configure Cisco Unified Communications Manager to send call records to the Cisco Prime Collaboration server follow these steps:

Step 1. On the Unified Communications Manager, select **Administration**.

Step 2. Go to the Service Parameters Configuration page by selecting **System > Service Parameters**.

Step 3. Set parameters for:

- CDR Enabled Flag by scrolling down to **System** and selecting **True**.
- Call Diagnostics Enabled by scrolling down to **Cluster wide Parameters** (Device - General) and selecting **Set to Enable Only When CDR Enabled Flag Is True**.

Step 4. To add Cisco Prime Collaboration Assurance as a billing server in Cisco Unified Communications Manager:

a. Select **Tools > CDR Management**.

b. Scroll down to Billing Applications Server Parameters and click **Add New**.

c. Enter the following

- Host Name/IP Address: IP address of the system where Cisco Prime Collaboration is installed.
- User Name: Enter **smuser**
- Password: Default password is **smuser**

d. Select the SFTP Protocol.

e. Directory path: Enter **/home/smuser/**[Note the/at the end]

f. Select the **Resend on failure** check box.

Step 5. Click **Add**.

Cluster ID of a Cisco Unified Communications Manager Cluster

Cisco Prime Collaboration relies on the cluster ID of the Cisco Unified Communications Manager cluster to uniquely identify and manage the Cisco Unified Communications Manager deployment. Therefore, if two Cisco Unified Communications Manager deployments belonging to different clusters have the same cluster ID then Cisco Prime Collaboration Assurance cannot manage them as two distinct clusters. Cisco Unified Communications Manager has a default cluster name of StandAloneCluster. If you are managing multiple Cisco Unified Communications Manager deployments belonging to different clusters, you will need to change the cluster ID of these Cisco Unified Communications Managers so that they have unique names.

To change the cluster ID of a Cisco Unified Communications Manager, do the following:

Step 1. Open the Cisco Unified Communications Manager Administration page.

Step 2. From the menu, select **System**, and choose **Enterprise Parameters**.

a. The **Enterprise Configuration** page is displayed.

Step 3. In the **Cluster ID** field, enter a new cluster ID.

b. The default is **StandAloneCluster**. This should be changed so that it is unique for every cluster.

Step 4. Click **Update**.

Step 5. You will need to restart the Cisco Unified Communications Manager service for these changes to take effect. Restarting these Cisco Unified Communications Manager services causes a service disruption. To minimize disruption, be sure to schedule this task for a time when system maintenance is being done.

Preparing Cisco TelePresence Video Communication Server

Cisco TelePresence VCS serves as a call-control appliance for the Cisco TelePresence C Series, E Series, and other similar video endpoints.

Enable HTTP

You can access Cisco TelePresence VCS through a web browser, http://<vcs_serveraddress>, where <vcs_serveraddress> is the IP address or hostname of your VCS appliance. The default password for the administrator user admin is TANDBERG. If you cannot log in to the web GUI, Cisco Prime Collaboration will not be able to log in either. Unless this problem is fixed, Cisco Prime Collaboration will not be able to successfully manage the VCS. If the password is left blank, Cisco Prime Collaboration will not be able to manage it either; it is not recommended to leave the password blank.

Enable SNMP

You can easily turn on SNMP from the Cisco VCS web GUI. Navigate to System > SNMP and enter all the SNMP information. Figure 21 is a sample screen shot showing how SNMPv2 is configured.

Figure 21. Sample Screen Shot Showing SNMP Configuration

The screenshot shows the Cisco VCS web GUI with the 'System' tab selected. Under the 'System' tab, the 'SNMP' sub-tab is active. The 'Configuration' section contains the following fields:

- SNMP mode: v2c (dropdown menu)
- Community name: snmpro (text input)
- System contact: Tejas (text input)
- Location: SJC-BLDGO-1 (text input)

Each field has an information icon (i) to its right. A 'Save' button is located at the bottom left of the configuration area.

Preparing Video Endpoints

Cisco Prime Collaboration can manage various video endpoints, as shown in Table 1.

