

Cisco Prime Collaboration Manager 1.1

Deployment Guide

November, 2011

For further information, questions and comments please contact ccbu-pricing@cisco.com

Contents

1. Scope	4
2. Introduction	4
2.1 Video Infrastructure	4
3. Installation	5
3.1 Prerequisites	5
3.1.1 Server Requirement	5
3.1.2 Client Requirement	5
3.2 How to Install the Virtual Appliance	5
3.3 Configuring the Virtual Appliance	6
3.4 Licensing the Product	7
3.4.1 Obtaining a PAK	7
3.4.2 Obtaining a License File	7
4. Preparing the Network	8
4.1 Cisco Supported Version Matrix for Video Infrastructure	8
4.2 Mandatory Protocol Matrix for Cisco Video Infrastructure	8
4.3 Verifying Credentials	9
4.4 Preparing Call Scheduling and Calendaring for Cisco Prime Collaboration Manager	10
4.4.1 Preparing Cisco TelePresence Management Suite	10
Enable HTTP	10
Enable SNMP	10
Verify Credentials	11
Booking API for Cisco TMS	11
4.4.2 Preparing Cisco TelePresence Server Manager	12
Requirements for the Cisco TelePresence Server Manager and LDAP and Exchange	12
Enable HTTP	13
Enable SNMP	13
Verify Credentials	13
4.5 Preparing Multipoint Bridges and Switches for Conferencing	14
4.5.1 Preparing MCUs for Cisco Prime Collaboration Manager	14
Enable HTTP	14
Enable SNMP	14
Verify Credentials	14
4.5.2 Preparing Cisco TelePresence Multipoint Switch for Cisco Prime Collaboration Manager	14
Enable HTTP	14
Enable SNMP	14
Verify Credentials	15
4.5.3 Preparing the Cisco TelePresence Server (Appliance and Blade)	15
Enable HTTP	15
Enable SNMP	15
Verify Credentials	15
4.6 Preparing Call Controllers and Processors for Cisco Prime Collaboration Manager	15
4.6.1 Preparing Cisco Unified Communications Manager	15
Enable HTTP	15
Enable SNMP	17
Enable JTAPI	18
Device Profile Tips for Cisco Unified Communications Manager	19
Verify Credentials	20
4.6.2 Preparing Cisco TelePresence Video Communication Server	20
Enable HTTP	20
Enable SNMP	20
Verify Credentials	20
4.7 Preparing Video Endpoints	21
4.7.1 Cisco TelePresence Server Video Endpoints	21
Enable HTTP	21

Enable SNMP	21
Enable CLI Access	21
Verify Credentials	22
4.7.2 Cisco TelePresence C and EX Series Video Endpoints	22
Enable HTTP	22
Enable SNMP	22
Enable CLI Access	23
Verify Credentials	23
4.8 Preparing Network Devices	23
4.8.1 Non-medianet Routers and Switches	23
4.8.2 Medianet-Capable Routers and Switches	24
Verify Credentials	25
5. Discovering the Network	25
5.1 Discovering Using Cisco TelePresence Server Manager or Cisco TMS	25
5.2 What About Network Devices?	26
6. Troubleshooting Tips for Initial Deployment	26
6.1 Why Can't I See Any Cisco TelePresence Sessions at All in Cisco Prime Collaboration Manager? ..	27
6.2 Why Do Devices Show Up as Inaccessible?	27
6.3 Why Do Devices Show Up as Unsupported?	27
6.4 Why Does Cisco Prime Collaboration Manager Tag Devices as Unsupported for Medianet Category When They Are Medianet-Capable?	27
7. Appendix	27
7.1 Cisco Prime Collaboration Manager page on Cisco.com:	27
7.1.1 Install and Upgrade Guide for Cisco Prime Collaboration Manager 1.1:	27
7.1.2 End-User Guide for Cisco Prime Collaboration Manager 1.1:	27
7.1.3 Cisco TelePresence Management Suite (TMS):	27
7.1.4 Cisco TelePresence Server Manager (Cisco TelePresence Server Manager)	28
7.1.5 Cisco Unified Cisco Unified Communications Manager:	28
7.1.6 Cisco TelePresence Video Communication Server (VCS)	28

1. Scope

This document provides a step-by-step guide for successful deployment of Cisco Prime® Collaboration Manager Version 1.1 in a virtualized environment.

2. Introduction

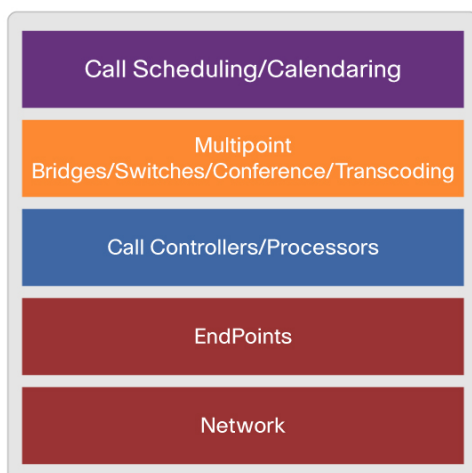
Cisco Prime Collaboration Manager allows video network operations centers (NOCs) to visualize, monitor, and troubleshoot Cisco TelePresence® and Video Infrastructure applications. This guide examines the details of all the aspects of deploying Cisco Prime Collaboration Manager. New users can use this guide to deploy the virtual appliance, and advanced users can use it as a starting point for troubleshooting purposes.

2.1 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 telepresence session. Figure 1 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 other in real time.
- **Call scheduling and calendaring:** This application allows the video calls to be scheduled just like the 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 1. Typical Video Infrastructure



3. Installation

Installing the Cisco Prime Collaboration Manager virtual appliance takes only about 15 to 30 minutes. This guide describes the shortest way to start reaping the benefits of Cisco Prime Collaboration Manager in monitoring and troubleshooting your Video Infrastructure.

