Contents

Setting up Devices on the Network for Prime Collaboration Manager

This section describes how to configure devices on the network before you manage them in Cisco Prime Collaboration Manager.

Refer to Cisco Prime Collaboration Manager 1.2 Quick Start Guide for instructions on installing and upgrading Cisco Prime Collaboration Manager.

You must configure the endpoints, application managers, call processors, multipoint switches, and network devices with the following credentials:

- HTTP - Access the device through HTTP to poll system status and meeting information.
- SNMP - Read Community String and SNMP Authentication Protocol (SNMP V2 or SNMP V3) - Discover and manage the device.
- CLI - Access the device through CLI to discover media path for troubleshooting.
- JTAPI - Retrieve the session status information frosm the Cisco Unified CM.
- CDP - Discover neighboring devices.

Configuring Call Controllers and Processors

Configuring Cisco Unified Communications Manager

All CTS endpoints must be added as controlled devices in Cisco Unified CM to facilitate call detection. You must configure a HTTP and JTAPI user on the call processor.

Enable HTTP

You do not have to create a new user if you want to allow Cisco Prime Collaboration Manager to use admin credentials to log in. Alternatively, if you want to allow Cisco Prime Collaboration Manager to use 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 Manager can use to communicate.

To create a user:

1. Create a user group with sufficient privileges. Log in to the Cisco Unified Communications Manager Administration web interface using the administrator role.
2. Navigate to **User Management > User Groups** and create a new group with a suitable name, CPCM_HTTP_Users in this case.
3. Click **Role**.
4. Click **Assign Role to Group** and select the following roles:
    - Standard AXL API Access
    - Standard CCM Admin Users
    - Standard SERVICEABILITY Administration
5. Click **Save**.
6. From the main menu, navigate to **User Management > Application Users > Create a new user**. Specify a suitable password on the **Application User Configuration** page. You can select only certain type of devices from the Available Devices text area, or allow Cisco Prime Collaboration Manager to monitor all devices.
7. In the **Permission Information** section, click **Add to User Group** and select the group that was created in Step 1. (CPCM_HTTP_Users, for instance).
8. Click **Save**. The page is refreshed and the right privileges are displayed.

Enable SNMP

SNMP is not enabled in Cisco Unified Communications Manager by default.

To enable SNMP:

1. Log in to the **Cisco Unified Serviceability** view in the Cisco Unified Communications Manager web GUI.
2. From the main menu in the Cisco Unified Serviceability view, navigate to SNMP > v1/v2c > community string.
3. Select a Server and click **Find**.
   If the community string is already defined, the Community String Name is displayed in the Search Results.
4. Click **Add new** to add a new string if no results are displayed.
5. Specify the required SNMP information and save the configuration.

Enable JTAPI

JTAPI (Java Telephony API) 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 CM manages multiple call processor clusters. You must ensure that the cluster IDs are unique. Create a new JTAPI user to help Cisco Prime Collaboration Manager get the required information.

To create a new JTAPI user:

1. Log in to the Cisco Unified Communications Manager administration web interface using administrator role.
2. Navigate to User Management > **User Groups** and create a new group with a suitable name, **CPCM_HTTP_Users** in this case.
3. Move all endpoint devices (for example, Cisco TelePresence codecs) to the Controlled Devices table.
4. Click **Roles**.
5. Click **Assign Role to Group** and select the following roles:
    - Standard CTI Allow Call Monitoring

- Standard CTI Enabled
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf

6. Click **Save**.
7. From the main menu, navigate to **User Management > Application Users > Create a new user**. Specify a suitable password on the **Application User Configuration** page. You can select only certain type of devices from the Available Devices text area, or allow Cisco Prime Collaboration Manager to monitor all devices.
   Note: The password must not contain a semicolon (;) or equals (=).
8. In the **Permission Information** section, click **Add to User Group** and select the group that was created in step 1. (CPCM_HTTP_Users, for instance).
9. Click **Save**. The page is refreshed and the right privileges are displayed.

```
Note:
*Ensure the following services are activated and started:
 **Cisco CTIManager
 **Cisco AXL Web Service
 See the Cisco Unified Communications Manager guide for details about how
 to configure the application user.

*Check the following log to verify if the endpoints are CTI-controlled in the CUCM
and such JTAPI-related issues:[https://<cpcm-ip>/emsam/log/Tomcat/CUCMJTAPIDiag.log]
```

Configuring 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 successfully manage the VCS. Ensure the password field is not blank as it is not recommended.

Enable SNMP

You can easily enable SNMP from the Cisco VCS web GUI: Navigate to **System > SNMP** and enter the SNMP information.

Configuring Endpoints

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. To change the SNMP community string:

1. Navigate to Cisco Unified Communications Manager Administration.
2. Navigate to **Device > Phone** and search for Cisco TelePresence Server endpoints.
3. Click the **Device Name** link to go to the phone configuration page.
4. Edit the SNMP Configuration Parameters.
5. Click **Save and Apply Config**.