Table 1. Cisco Prime Collaboration Endpoint Management

Endpoint Type	Supported Endpoint Models
Immersive endpoint systems	Cisco TelePresence System 3010, 3210, 500, 1300, and 1100
Multipurpose endpoints	Cisco TelePresence System Profile 65-inch Dual, Profile 65-inch, Profile 52-inch Dual, Profile 52-inch, and Profile 42-inch
Personal endpoints	Cisco TelePresence System EX90 and EX60
Solutions platform	Cisco TelePresence System Quick Set C20, Quick Set C40, Quick Set C60, and Quick Set C90 Series

Generally all three types of access are desirable for all endpoints: SNMP, HTTP, and CLI.

Cisco TelePresence Server Video Endpoints

Enable HTTP

You can access Cisco TelePresence Server video endpoints through a web browser (preferably using Internet Explorer, if possible) by pointing the browser to <https://<serveraddress>>, where <serveraddress> is the IP address or hostname of the Cisco TelePresence Server Video Endpoint.

Enable SNMP

SNMP for Cisco TelePresence Server devices is configured using Cisco Unified Communications Manager phone configuration. In order to change the SNMP community string, go to Cisco Unified Communications Manager Administration. Go to Device > Phone > Search for your Cisco TelePresence Server Endpoints and click the Device Name link to go to the phone configuration page. Edit the section as shown in Figure 22 and then click Save and Apply Config.

Figure 22. SNMP Configuration Parameters

SNMP Configuration Parameters	
Enable SNMP*	Enabled (v2c) ▼
SNMP(v3) Security Level*	(v3) Authentication, No Privacy ▼
SNMP(v3) Auth. Algorithm*	MD5 ▼
SNMP(v3) Auth. Password*
SNMP(v3) Privacy Algorithm*	DES ▼
SNMP(v3) Privacy Password*
SNMP System Location*	Location
SNMP System Contact*	Contact
SNMP(v2c) Community Read Only*	snmpro
SNMP(v2c) Community Read Write*	snmprw

Enable CLI Access

SSH access to the Cisco TelePresence Server devices is also controlled through Cisco Unified Communications Manager phone configuration. Just above the SNMP section is a section “Secure Shell Information” (Figure 23).

Figure 23. Secure Shell Information

Secure Shell Information	
SSH admin User*	admin
SSH admin Password*
SSH admin Life*	0
SSH helpdesk User*	helpdesk
SSH helpdesk Password*
SSH helpdesk Life*	0

Note that if the SSH admin Life and SSH helpdesk Life fields are left at 0, the password never expires (recommended for lab testing scenarios). If this value is not 0, it is up to the administrator to make sure that passwords are changed before the specified interval to ensure that anyone or any application can perform SSH in the device, including Cisco Prime Collaboration.

Cisco TelePresence C and EX Series Video Endpoints

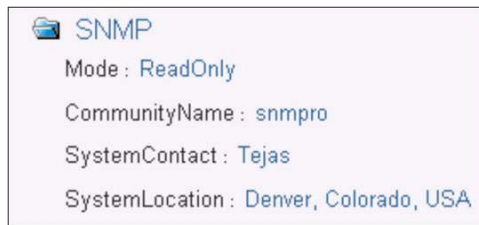
Enable HTTP

By default, HTTP is enabled for Cisco TelePresence endpoints. Simply point the web browser to `http://<ip_address>`, where `<ip_address>` is the IP address or hostname of the video endpoint. The default password for the administrator user admin is “ ” (blank). Cisco Prime Collaboration cannot manage video endpoints with blank passwords; in addition leaving the password blank is not recommended for security reasons.

Enable SNMP

To enable SNMP access for Cisco Prime Collaboration from the web interface, go to Configuration > Adv Configuration > Network Services > SNMP and click the value itself to edit it (Figure 24).

Figure 24. Enable SNMP



It is also recommended to put a descriptive SystemUnit Name by navigating to Configuration > Adv Configuration > SystemUnit > Name and clicking the value itself to edit it (Figure 25).