3.1 Prerequisites

You can install Cisco Prime Collaboration Manager as a VMware Virtual Appliance only (as an [.ova](#)) file that you can import into your VMware Virtual Infrastructure (ESX/ESXi 4.1). You must install Cisco Prime Collaboration Manager on 64-bit hardware. Specifications of server and client follow.

3.1.1 Server Requirement

Table 1 shows the server that is required to host the Cisco Prime Collaboration Manager Virtual Application (vApp).

Table 1. Virtual Machine Requirements

Endpoints Managed in Cisco Prime Collaboration Manager	CPU	RAM	NIC	Disk Space
Up to 1000 endpoints	4	8 GB	1 Gbps	90 GB
More than 1000 endpoints	4	16 GB	1 Gbps	90 GB

3.1.2 Client Requirement

Table 2 shows the client requirement for using Cisco Prime Collaboration Manager. Screen resolution of 1024 x 768 or higher is recommended. Adobe Flash Player Version 10.0 is required for some of the dashlets to work on the Landing Page or Home page.

Table 2. Client Requirement

Operating System	Browser Version	Flash Version
Windows	Mozilla Firefox 3.6, 4, 5 or Internet Explorer 8 8.0 or 9.x	Adobe Flash 10
Mac	Mozilla Firefox 3.6, 4, or 5	Adobe Flash 10
Linux	Mozilla Firefox 3.6, 4, or 5	Adobe Flash 10

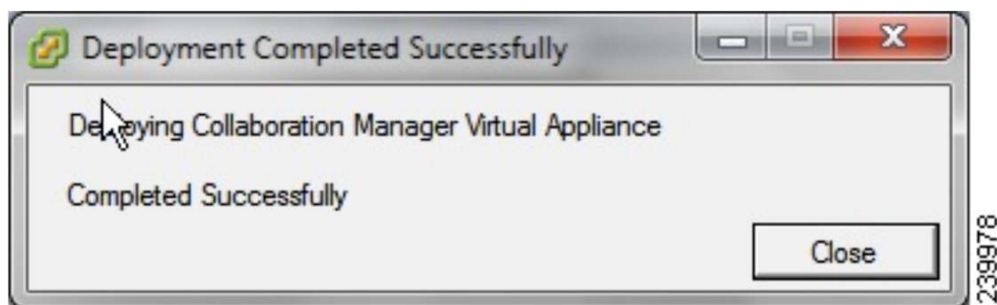
3.2 How to Install the Virtual Appliance

Cisco Prime Collaboration Manager is delivered as an Open Virtual Appliance ([OVA](#)) file. An OVA allows you to easily deploy a prepackaged virtual machine. Before you begin, make sure the .OVA file is downloaded (you can download an evaluation copy of Cisco Prime Collaboration Manager from <http://www.cisco.com/go/nmsevals>) and saved to the same machine where VMware vSphere client is installed. Do the following to install the virtual appliance using VMware vSphere Client:

- Step 1. Launch your VMware vSphere Client. (The best way is to point to the ESX host's webpage.)
- Step 2. Choose File > Deploy OVF Template.
- Step 3. Use the default option of "Deploy from file". Click the Browse button and select the .ova file.
- Step 4. Click Next and review the settings to make sure Cisco Prime Collaboration Manager is selected.
- Step 5. Specify a name and location for the template that you are deploying. The name must be unique within the inventory folder; it can contain up to 80 characters.

- Step 6. Pick the right Host, Cluster for the virtual machine, resource pool, and data store in the next couple of steps. This information will be unique to each virtual infrastructure.
- Step 7. On the Disk Format screen, choose “Thick Provisioning” (default for Cisco Prime Collaboration Manager .ova).
- Step 8. On the “Ready to Complete” screen, review the virtual appliance settings and click “Finish” to start uploading the .ova file to the ESX host.
- Step 9. This process may take a few minutes to complete. Check the progress bar in the “Deploying Virtual Application” window to monitor the task status. On successful completion of the deployment task, a confirmation window appears as shown in Figure 2.

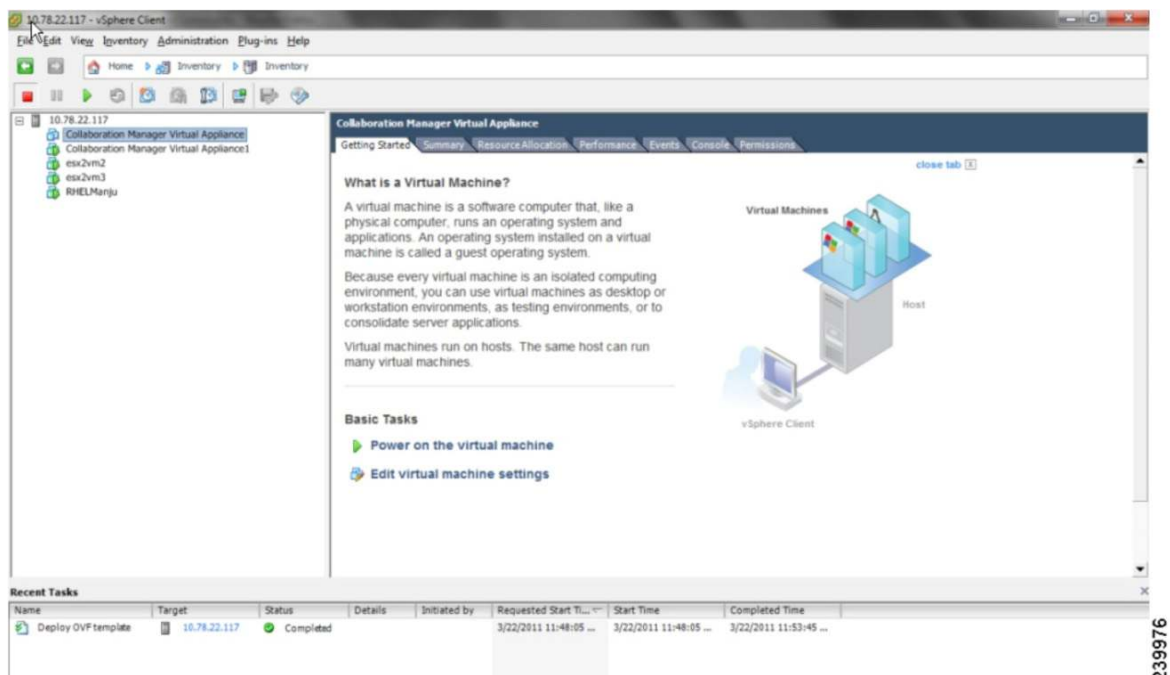
Figure 2. Window Showing Successful Completion