Enable CLI Access

SSH access to the Cisco TelePresence Server devices is also controlled through Cisco Unified Communications Manager Phone Configuration.

```
Note:
If the value of SSH admin Life and SSH helpdesk Life field is zero, the password never
expires (recommended for lab testing scenarios).
However, if the value is not zero, the admin must ensure that passwords are changed
before the specified interval, for anyone or any application to be able to perform SSH
in the device including Cisco Prime Collaboration Manager.
```

Cisco TelePresence C and EX Series Video Endpoints

Enable HTTP

By default, HTTP is enabled for Cisco TelePresence Endpoints. 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 space.

Enable SNMP

To enable SNMP access for Cisco Prime Collaboration Manager from the web interface:

Navigate to **Configuration > Adv Configuration > Network Services > SNMP** and click the value to edit.

Enable CLI Access

SSH must be enabled by default on TC 4.0 releases. Provide **admin** user access to Cisco Prime Collaboration Manager ensure that the admin password is set and is not the default value, which is blank. Admin user access is necessary if you want to troubleshoot video sessions from Cisco TelePresence devices using Cisco Prime Collaboration Manager. Some of the commands required to run the traceroutes are available only when you log in as root.

We recommend that you enter the real interface IP address of the gateway that runs the Hot Standby Router Protocol (HSRP), instead of the virtual IP address, while configuring the CTS. This enables Cisco Prime CM to accurately discover the troubleshooting path.

Endpoint monitoring is based on the SNMP polling. You can configure traps and syslogs on the endpoints, if required.

To monitor traps and syslogs:

- Configure trap and syslog receivers for endpoints in call processors.
- Enter the Cisco Prime CM IP address to configure the trap receiver: <PrimeCM_ip_addr>
- Enter the Cisco Prime CM IP address and port number 20514 to configure syslog receiver.: <PrimeCM_ip_addr>:20514.
- Enable endpoints to send traps and syslogs.

To enable traps:

- In CISCO-TELEPRESENCE-MIB, set ctpPeripheralErrorNotifyEnable to true (1)
- In CISCO-TELEPRESENCE-CALL-MIB, set ctpcStatNotifyEnable to true (1)
- In CISCO-TELEPRESENCE-CALL-MIB, set threshold values for call stats ctpcStatMonitoredEntry

To enable syslogs: In CISCO-SYSLOG-MIB, set clogNotificationsEnabled to true (1).

Preparing Call Scheduling and Calendaring

Preparing Cisco TelePresence Management Suite

HTTP and SNMP access are required 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 successfully monitor Cisco TMS.

Enable SNMP

By default, **public** and **Public** are enabled as SNMP Read Only (RO) community strings for Cisco TMS. This string is used by Cisco TMS to poll other devices.

If you need to add or change these strings:

Go to the web GUI and navigate to **Administrative Tools > Configuration > Network Settings** and change the SNMP settings.

In addition to the Web GUI, SNMP service on the Cisco TMS server must be enabled.

To enable SNMP:

1. Go to **Start** on the server console.
2. Click **Run** and specify services.msc.
   A Service window will pop open on the server console.
3. Right-click **SNMP Service** and select **Properties**.
4. Click **Security** and select **Add new SNMP** string.
   Do not modify the default selection: Accept SNMP packets from any host unless you want only specific hosts polling SNMP from Cisco TMS.
5. Optionally, click **Traps** to add the IP address of Cisco Prime Collaboration Manager and a community string. This address is used in SNMP traps.
6. Optionally, click **Agent** to specify SNMP contact and location for Cisco TMS. The Cisco Prime Collaboration Manager uses this information to display the location of Cisco TMS in the inventory.
7. Restart the **SNMP Service** after the necessary modifications.

Configuring Reporting API for CTS-Manager 1.8

For Cisco Prime CM server to retrieve scheduled meetings from from CTS-Manager 1.8, you must have a valid Metrics Dashboard and Reporting API license in CTS-Manager. This user account should be configured in Active Directory with a mailbox and in a user group with general security. The Active Directory user group should be assigned the **Reporting API** role and the **Live Desk** role in the CTS-Manager Access Management page.

```
Note:
We recommend that you review the Getting Started With TelePresence Reporting API
document available at [http://developer.cisco.com/web/tra/start] for an understanding
of the Reporting API.
```

To enable Cisco Prime CM server to retrieve scheduled meetings from from CTS-Manager 1.8:

1. In the LDAP server, create a user group. For example,create a group named cm_group.
2. In the group that you created in the LDAP server, create a user. For example, create a user named cm_user.
   You must ensure that a valid mailbox is configured for the user created in the group in the LDAP server.
3. In CTS-Manager, in the **Access Management** page, assign the **Live Desk** role and the **Reporting API User** role for the group you created in the LDAP server, for example, cm_group created in *Step 1*.
4. Discover the CTS-Manager in Cisco Prime CM with the user that you created in the LDAP server. For example, use cm_user.