Figure 25. Entering SystemUnit Name



Enable CLI Access

SSH should be enabled by default on TC 4.0 releases. Giving the admin user access to Cisco Prime Collaboration is sufficient in most cases; just make sure that the admin password is set and not left blank, because that is the default. If you want to troubleshoot video sessions from Cisco TelePresence devices using Cisco Prime Collaboration, admin user access is necessary. Some of the commands needed to run the traceroutes are available only when the user is logged in as root.

Preparing Network Devices

Cisco Prime Collaboration uses Cisco solutions for optimizing medianets that are instrumented within medianet-capable devices. Table 2 is a snapshot of medianet-capable devices at the time of writing of this document.

Table 2. Medianet-Capable Devices

Feature	Routers	Switches	Cisco IOS® Software Release Supported
Mediatrace 1.0	Cisco 1800, 2800, 2900, 3800, 3900 Integrated Services Routers	Cisco Catalyst® 3560E, Catalyst 3560X, Catalyst 3750, Catalyst 3750-Metro (only 12.2SE), Catalyst 3750E, and Catalyst 3750X	12.2SE 15.0SE 15.1T 15.1M
IP service-level agreement (SLA) video operation	Routers will be supported soon. Please check the feature navigator as mentioned below	Cisco Catalyst 3560E, Catalyst 3560X, Catalyst 3750, Catalyst 3750E, and Catalyst 3750X	12.2SE 15.0SE

For the latest platform and Cisco IOS Software mapping, please visit <http://www.cisco.com/go/fn>. Browse by feature and select either “MediaTrace 1.0” or “IP SLAs Video Operation” to see an updated list of device support.

Nonmedianet Routers and Switches

If video endpoints are connected with either third-party devices or devices that do not have medianet capabilities, SNMP read-only access should suffice.

Medianet-Capable Routers and Switches

If video endpoints are connected to [medianet](#)-capable Cisco devices, much more diagnostic information can be polled out from these devices by using medianet instrumentation within the Cisco devices. More information about the hardware, software, and license matrix is available at http://www.cisco.com/en/US/prod/collateral/routers/ps10536/data_sheet_c78-612429.html.

After a device is made medianet-capable (that is, the appropriate hardware, software, and license are configured), you can use the following configuration to enable medianet for Cisco Prime Collaboration 9.5. (Note: Items in bold are variables for which you need to substitute your values).

```
!  
username username priv 15 secret username_enable_password  
!  
ip http server  
ip http authentication local  
no ip http secure-server  
ip http timeout-policy idle 60 life 86400 requests 10000  
!  
wsma agent exec profile wsma_listener_http  
wsma agent config profile wsma_listener_http  
!  
wsma profile listener wsma_listener_http  
transport http  
!  
wsma profile listener wsma_listener_ssh  
transport ssh  
!  
mediatrace responder
```

```
mediatrace initiator source-ip source_interface_ip
!
```

If you want the performance monitor feature within [medianet](#), you need to perform additional configuration on the interfaces where you want deeper visibility. Following is a generic service policy for performance monitoring. Refer to [Configuring Performance Monitoring](#) to fine-tune the policy. Configure the interface policy on the ingress or egress interface as desired (GigabitEthernet 0/0 and GigabitEthernet 0/1 are just used as examples).

```
!
interface GigabitEthernet 0/1
!
service-policy type performance-monitor inline input
  flow monitor inline
  record default-rtp
!
!
interface GigabitEthernet 0/0
!
service-policy type performance-monitor inline output
  flow monitor inline
  record default-rtp
!
```

[IP SLA](#) is another instrumentation feature within Cisco IOS Software. Cisco IOS Software IP SLAs help enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video. The latest Cisco Prime Collaboration addition to IP SLA is called IP SLA Video Operation (IP SLA VO). With IP SLA VO, you can now generate synthetic video traffic without the video endpoints and see if there are any discrepancies in the network ahead of time. For Cisco Prime Collaboration Assurance to set up the synthetic traffic from within the application, navigate to Monitoring > Proactive Monitoring. Choose the qualified devices and other settings from the pull-down menus and click Start.

To check for the latest device support for IP SLA VO, please visit [Cisco Feature Navigator](#) and click Search by Feature, and then search for IP SLA Video Operation, and you should see the latest device support for this feature.