3.3 Configuring the Virtual Appliance

- Step 1. Power on the virtual machine. To do this, right-click the virtual appliance, choose Power > Power On (Figure 3).

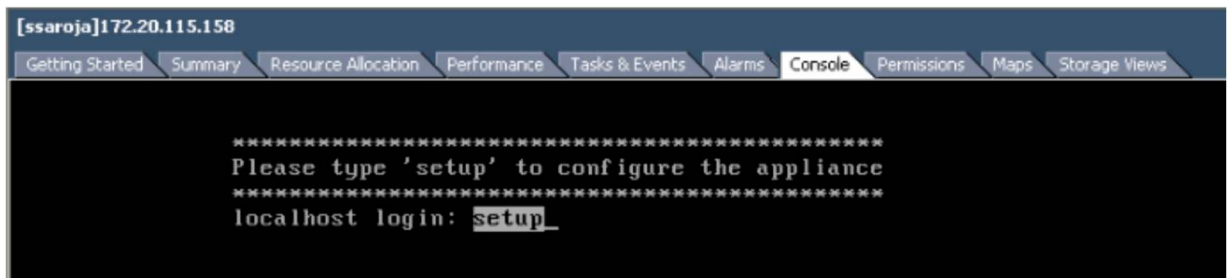
Figure 3. Powering On



- Step 2. Click the Console Tab, and click the black space to see the prompt.

Step 3. At the local host login prompt, enter setup (Figure 4).

Figure 4. Application Setup from Virtual Machine Console



Step 4. The console prompts you for the following parameters:

- a. IP Address: Enter the IP address of the virtual appliance.
- b. IP default netmask: Enter the default subnet mask for the IP address.
- c. IP default gateway: Enter the IP address of the default gateway.
- d. Default DNS domain: Enter the default domain name.
- e. Primary name server: Enter the primary name server. You may add or edit this name server. To configure multiple name servers or Network Time Protocol (NTP) servers, enter y.
- f. Primary NTP server [time.nist.gov]: Point to the corporate NTP server.
- g. Time zone: The default time zone is UTC. Time zones could be entered as PST8PDT or US/Pacific.
- h. Username: Enter the name of the first administrative user. You can accept the default, which is admin.
- i. Password: Enter the password for command-line interface (CLI) access to Cisco Prime Collaboration Manager.

After the OS and application are installed, go the virtual machine Console tab and accept the user agreement in to use to use the application.

3.4 Licensing the Product

3.4.1 Obtaining a PAK

The Product Activation Key (PAK) is located on the software claim certificate. You can obtain the claim certificate through the eDelivery system. For information about eDelivery, please visit:

<http://www.cisco.com/web/partners/tools/edelivery.html>.

3.4.2 Obtaining a License File

To obtain a license file, you must register the Cisco Prime Collaboration Manager product with Cisco.com, using the PAK and the Universal Unique Identifier (UUID) that is generated on each Cisco Prime Collaboration Manager server. The UUID is automatically generated on the server when you install the Cisco Prime Collaboration Manager evaluation version. You can get the UUID from the About page in the application. You need to provide this value when you generate the license file. You can generate your license file at

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

After you obtain the license file, you must add the license to Cisco Prime Collaboration Manager. Refer to the Cisco Prime Collaboration Manager 1.1 Administration and User Guide for information about adding license files. When you add the license file, the evaluation license is automatically converted into the perpetual license type that

you purchased. The evaluation license is valid for 3 months from the time Cisco Prime Collaboration Manager is installed, allowing 5000 units to manage.

4. Preparing the Network

This part is the most important part in successfully deploying Cisco Prime Collaboration Manager. You must make sure all the credentials are in place and are correctly entered in the application. Tables 3 and 4 give information about versions, protocols, and types of credentials needed for each infrastructure component.

4.1 Cisco Supported Version Matrix for Video Infrastructure

Table 3. Cisco Supported Version Matrix for Video Infrastructure

Video Infrastructure Component	Description - Application or Devices	Minimum Versions	Supported Versions
Call scheduling and calendaring	Cisco TelePresence Management Suite (Cisco TMS)	13.0	13.0 or 13.1
	Cisco TelePresence Server Manager	1.7	1.7 or 1.8
Multipoint bridges, switches, and conferencing	Multipoint-control-unit (MCU) device and blade	4.1	4.1 or 4.2
	Multipoint Switch	1.6.3	1.6.3, 1.7, or 1.8
	Cisco TelePresence Server - Device and blade	2.1	2.1 or 2.2
	Cisco TelePresence Server MSE Supervisor	2.1	2.1, or 2.2
Call controllers and processors	Cisco Unified Communications Manager	7.1	8.6
	Cisco VCS - Control and Cisco TelePresence Expressway technology (Expressway)	6.1	6.0, 6.1, or 7.0
Endpoints	Cisco TelePresence C and EX Series based endpoints	4.1	4.1 or 4.2
	Cisco TelePresence Server	1.7.0	1.6.4, 1.7, or 1.8
Networking devices	Cisco routers	15.1(3)	15.1(3) or Later
	Cisco switches	12.2(58)	12.2(58) or Later

4.2 Mandatory Protocol Matrix for Cisco Video Infrastructure

Table 4 shows the type of credential information that you need to enter in Cisco Prime Collaboration Manager in order to successfully manage the Cisco Video Infrastructure.

