



Setting up Devices for Cisco Prime Collaboration Assurance

Published On: April 17, 2019

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

Required Protocols for the Devices

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

- 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 from the Cisco Unified CM.
- MSI - Obtain Mediatrace information, discover media path, and collect statistics for the various midpoints.
- CDP - Discover neighboring devices.

Note: For supported software versions, see [Supported Devices for Cisco Prime Collaboration Assurance](#).

Device	SNMP	HTTP	CLI	JTAP	MSI	CDP	Notes
Analog Gateway	Yes	–	–	–	–	–	
Unified Contact Center Enterprise	Yes	Yes	–	–	–	–	If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure HTTP credentials for Unified CCE along with SNMP. You must enter the HTTP credentials in the following format when you add Unified CCE in the Cisco Prime Collaboration Assurance user interface: domain\administrator. For example hcsdc2\administrator.
Cisco Unified Intelligence	Yes	Yes	–	–	–	–	If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure

Center							HTTP credentials for Cisco Unified Intelligence Center along with SNMP.
Cisco SocialMiner	Yes	Yes	–	–	–	–	If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure HTTP credentials for Cisco SocialMiner along with SNMP.
Unified Contact Center Express	Yes	Yes	–	–	–	–	If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure HTTP credentials for access to Cisco Unified Serviceability (not CCX Serviceability).
Cisco TelePresence Multipoint Switch	Yes	Yes	–	–	–	–	The HTTP user account must have both the Meeting Manager and Diagnostic Technician roles.
Cisco TelePresence System (CTS)	Yes	–	Yes	–		–	<ul style="list-style-type: none"> ■ Requires the Reporting API license and the Reporting API role for the Cisco Prime Collaboration user. ■ The HTTP user needs to be an exchange mailbox user and its User Group must have Reporting API and Live Desk roles in CTS-Manager. ■ If you have installed a licensed version of Prime Collaboration, it is mandatory to configure the CTS-Manager Reporting API. If this feature is not configured on the CTS-Manager 1.7, 1.8, or 1.9, Prime Collaboration will not manage the CTS-Manager.
Cisco Unified CM	Yes	Yes	–	Yes	–	–	<ul style="list-style-type: none"> ■ Cisco Prime Collaboration supports Cisco Unified CM clusters. You must ensure that the cluster IDs are unique. To verify the cluster ID go to the Enterprise Parameters Configuration page (System >

							<p>Enterprise Parameters) on Cisco Unified CM publisher (for every cluster).</p> <ul style="list-style-type: none"> ■ The same credentials must be created for all devices in the cluster whenever clustering is used. ■ The JTAPI user needs to have these roles Standard AXL API Access, CCM Admin Users, SERVICEABILITY Administration, CTI Enabled, and CTI Allow Call Monitoring. ■ The session monitoring feature is supported only from Cisco Unified CM 8.5 release onwards.
Cisco Unified Communications Manager Business Edition	Yes	Yes	–	Yes	–	–	
Cisco Unified Customer Voice Portal	Yes	Yes	–	–	–	–	<p>If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure HTTP credentials for Cisco Unified Customer Voice Portal along with SNMP. You must enter the HTTP credentials for Cisco Unified Customer Voice Portal (CVP) which have the <i>ServiceabilityAdministrationUserRole</i> privileges. The default username <i>wsmadmin</i> has this privilege.</p>
<ul style="list-style-type: none"> ■ Cisco Codec EX series ■ Cisco TelePresence System Integrator C Series ■ Cisco 							

<p>TelePresence MX Series</p> <ul style="list-style-type: none"> ▪ Cisco Collaboration Endpoint Software for DX70, DX80 Series ▪ Cisco TelePresence System Profile Series ▪ Cisco TelePresence SX20 Quick Set ▪ Cisco TX 9000 series ▪ Cisco TelePresence MX700 and MX800 (supported by Cisco Prime Collaboration Assurance 10.5.1 and later versions) ▪ Cisco 	<p>Yes</p>	<p>Yes</p>	<p>Yes</p>	<p>–</p>	<p>Yes</p>	<p>–</p>	<ul style="list-style-type: none"> ▪ The HTTP user requires Admin privilege. ▪ For TC 6.0 and TE 6.0, use the same HTTP credentials for MSI. ▪ For TX 6.0, use the default credentials msiuser and cisco for MSI.
--	------------	------------	------------	----------	------------	----------	--