In order for Cisco Prime Collaboration Assurance to use IP SLA VO functions, you need to configure only the following line on the devices that support IP SLA VO:

```
!
ip sla responder
!
```

Initial Configuration

Discovering the Network

Cisco Prime Collaboration has a few options for discovering your network: logical discovery, ping discovery, and Cisco Discovery Protocol-based discovery.

Logical Discovery

This can be done using the Cisco Unified Communications Manager publisher, Cisco TelePresence Management Suite, Cisco TelePresence Manager, or VCS IP as the seed device.

Cisco voice and video infrastructure is discovered using the above devices as the seed device. All of the voice and video infrastructure devices including video endpoints are automatically mapped to the appropriate credential profile and managed automatically if the credentials are successful. It is strongly recommended to test the credential profile against at least one IP address in each of the credential profiles. After all the credentials are known to be entered correctly, only then proceed to do the discovery.

Discovery Using Cisco TelePresence Manager or Cisco TelePresence Management Suite

Navigate to Operate > Device Work Center > Discover Devices and enter an easy-to-find job name; most importantly, enter the IP address of Cisco TelePresence Managers or Cisco TelePresence Management Suite. Click Run Now at the bottom of the Discovery Setup window (Figure 26).

Figure 26. Discovery Setup

Discover Devices

Manage Credentials → Device Discovery

1 Ensure creating Cluster information using "Manage CTS-MAN/TMS Cluster" UI before discovering CTS-MAN/TMS cluster. * Indicates required field

Job Name: Discovery 2013-Aug-05 15:00:22 PDT

☒ Check Device Accessibility

Discovery Methods: Logical Discovery (use UCM Publisher IP, CTS-MAN IP, TMS IP and VCS IP as seed device)

*IP Address: Logical Discovery (use UCM Publisher IP, CTS-MAN IP, TMS IP and VCS IP as seed device)
Cisco Discovery Protocol
Ping Sweep

Filters

Advanced Filters

Schedule

Start Time: ☐ Date: 2013/08/05 03:00 PM (yyyy/MM/dd hh:mm AM/PM)

Recurrence: ☒ None ☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly

Settings

End Time: ☒ No end date/time ☐ End at: 2013/08/05 03:00 PM (yyyy/MM/dd hh:mm AM/PM)

Back Schedule Run Now

As mentioned previously, if Cisco TelePresence Manager or Cisco TelePresence Management Suite is not deployed, you also can initiate discovery using Cisco Unified Communications Manager or Cisco TelePresence VCS as seed devices. When the discovery is running, you can check its status by going to the Discovery Jobs tab

in the Device Work Center. The first job is always the latest job. The bottom pane of the page shows details of the job that are selected in the top pane of the page.

What About Network Devices?

The only things you need to configure are the valid credential profiles for routers and switches. Cisco Prime Collaboration takes care of the rest. Networking devices are discovered in real time when a troubleshooting session is initiated from session monitoring of a video call. For the Cisco TelePresence Server endpoints, only during discovery, the first-hop switch and router for every endpoint will be discovered. All the other devices in the path are learned automatically, and information is fetched on an impromptu basis. The device is then added to the inventory automatically at that point. If for some reason you need to manually add a device for troubleshooting purposes, you can add routers or switches in the Operate > Device Work Center > Discovery Devices page. You can choose “None” as the option for Discovery methods and then click Run Now.

Diagnostic Tests

Synthetic Tests

Synthetic testing is a mechanism by which Cisco Prime Collaboration Assurance emulates a phone. For example, Cisco Prime Collaboration Assurance makes phone calls, logs into conferences, leaves voice mails, makes emergency calls, and downloads TFTP files.

Note: MAC addresses for synthetic phones must be between 00059a3b7700 and 00059a3b8aff.