Table 4. Mandatory Protocol Credential Matrix for Cisco Video Infrastructure

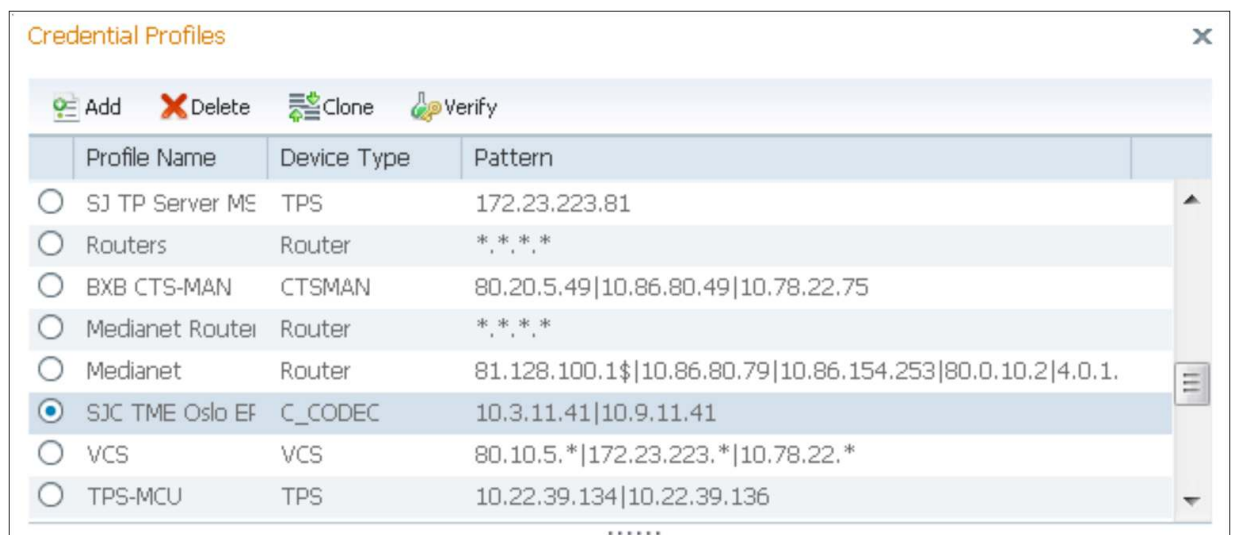
Video Infrastructure Component	Component	HTTP	SNMP (Read Only)	CLI (SSH/Telnet)	JTAPI
Call scheduling and calendaring	Cisco TMS	Yes ^e	Yes	No	No
	Cisco TelePresence Server Manager	Yes ^e	Yes	No	No
Multipoint bridges, switches, and conferencing	MCU (appliance and blade)	Yes	Yes	No	No
	Multipoint Switch	Yes	Yes	No	No
	Cisco TelePresence Server (appliance and blade)	Yes	No	No	No
	Cisco TelePresence Server MSE Supervisor	Yes	Yes	No	No
Call controllers and processors	Cisco VCS (control and Expressway)	Yes	Yes	No	No
	Cisco Unified Communications Manager	Yes	Yes	No	Yes
Endpoints	Cisco VCS-based endpoints (Cisco TelePresence C and EX Series)	Yes	Yes	Yes ^a	No
	Cisco TelePresence Server endpoint	No	Yes	Yes ^a	No

Video Infrastructure Component	Component	HTTP	SNMP (Read Only)	CLI (SSH/Telnet)	JTAPI
Networking devices	Router and switch	No	Yes	Yes ^b	No
Notes: <ol style="list-style-type: none"> For video endpoints, CLI login credentials are required for troubleshooting. For routers and switches, CLI login credentials are required (in addition to Simple Network Management Protocol [SNMP] read-only access) if you want to perform medianet based troubleshooting. Note that medianet features are available only in the newer Cisco IOS® Software releases. You also need to enable Cisco Discovery Protocol on all network devices if you want to trace the troubleshooting path. Cisco Prime Collaboration Manager needs to access the Cisco VCS Expressway devices in the demilitarized zone (DMZ) using HTTP and SNMP protocols. If these protocols are blocked by firewalls, then you cannot manage or monitor Cisco VCS Expressway with Cisco Prime Collaboration Manager. The HTTP user for Cisco TMS and Cisco TelePresence Server Manager must have booking application-programming-interface (API) access and LiveDesk access, respectively. More information about configuring this access is available at Configuring Cisco TMS Third Party Booking API User and Configuring Reporting API for Cisco TelePresence Server Manager 1.8. 					

4.3 Verifying Credentials

As you prepare to manage various components in the Cisco Video Infrastructure, you need to verify that the entered credentials are correct. Cisco Prime Collaboration Manager 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 Inventory > Device Inventory > Manage Credentials > Select the credential set that contains the device/appliance/server and click Verify (Figure 5).

Figure 5. Credential Profiles



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 6).

Click on Another profile to get back to editing the profile.

Figure 6. Verifying Credentials

The screenshot shows a 'Credential Profiles' window with a table of profiles and a test result section.