For more information about the Reporting API, see *Cisco Telepresense Manager Reporting API Developer's Guide for Release 1.8.*

For more information about user and group configuration in LDAP server, see *Cisco Telepresense Manager 1.8 Administration and Installation Guide*.

```
Note:
After creating the user account in CTS-Manager for the Prime CM application, we recommend
that you log in with this account in CTS-Manager at least once before you enter the
credentials in the Prime CM server.
```

Configuring Cisco TMS Third Party Booking API User

For the Cisco Prime CM server to retrieve scheduled meetings from Cisco TMS server 13.0 and Cisco TMS server 13.1, you must have one Application Integration License for each server that uses the API.

```
Note:
*We recommend that you review the Cisco TMS Third Party Booking API document available
at [http://www.tandberg.com/support/tms_documentation.jsp] for an understanding of the
Booking API.

*For Cisco TMS 13.2 and later, any HTTP user can be used to retrieve scheduled meetings
from Cisco TMS server. In addition, you do not need to install a Booking API License to
use the API.
```

To enable Cisco Prime CM server to retrieve scheduled meetings from Cisco TMS:

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

The RemoteSetupService page appears. You may replace localhost in the above URL with the IP address of the Cisco TMS server.

2. Choose **GenerateConferenceAPIUser**.
3. Enter the values for the following parameters:
    - userNameBase - The base portion of the user name. For example, cpcm_user.
    - encPassword - A base64 encoded password that is to be 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 email address of the user. Do not enter values in this field.
    - sendNotifications - To allow the user to receive scheduling notifications. You must enter False in this field since Cisco Prime CM will be polling from Cisco TMS.
4. Click **Invoke**.
5. In the Cisco TMS application, verify the user name configured in Step 3is listed in the Users page.
6. In the Cisco TMS application, create a user group. For example, create a group named cm_group.
7. Add the user created in Step 3to the group created in Step 6. For example, add cm_user to cm_group.
8. In the **Groups** page, for the group created in Step 6, check the Read permission check box for List Conferences-All (under the Booking pane). For example, cm_group must have the read permission to List Conferences-All.
9. Discover the Cisco TMS in Cisco Prime CM with the user that you created in Step 3. For example, use cm_user.

For more information about the Cisco TMS, see the documents available at TANDBERG site.

For more information on creating groups and setting permission to the group, see *Ciso Telepresence Management Suite Administrator Guide*.

Configuring MCUs

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 a blank space (no password). If you cannot log in to the web GUI, 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:

1. Navigate to **Network > SNMP**.
2. Edit the SNMP Read Only and Read Write strings as required.

3. Click **Update SNMP Settings** to apply the changes.

Configuring Cisco TelePresence Multipoint Switch

Enable HTTP

A separate HTTP user account must be created with the Meeting Scheduler and Diagnostic Technician roles assigned to it for the Prime CM application. 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) 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 (navigate 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.

The following SNMP settings are 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 SNMP Read and Read/Write community strings.
After creating the user account in CTMS for the Prime CM application, we recommend
that you log in with this account in CTMS at least once before you enter the
credentials in the Prime CM server.
```

Configuring Cisco Mediatrace, Cisco IOS IP SLA, and Performance Monitoring for Network Devices

If you have enabled Cisco Mediatrace on your network nodes, Cisco Prime CM provides Medianet Path View as part of the troubleshooting data. If you have enabled Cisco IOS IP Service Level Agreements (SLAs) on your network nodes, you can measure the network performance and health using the Proactive Troubleshooting feature.

For Cisco Mediatrace:

- Enable the initiator and/or responder roles on relevant routers and switches using the following commands:
  For Mediatrace Initiator:

```
mediatrace initiator source-ip ''IP Address''
```

For Mediatrace Responder:

```
mediatrace responder
```

- Configure a Telnet local login user with privilege 15 on the initiators.
- Configure Web Services Management Agent (WSMA) over HTTP or HTTPS on the initiators. See *Web Services Management Agent (WSMA) Configuration Guide* for details on the configuration commands.

Local Auth Example:

```
username <username> priv 15 secret <username_enable_password>
ip http authentication local
```

For WSMA (HTTP) Configuration:

```
ip http 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
```

For WSMA (HTTPS) Configuration:

```
ip http secure-server
wsma agent exec profile wsma_listener_https
wsma agent config profile wsma_listener_https
!
wsma profile listener wsma_listener_https
transport https
```

For WSMA SSH Configuration:

```
crypto key generate rsa
ip ssh timeout 120
ip ssh version 2
```

```
!
wsma agent exec profile wsma_listener_ssh
wsma agent config profile wsma_listener_ssh
!
wsma profile listener wsma_listener_ssh
transport ssh
```

For Cisco IOS IP Service Level agreement (SLA):

- Enable the responder role using the command:

```
ip sla responder
```

- The initiator role is not required.
- Configure a Telnet local login user with privilege 15 on the IP SLA initiators.

You can verify whether these roles are enabled on the device by using Cisco Prime CM Inventory (Inventory > Device Inventory> Current Inventory table).

For Performance Monitoring (PM) Configuration:

Configure the Performance Monitor policy on the relevant interfaces. Cisco Prime CM collects PM flow statistics through MIBs. If this is configured, Cisco Prime CM does not require the CLI access to routers.

For a list of supported server time zones, see Supported Time Zones for Prime Collaboration Manager.