When a synthetic test is unsuccessful, it generates one of the following events:

- SyntheticTestFailed: Individual test failed.
- TooManyFailedSyntheticTests: Out of a sample of four tests, the actual percentage of tests that failed exceeds the threshold value.
- MWIOnTimeExceeded: Number of seconds in which the Cisco Unity message waiting indicator (MWI) light appears exceeds the value of the MWI on-time threshold.
- SyntheticTestsNotRun: Tests were not run for more than 10 minutes on the Cisco Prime Collaboration Assurance server (possibly because of insufficient CPU).

Synthetic tests are supported on a variety of applications: Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, TFTP Server, Cisco Conference Connection, Cisco Emergency Response, Cisco Unity, and Cisco Unity Express. The synthetic tests can be scheduled to be run on a periodic basis.

Synthetic Test Descriptions and Expected Results

Table 3 describes the synthetic tests and gives the expected results.

Table 3. Synthetic Test Descriptions

Synthetic Test	Description	Expected Results
Phone Registration	Opens a connection with Cisco Unified Communications Manager/Cisco Unified Communications Manager Express and registers a simulated IP phone	Successful registration of the phone.

Synthetic Test	Description	Expected Results
Off-Hook	Simulates an off-hook state to Cisco Unified Communications Manager/Cisco Unified Communications Manager Express and checks for receipt of a dial tone	<p>Receives a dial-tone signal from Cisco Unified Communications Manager. The registration of the synthetic phone takes place only for the first time because registration is a costly operation on Cisco Unified Communications Manager.</p> <p>However, if the test fails, then synthetic phones are registered again for the next test cycle only.</p> <p>After the synthetic phone is registered, Cisco Prime Collaboration Assurance checks for a dial-tone signal from Cisco Unified Communications Manager.</p>
End-to-End Call	Initiates a call to a second simulated or real IP phone	<p>Registers, goes off-hook, and places the call.</p> <p>Ring indication.</p> <p>Destination phone goes off-hook to accept the call.</p> <p>If call progress tones and announcements are configured on the gateway for your end-to-end call, the test may succeed even before the phone rings or after a couple of rings.</p> <p>This indicates that your gateway is working correctly. It can also confirm that the destination route pattern is correct.</p> <p>The registration of the phone occurs only during the first test because registration is a costly operation on Cisco Unified Communications Manager/Cisco Unified Communications Manager Express. However, if the test fails, the registration will occur for the next test cycle only.</p> <p>Enable RTP transmission: Cisco Prime Collaboration Assurance plays a recorded announcement upon answer. Use this feature in conjunction with the Cisco 1040 Sensor to monitor the quality of voice (QoV) of the test call.</p>
TFTP Receive Test	Performs a TFTP get-file operation on the TFTP server	Successful download of a configuration file from the TFTP server.
Emergency Call Test	Initiates a call to the emergency number to test the dynamic routing of emergency calls	<p>All calls initiated.</p> <p>Ring indication on Public Safety Answering Point (PSAP) and On Site Alert Number (OSAN), if configured.</p>
Cisco Conference Connection Test	Creates a conference (meeting) in the Conference Center and connects to the meeting	<p>Conference created with the specified meeting ID.</p> <p>Call initiated.</p> <p>First person and second person (if configured) successfully connect to the conference.</p>
Cisco Unity Message Waiting Indicator Test	Calls the target phone and leaves a voice message in the voice mailbox	Activation of the phone's message-waiting indicator. The message is then deleted and the message-waiting indicator is deactivated.

How Many Simulated IP Phones Do I Need?

The number of simulated IP phones you need to define in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express depends on the number of tests you plan to configure. Different types of confidence tests need a different number of IP phones. See Table 4.

A predefined MAC address range has been set aside for these IP phones so that it does not clash with any of the real IP phones or devices in the network. The MAC address range that is available for synthetic testing is between 00059a3b7700 and 00059a3b8aff.

It is recommended that you input the description for these IP phones as **Cisco Prime Collaboration Assurance Simulated Phone** when they are configured in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express so that the description is distinct from the descriptions of other IP phones in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express. The phones to be used in confidence testing must be configured as 7960 phones in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express.