	Profile Name	Device Type	Pattern
<input type="radio"/>	SJ TP Server ME	TPS	172.23.223.81
<input type="radio"/>	Routers	Router	*,*,*,*
<input type="radio"/>	BXB CTS-MAN	CTSMAN	80.20.5.49 10.86.80.49 10.78.22.75
<input type="radio"/>	Medianet Router	Router	*,*,*,*
<input type="radio"/>	Medianet	Router	81.128.100.1\$ 10.86.80.79 10.86.154.253 80.0.10.2 4.0.1.
<input checked="" type="radio"/>	SJC TME Oslo EF	C_CODEC	10.3.11.41 10.9.11.41
<input type="radio"/>	VCS	VCS	80.10.5.* 172.23.223.* 10.78.22.*
<input type="radio"/>	TPS-MCU	TPS	10.22.39.134 10.22.39.136

Test Credential Profile

Enter IP address to which the credential profile need to be tested.

Profile Name **SJC TME Oslo EPs**

Device Type **C_CODEC**

IP Address

Test

Test Credential Result

SNMP **Passed** (Response Time : in 0.695 sec)

HTTP **Passed** (Response Time : in 0.636 sec)

CLI **Passed** (Response Time : in 10.789 sec)

Close

4.4 Preparing Call Scheduling and Calendaring for Cisco Prime Collaboration Manager

4.4.1 Preparing Cisco TelePresence Management Suite

From Table 4, we can see that only HTTP and SNMP access is needed to successfully monitor Cisco TMS.

Enable HTTP

Cisco TMS 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 Manager will not be able to log in, either. Unless this problem is fixed, Cisco Prime Collaboration Manager will not be able to successfully monitor Cisco TMS. Refer to "Installation and Getting Started Guide" for Cisco TMS 13.0 for detailed instructions about how to change the admin password.

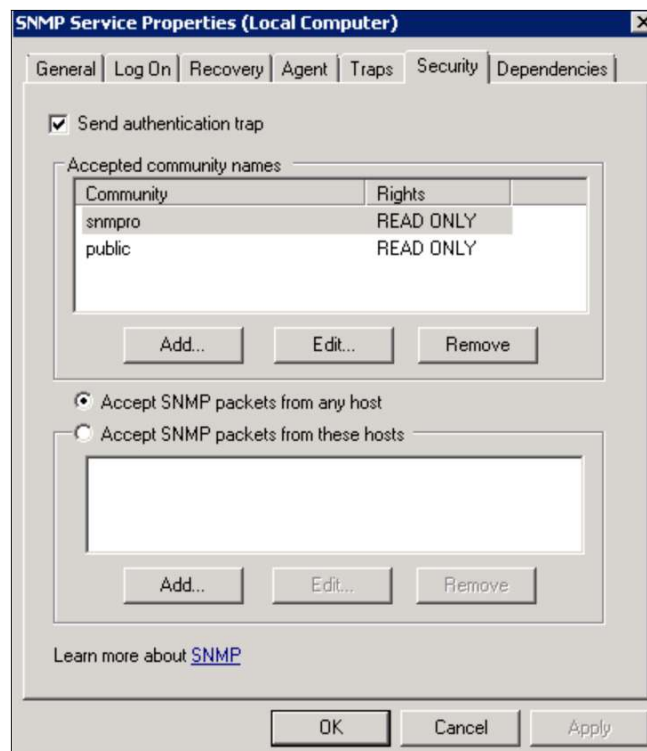
Enable SNMP

By default, "public" and "Public" are enabled as SNMP Read Only (RO) community strings for Cisco TMS. This string is what Cisco TMS 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 > change the SNMP settings here.

In addition to the Web GUI, SNMP service on the Cisco TMS 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 on that service, and go to Properties. Click the Security tab and choose Add new SNMP string (Figure 7). Unless you want only specific hosts polling SNMP from Cisco TMS, you can leave the default setting of “Accept SNMP packets from any host”.

Figure 7. SNMP Service Properties



You can also click the Traps tab next to Security and add the IP address of Cisco Prime Collaboration Manager 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 TMS. Cisco Prime Collaboration Manager will use this information to show where Cisco TMS is located in the inventory.

Restart the SNMP Service after the changes are made.

Verify Credentials

Please refer to section 4.3 for verifying credentials.

Booking API for Cisco TMS

The TANDBERG Management Suite (TMS) 3rd Party Booking API is an API that gives developers access to the booking functionality in TMS. The interface is used by TANDBERG in its Microsoft Exchange and IBM Lotus Domino implementations, and provides the same feature set as the user interface for the TANDBERG Scheduler.

To create the Booking API user:

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

The RemoteSetupService page appears.

Note: You may replace local host in the URL with the IP address of the Cisco TMS 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 the following URL:
<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 Manager will be polling from Cisco TMS.

Step 4. Click Invoke.

For more information about the Cisco TMS, refer to the documents available at:

http://www.tandberg.com/support/tms_documentation.jsp.

4.4.2 Preparing Cisco TelePresence Server Manager

From Table 4, we can see that only HTTP and SNMP access is needed to successfully manage Cisco TelePresence Server Manager. For the Cisco Prime Collaboration Manager server to retrieve data from Cisco TelePresence Server Manager 1.7, you must have a valid Metrics Dashboard (room and endpoint) and Reporting API license in Cisco TelePresence Server 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 Server Manager and LDAP and Exchange

On the Cisco TelePresence Server Manager side:

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

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:

```
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:█
```

2. Proper License is required for the Cisco TelePresence Server 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 Manager.
 - a. This user needs to have mailbox.
 - b. This user must be used as a HTTP user in Cisco Prime Collaboration Manager.