Table 4. Number of Phones Required for Confidence Tests

Type of Test	Phones Needed for Test	Total Phones Needed
Phone Registration	1 (synthetic phone)	1 per Cisco Unified Communications Manager and Communications Manager Express
Off-Hook	1 (synthetic phone)	1 per Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
End-to-End Call Test with real phones	2 (1 synthetic phone and 1 real phone)	2 per Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
End-to-End Call Test with synthetic phones	2 (synthetic phones)	2 per Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
TFTP Receive Test	0	
Emergency Call Test (without on-site alert number)	2 (synthetic phones)	
Emergency Call Test (with on-site alert number)	3 (synthetic phones)	
Cisco Conference Connection Test	2 (synthetic phones)	
Cisco Unity Message-Waiting Indicator Test	2 (synthetic phones)	

Creating Synthetic IP Phones in Cisco Unified Communications Manager

To define simulated phones in Cisco Unified Communications Manager for the synthetic tests, do the following:

- Step 1.** Launch and log in to the Cisco Unified Communications Manager Administration page.
- Step 2.** From the Cisco Unified Communications Manager Administration tool, select from the menu **Device > Add a New Device**.
- Step 3.** Change the device type from the drop-down menu to **Phone** and click **Next**.
The phone type for the simulated phone must be Cisco 7960.
- Step 4.** Select this model as the phone type and click **Next**.
- Step 5.** In the Phone Configuration window, enter a MAC address between 00059a3b7700 and 00059a3b8aff.
The tool automatically fills in the Description field. Other required fields are Device Pool and Button Template. Keep the default values for these fields.
- Step 6.** Click **Insert**.

Schedule an IP Phone Discovery; it must complete before the new synthetic IP phone can be used in the synthetic test.

Node-to-Node Tests

Node-to-node tests are typically used to measure jitter, packet loss, and delay on synthetic test traffic generated by the Cisco IOS Software IP SLA on any Cisco IOS device across a WAN.

Preparing Devices for Node-to-Node Tests

The IP SLA is enabled manually in Cisco IOS Software. You may need to configure, depending on the Cisco IOS device, the RTR Responder, or the IP SLA Responder command-line interface. The codec type for the jitter test is supported only on certain versions of Cisco IOS Software (specifically, 12.3(4)T and later). Therefore, it is possible that the codec type selection may be grayed out based on the source device you choose.

Node-to-Node Test Events

The events are raised on the source device. A threshold event is generated when the threshold violation occurs for three consecutive polling cycles. The event is cleared if the value falls below the threshold in the following polling cycle.

The following node-to-node events can be generated:

- NodeToNodeTestFailed
- RoundTripResponseTime_ThresholdExceeded
- RingBackResponseTime_ThresholdExceeded
- RegistrationResponseTime_ThresholdExceeded
- AverageLatency_ThresholdExceeded
- PacketLossSD_ThresholdExceeded
- PacketLossDS_ThresholdExceeded

Batch Tests

Batch tests help enable you to test the health and connectivity of a branch office. Batch tests consist of a set of synthetic tests that are run on voice applications (for instance, Cisco Unified Communications Manager Express or Cisco Unity Express) that are deployed in a branch office and a set of phone tests that are run on real phones in the branch office. Batch tests can be run on demand for troubleshooting purposes or on a scheduled basis to verify the health of the voice network in the branch office.

The batch test import file is an XML file. You can find the template of an import file in the /opt/CSCOpX/ImportFiles folder. You need to use SFTP as the root user to the Cisco Prime Collaboration Assurance server. The SFTP port is port 26. You should create your own XML file by modifying the template file batchtest.xml, and then create the batch test by importing your XML file (**Diagnostics > Batch Tests > Create**).

If you encounter an error message similar to “The batch test import file has fatal errors” please correct the import file and import again, and verify that your seed file is formatted correctly.

Cisco Prime Collaboration Assurance saves the data collected by the batch tests to disk. Batch test data is stored on the Cisco Prime Collaboration Assurance server in the following location: /opt/CSCOpX\data\bt.

Understanding Phone Tests

The phone tests that are run as part of batch testing take control of a real phone in the network and make a call from that phone to another phone. Phone tests use JTAPI credentials. These credentials must be included in the batch test import file.

Table 5 describes the different phone tests that are used in batch testing.

Table 5. Phone Test Descriptions - Batch Tests

Test	Description
Call	Takes control of a phone and places a call to a given number. The call can be from a real phone to a number, in which case the test is controlling the caller only. Alternatively, the call can be from a real phone to a real phone, in which case the test is controlling both the caller and the receiver.
Call Hold	Takes control of two phones and performs the following: Places a call from phone A to phone B. Has phone B put the call on hold.

Test	Description
	Disconnects the call.
Call Forward	<p>Takes control of three phones and performs the following:</p> <p>Places a call from phone A to phone B.</p> <p>Forwards the call to phone C from phone B.</p> <p>Verifies that the call is received by phone C.</p> <p>Disconnects the call.</p>
Call Park	<p>Takes control of three phones and performs the following:</p> <p>Places a call from phone A to phone B.</p> <p>Has phone B park the call. The call disappears from phone B and a message is displayed to tell you where the call is parked (for example, Call Park at 80503).</p> <p>Has phone C dial the number where the call is parked. The parked call is transferred to the phone that you made the call from.</p> <p>Disconnects the call.</p>
Call Transfer	<p>Takes control of three phones and performs the following:</p> <p>Places a call from phone A to phone B.</p> <p>Gets phone B to transfer the call to phone C.</p> <p>Gets phone C to accept the call.</p> <p>Disconnects the call.</p>
Conference	<p>Takes control of three phones and performs the following:</p> <p>Places a call from phone A to phone B.</p> <p>Places a conference call from phone A to phone C.</p> <p>Disconnects the call.</p>

When you are creating a JTAPI application user, make sure of the following:

- Communications Manager 5.x/6.x and greater: All the test phones and test probes need to be controlled devices for the JTAPI application the user created for phone testing. Also make sure the JTAPI application user is assigned to the Standard CTI Enabled group and the Standard CTI Allow Control of All Devices group, as shown in Figure 27.

Figure 27. Communications Manager 8.x JTAPI User Setup

Device Information

Available Devices

Find more Phones
Find more Route Points
Find more Pilot Points

Controlled Devices

SEP00036B8B0991
SEP00036B8B0975
SEP00036BE7B3DF
SEP0002B9A7502E
SEP00059A3B7701

CAPF Information

Associated CAPF Profiles

Edit Profile

Permissions Information

Groups

Standard CTI Allow Control of All Devices
Standard CTI Enabled

Edit Group

Roles

Standard CTI Allow Control of All Devices
Standard CTI Enabled

Edit Role

You also need to include test phones and test probes in an XML file. Test phones are the phones that actually perform the phone functionality (call, call forward, call conferencing, call park, and call hold). Test probes are the other phones that participate in the phone tests.

For instance, the call conference test would be:

- Place a call from phone A to phone B
- From phone A, conference to phone C

You should define phone A as a test phone and phones B and C as test probes in XML.

The call-forward test would be:

- Place a call from phone A to phone B
- Forward the call to phone C by way of phone B
- Verify that the call is received by phone C

Then, in your XML test file, define phone A as a test phone, and define phones B and C as test probes.

Resolving Batch Test Failure

No events or alerts are generated when a component of a batch test fails. You must use the Batch Test Results report to see the results of a batch test. A new Batch Test Results report is generated every 24 hours for each batch test. The Batch Test Results report provides any error message for the individual tests that are a part of the batch test, and this might help you resolve the batch test failure.

- When the error message displayed is “Unable to create provider - Connection refused: connect”: Make sure that Cisco Unified Communications Manager CTI service is activated and the JTAPI user is created on Cisco Unified Communications Manager.
- When the error message displayed is “Unable to create provider - bad login or password”: Make sure that you include the same JTAPI user/password you have defined on Cisco Unified Communications Manager in the XML file.
- When the error message displayed is “Invalid phone address XXXX for the CCM XXXX”: Make sure that test phones and test probes are associated with the JTAPI user in the Cisco Unified Communications Manager configuration.
- When the error message displayed is “Address XXXX is not in provider’s domain”: Make sure that test phones and test probes are in your phone inventory. Run the phone inventory collection to bring newly added phones to the Cisco Prime Collaboration Assurance inventory.
- When the error message displayed is “The test did not complete in the stipulated 30 seconds”: Make sure no other synthetic test is run on the same test phones and test probes. It is also recommended that you run the individual test manually if you expect the test to be successful.