Back on the Cisco TelePresence Server Manager side:

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

Enable HTTP

Cisco TelePresence Server 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 Server 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 Secure Shell (SSH) Protocol into the Cisco TelePresence Server Manager. (Refer to the Cisco TelePresence Server 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 image 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 snmp r
Successfully added user
admin:█
```

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.5 Preparing Multipoint Bridges and Switches for Conferencing

The main products that are normally deployed for conferencing needs are 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.

4.5.1 Preparing MCUs for Cisco Prime Collaboration Manager

A Cisco TelePresence MCU MSE 8510 (MCU MSE 8510) cluster consists of a Cisco TelePresence MCU MSE 8050 Supervisor Blade (MCU MSE 8550) and a 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 Manager will not be able to log in, either. Unless this problem is fixed, Cisco Prime Collaboration Manager 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 MCU Codian Web Interface as mentioned previously. Navigate to Network > SNMP > Bottom portion of this page, which has the SNMP Read Only and Read Write strings. Change/Edit them as needed, and click “Update SNMP Settings” to apply the changes.

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.5.2 Preparing Cisco TelePresence Multipoint Switch for Cisco Prime Collaboration Manager

Enable HTTP

A dedicated user with minimum role of diagnostic technician should be good enough for managing the Multipoint Switch within Cisco Prime Collaboration Manager. 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 Manager 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.

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.5.3 Preparing the Cisco TelePresence Server (Appliance and Blade)

Enable HTTP

The user with API access should be sufficient for Cisco Prime Collaboration Manager to manage Cisco TelePresence Server. This user can be configured by logging into 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 telepresence server.

Enable SNMP

SNMP is not required for Cisco TelePresence Server.

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.6 Preparing Call Controllers and Processors for Cisco Prime Collaboration Manager

4.6.1 Preparing Cisco Unified Communications Manager

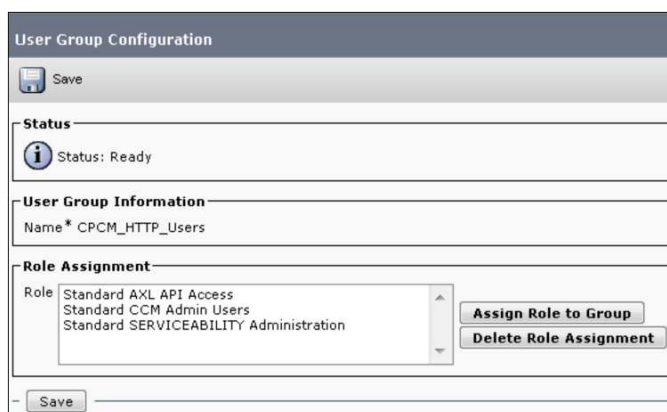
Enable HTTP


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

Step 1. 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 checkbox indicating that it is a user-defined group.

Figure 8. User Group Configuration



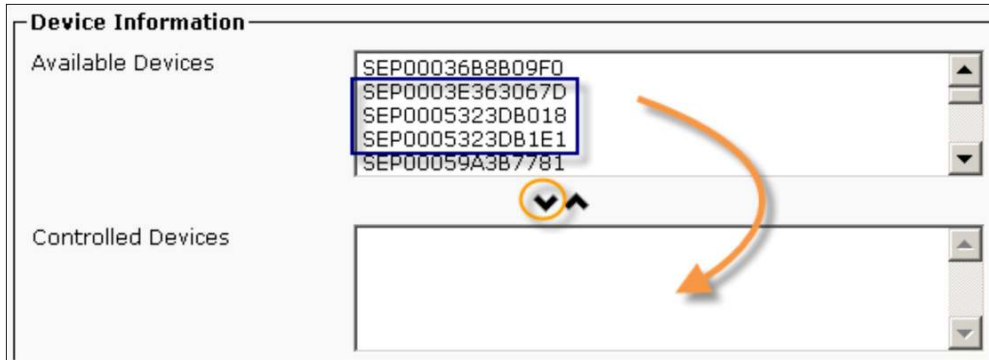
Step 2. Click the  (Roles) icon. A new window will pop up. Click the Assign Role to Group button > Select the following roles:

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

You should get a screen that looks something like Figure 8. Now click the Save button to save the configuration.

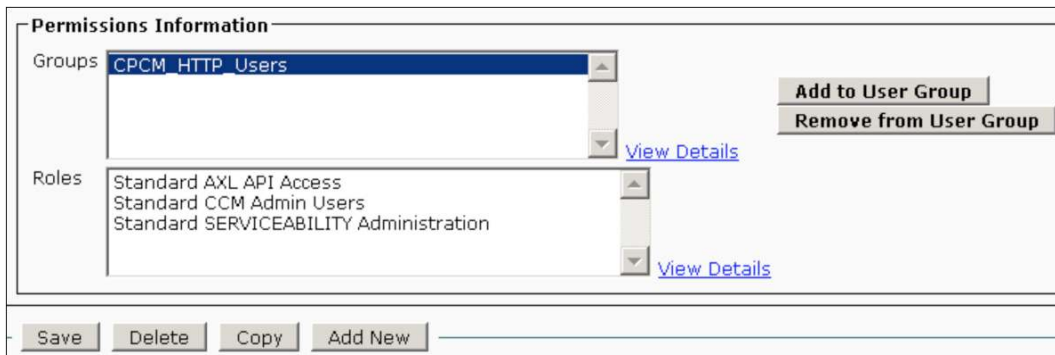
Step 3. From the main menu, navigate to User Management > Application Users > Create a new user. Call it “ccpm-http”, for example. Give a suitable password on the Application User Configuration page. Now from the Available device text area, you can either select the only certain type of devices. If you want to allow Cisco Prime Collaboration Manager 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 9

Figure 9. Device Information



Step 4. Scroll down to the Permission 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 right privileges as shown in Figure 10.

Figure 10. 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 into 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 > Select a Server and click Find (Figure 11).

Figure 11. 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 12.

Figure 12. Search Results

Search Results		
<input type="checkbox"/>	Community String Name	Access Privileges
<input type="checkbox"/>	snmpro	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 necessary SNMP related information as follows and save the configurations.

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 Manager 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 ensure you can create a new JTAPI user to help Cisco Prime Collaboration Manager 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 using administrator Role > 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 checkbox indicating that it is a user-defined group.

Step 2. Click the ⓘ (Roles) icon. A new window will pop up. Click Assign Role to Group Button > Select the following roles:

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled

You should get a screen that looks something like Figure 13.

Figure 13. User Group Information



User Group Information	
Name *	CPCM_JTAPI_Users

Role Assignment	
Role	Standard CTI Allow Call Monitoring Standard CTI Enabled

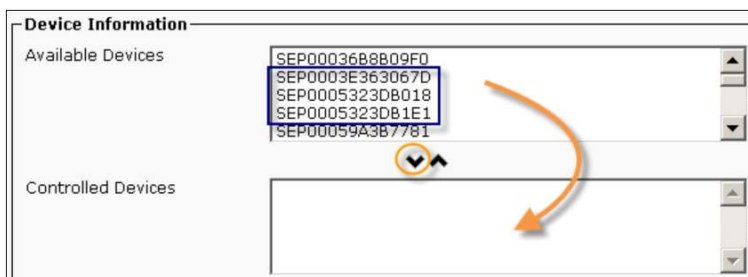
Assign Role to Group
Delete Role Assignment

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 few devices, or if you want to allow Cisco Prime Collaboration Manager 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 14.

Figure 14. Device Information



Device Information	
Available Devices	SEP00036B8B09F0 SEP0003E363067D SEP0005323DB018 SEP0005323DB1E1 SEP00059A3B7781
Controlled Devices	

Step 4. Scroll down to the Permission 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 right privileges as shown in Figure 15:

Figure 15. Permissions Information

Permissions Information

Groups: CPCM JTAPI Users [View Details](#) **Add to User Group** **Remove from User Group**

Roles: Standard CTI Allow Call Monitoring
Standard CTI Enabled [View Details](#)

Save **Delete** **Copy** **Add New**

Device Profile Tips for Cisco Unified Communications Manager

Following are some of the 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 right bandwidth. You can access the device pool from Cisco Unified CM Administration: System > Device Pool. Click the interested region 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 CTMS” section under Administrator Guide for Cisco Unified Communications Manager. Here is a link for Cisco Unified Communications Manager 1.7: 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 Manager CLI. Configure the Cisco Unified Communications Manager device profile to 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 it boots up.

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.6.2 Preparing Cisco TelePresence Video Communication Server

Cisco 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 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 administrator user “admin” is “TANDBERG”. If you cannot log in to the web GUI, Cisco Prime Collaboration Manager will not be able to log in, either. Unless this problem is fixed, Cisco Prime Collaboration Manager will not be able to successfully manage

the VCS. If the password is left blank, Cisco Prime Collaboration Manager will not be able to manage it, either; it is not recommended.

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 16 is a sample screen shot showing how SNMP v2 is configured.

Figure 16. Sample Screen Shot Showing SNMP Configuration

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.7 Preparing Video Endpoints

Cisco Prime Collaboration Manager 1.1 can manage various video endpoints, as shown in Table 5.

Table 5. Cisco Prime Collaboration Manager Endpoint Management

Endpoint Type	Supported Endpoint Models
Immersive endpoints 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 type of access are desirable for all endpoints: SNMP, HTTP, and CLI.

4.7.1 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 17 and then click Save and Apply Config.

Figure 17. 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 is a section “Secure Shell Information” (Figure 18).

Figure 18. 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 zero, it is up to the admin 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 Manager.

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.7.2 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 Manager cannot manage video endpoints with blank passwords; leaving the password blank is not recommended either for security reasons.

Enable SNMP

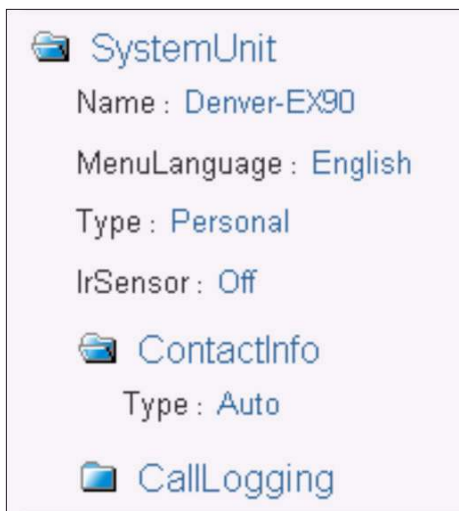
To enable SNMP access for Cisco Prime Collaboration Manager from the web interface, go to Configuration > Adv Configuration > Network Services > SNMP and click the value itself to edit it (Figure 19).

Figure 19. Enable SNMP



It is also recommended to put descriptive SystemUnit Name by navigating to Configuration > Adv Configuration > SystemUnit > Name and click the value itself to edit it (Figure 20).

Figure 20. Entering SystemUnit Name



Enable CLI Access

SSH should be enabled by default on TC 4.0 releases. Giving “admin” user access to Cisco Prime Collaboration Manager is sufficient for most cases; just make sure that the admin password is set and not left blank, because that is default. If you want to troubleshoot video sessions from Cisco TelePresence devices using Cisco Prime

Collaboration Manager, admin user access is necessary. Some of the commands needed to run the traceroutes are available only when logged in as root.

Verify Credentials

Please refer to section 4.3 for verifying credentials.

4.8 Preparing Network Devices

Cisco Prime Collaboration Manager uses Cisco solutions for optimizing medianets that are instrumented within medianet-capable devices. Table 6 is a snapshot of medianet-capable devices at the time of writing of this document.

Table 6. 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 feature navigator as mentioned below.	Cisco Catalyst 3560E, Catalyst 3560X, Catalyst 3750, Catalyst 3750E, and Catalyst 3750X	12.2SE 15.0SE

For 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 and updated list of device support.

4.8.1 Non-medianet 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.

4.8.2 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. In addition to the matrix mentioned above in Table 6, 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 right hardware, software, and license), you can use the following configuration to enable medianet for Cisco Prime Collaboration Manager 1.1. (Note: Letters in bold are variables that you need to substitute.)