Troubleshooting Tips for Initial Deployment

Following are some of the most common questions that you might have when initially deploying Cisco Prime Collaboration 9.5. More are available on the Cisco Prime Collaboration documentation page at <http://www.cisco.com/go/primecollaboration>.

1. Why can't I see any Cisco TelePresence sessions at all in Cisco Prime Collaboration?

Cisco Prime Collaboration learns of the call from Cisco VCS or Cisco Unified Communications Manager. If Cisco VCS or Cisco Unified Communications Manager is in "managed" state, make sure JTAPI credentials are valid in the Cisco Unified Communications Manager profile. Make sure all the endpoints are added as controlled devices.

If the call is using Cisco VCS, make sure that the Cisco Prime Collaboration server is registered as one of the feedback servers in all the Cisco VCS servers. A quick way to verify whether or not Cisco Prime Collaboration is registered with a particular Cisco VCS is to go to the following URL for Cisco VCS using a browser and replace the VCS_IPAddress with the IP address of the VCS Server: [Error! Hyperlink reference not valid.](#)

2. Why do devices show up as inaccessible?

When devices show as inaccessible, Cisco Prime Collaboration can reach the IP address but is not able to get any information from the device using SNMP or HTTP. Please refer to the section on verifying credentials.

3. Why do devices show up as unsupported?

This indication really means that devices are either third-party devices or they are new devices that were released after Cisco Prime Collaboration 9.5 and need to be added to the Cisco Prime Collaboration device support. Check for an update for Cisco Prime Collaboration on Cisco.com to see if the latest patch supports the device in question.

4. Why does Cisco Prime Collaboration tag devices as unsupported for the medianet category when they are medianet-capable?

Make sure you have the appropriate hardware and software and a license that supports medianet for the device in question. Medianet also needs to be enabled (one-time configuration) for Cisco Prime Collaboration to take advantage of medianet capabilities for troubleshooting. Check to see if the HTTP user is blocked by an access list.

5. Why do the Top 5 Poor Voice Quality Locations and Top 5 Call Failure Locations show no data?

Check if you have added the Cisco Prime Collaboration Assurance server IP as a billing server in Cisco Unified Communications Manager. Check if you have any poor calls by navigating to Reports > Interactive Reports > Voice Call Quality Reports > Endpoints and running a report by choosing Poor calls in the Grade filter. The Global Call Quality Settings in Administration > Alarm and Event Configuration > Threshold Settings define the MOS values for different codecs that define whether a call is Poor, Acceptable, or Good.

Also if there are less than 0.5 percent of calls in a location that are poor then the Location graph won't show any data for that location. Same for the Top 5 Call Failure Locations graph. Check the Reports-InteractiveReports > Call Quality Reports > CDR report and filter for failed calls to see if there are any failed calls. If there are no failed calls for the last 15 minutes for any location then the Top 5 Call Failure Locations graph will not show any data.

Appendix

Cisco Prime Collaboration Page on Cisco.com

<http://www.cisco.com/go/primecollaboration>

Install and Upgrade Guide for Cisco Prime Collaboration 9.5

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration/9.5/quick/start/guide/Cisco_Prime_Collaboration_Quick_Start_Guide_9_5.html

End-User Guide for Cisco Prime Collaboration 9.5

http://www.cisco.com/en/US/products/ps12363/products_user_guide_list.html

Cisco TelePresence Management Suite

For the latest documents go to: <http://www.cisco.com/go/telepresence>

Cisco TelePresence Server

For the latest documents go to: <http://www.cisco.com/go/telepresence>

Cisco Unified Communications Manager

<http://www.cisco.com/en/US/products/sw/voicesw/ps556/index.html>

Cisco TelePresence Video Communication Server (VCS)

For the latest documents go to: <http://www.cisco.com/go/telepresence>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)