```
!  
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 Monitoring 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 example).

```
!
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 great instrumentation within Cisco IOS Software. Cisco IOS IP SLAs 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 Manager 1.1 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 Manager 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 > Search for “IP SLAs Video Operation” and you should be see the latest device support for this feature.

In order for Cisco Prime Collaboration Manager 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
!
```

Verify Credentials

Please refer to section 4.3 for verifying credentials for routers and switches.

5. Discovering the Network

Discovery for Cisco Prime Collaboration Manager works in a different way than traditional for network-management-system (NMS) applications. Cisco Video Infrastructure is discovered using Cisco TelePresence Server Manager or Cisco TMS as the seed device. If those applications are not deployed, next best option is to use Cisco Unified Communications Manager or Cisco VCS. All of the video endpoints are automatically mapped to the right 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.

5.1 Discovering Using Cisco TelePresence Server Manager or Cisco TMS

Navigate to Inventory > Device Inventory > Discover Devices and enter an easy-to-find “Job Name”; most importantly, enter the IP address of Cisco TelePresence Server Managers or Cisco TMS. Click “Run Now” at the bottom Figure 21).

Figure 21. Discovery Setup

Discovery Setup

Job Name: Discovery 2011-Oct-25 04:48:57 PDT

Discovery Settings

Check Device Accessibility: ☒ True ☐ False

Validate credentials(i.e SNMP,HTTP,CLI etc.) for each discovered device.

IP Address

10.78.22.75|10.86.80.14|192.168.138.202|192.168.138.201

Enter IP addresses separated by a unique delimiter: comma, colon, pipe or blank space.

Schedule

Start Date: (Mm/dd/yyyy)

Start Time: 11:55 AM

End Date: (Mm/dd/yyyy) ☐ No End Date

☒ Daily ☐ Weekly

Schedule Run Now Cancel

As mentioned previously, if Cisco TelePresence Server Manager or Cisco TMS is not deployed, you also can initiate discovery using Cisco Unified Communications Manager or Cisco VCS as seed devices. When the discovery is running, you can check its status by going to “List Discovery Jobs” under Inventory > Device Inventory. 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.

5.2 What About Network Devices?

The only things you need to configure are the valid credential profiles for routers and switches. Cisco Prime Collaboration Manager 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 same way we added them in section 5.1 previously.

6. Troubleshooting Tips for Initial Deployment

Following are some of the most common questions that you might have when initially deploying Cisco Prime Collaboration Manager 1.1. More are available on the Cisco Prime Collaboration Manager documentation page at <http://www.cisco.com/go/cpcm>.

6.1 Why Can't I See Any Cisco TelePresence Sessions at All in Cisco Prime Collaboration Manager?

Cisco Prime Collaboration Manager learns 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, as mentioned in section 4.6.1 previously.

If the call is using Cisco VCS, make sure that the Cisco Prime Collaboration Manager 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 Manager is registered with a particular Cisco VCS is to go to the following URL for Cisco VCS: [Error! Hyperlink reference not valid.](#)

6.2 Why Do Devices Show Up as Inaccessible?

Devices shown as inaccessible means that Cisco Prime Collaboration Manager can reach the IP address but is not able to get any information from the device using SNMP or HTTP. Please refer to section 4.3 for verifying credentials.

6.3 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 Manager 1.1 and need to be added to the Cisco Prime Collaboration Manager device library. Check for an update for Cisco Prime Collaboration Manager on Cisco.com to see if the latest patch supports the device in question.

6.4 Why Does Cisco Prime Collaboration Manager Tag Devices as Unsupported for Medianet Category When They Are Medianet-Capable?

Refer to section 4.8.2 for medianet capability. Make sure you have the right hardware, software, and license that supports medianet for the device in question. Medianet also needs to be enabled (one-time configuration, as mentioned in section 4.8.2) for Cisco Prime Collaboration Manager to take advantage of medianet capabilities for troubleshooting. Check to see if the HTTP user is blocked by an access list.

7. Appendix

7.1 Cisco Prime Collaboration Manager page on Cisco.com:

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

7.1.1 Install and Upgrade Guide for Cisco Prime Collaboration Manager 1.1:

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration_manager/1.1/quickstart/guide/cm_qsg.html

7.1.2 End-User Guide for Cisco Prime Collaboration Manager 1.1:

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration_manager/1.1/user/guide/cm_uq.html

7.1.3 Cisco TelePresence Management Suite (TMS):

Admin Guide:

http://www.cisco.com/en/US/docs/telepresence/infrastructure/tms/admin_guide/Cisco_TMS_Admin_Guide_13-0.pdf

Install Guide:

http://www.cisco.com/en/US/docs/telepresence/infrastructure/tms/install_guide/Cisco_TMS_Install_Guide_13-0.pdf

7.1.4 Cisco TelePresence Server Manager (Cisco TelePresence Server Manager)

http://www.cisco.com/en/US/products/ps7074/tsd_products_support_series_home.html

7.1.5 Cisco Unified Cisco Unified Communications Manager:

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

7.1.6 Cisco TelePresence Video Communication Server (VCS)

<http://www.cisco.com/en/US/products/ps11337/index.html>



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)