<p>TelePresence MX300 G2 and MX200 G2 (supported by Cisco Prime Collaboration Assurance 10.5.1 and later versions)</p> <ul style="list-style-type: none"> ▪ Cisco TelePresence SX10 and SX80 (supported by Cisco Prime Collaboration Assurance 10.5.1 and later versions) 							
Emergency Responder	Yes	–	–	–	–	–	
Expert Advisor	Yes	–	–	–	–	–	
Finesse	Yes	Yes	–	–	–	–	If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure HTTP credentials for Cisco Finesse along with SNMP.
Cisco MCU	Yes	Yes	–	–	–	–	<ul style="list-style-type: none"> ▪ The HTTP user requires Admin privilege. ▪ This device also include the MSE8000 blade form factors:

							MSE-8420, MSE-8510, and MSE-8710.
Cisco TelePresence MSE Supervisor	Yes	Yes	–	–	–	–	The HTTP user requires Admin privilege.
Mediasense	Yes	Yes	–	–	–	–	If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure HTTP credentials for Cisco MediaSense along with SNMP.
Meeting Place	Yes	–	–	–	–	–	
Meeting Place Express	Yes	–	–	–	–	–	
Personal Assistant	–	–	–	–	–	–	
Cisco TelePresence System MXP series	Yes	Yes	Yes				
Cisco Unified Presence	Yes	Yes	–	–	–	–	End-to-end troubleshooting is not supported. However, the path trace can be discovered from the first-hop-router (FHR) if router CLI access is provided for Cisco Prime Collaboration.
Network devices (routers and switches)	Yes	–	Yes	–	–	Yes	<ul style="list-style-type: none"> ■ CDP needs to be enabled for the video Troubleshooting workflow. The Telnet or SSH access is required for Cisco Medianet features, which is part of the video Troubleshooting workflow. ■ See the table <i>Supported Software Versions for the Cisco Medianet Feature</i> below to view the troubleshooting Medianet-related data.
							<ul style="list-style-type: none"> ■ Requires Booking API license (TMS software version 13.1 or below). ■ The HTTP user for Cisco Prime Collaboration needs to be generated through the Booking

<p>Cisco TelePresence Management Suite (Cisco TMS)</p>	<p>Yes</p>	<p>Yes</p>	<p>–</p>	<p>–</p>	<p>–</p>	<p>–</p>	<p>API on the Cisco TMS windows server.</p> <ul style="list-style-type: none"> ■ Cisco Prime Collaboration supports only the default e-mail template for the Booking Confirm e-mail in Cisco TMS. The session import feature will not work, if the default e-mail template is not used.
<p>Cisco Telepresence Server Cisco Telepresence Server on Virtual Machine (supported by Cisco Prime Collaboration Assurance 10.5.1 and later versions) Cisco TelePresence Server on Multiparty Media 310 and 320 (supported by Prime Collaboration Assurance 10.5.1 and later versions)</p>	<p>–</p>	<p>Yes</p>	<p>–</p>	<p>–</p>	<p>–</p>	<p>–</p>	<ul style="list-style-type: none"> ■ The HTTP user account should have the API Access privilege. ■ This device also include the MSE8000 blade form factors: MSE-8420, MSE-8510, MSE-8710.

Cisco Meraki MX70 and MX80	–	Yes	–	–	–	–	
Cisco Telepresence Conductor	Yes	Yes	–	–	–	–	
Cisco Unity	Yes						
Cisco Unity Connection	Yes	Yes					
Cisco Unity Express	Yes	–	–	–	–	–	
Cisco TelePresence Video Communication Server (Control and Expressway)	Yes	Yes	–	–	–	–	The HTTP user requires Admin privilege.
Wireless	Yes	–	Yes	–	–	–	
Third party devices	Yes	–	–	–	–	–	
Cisco IP phones (89xx, 99xx)	–	–	–	–	–	–	<ul style="list-style-type: none"> ■ The Cisco IP Phones endpoints are discovered through Cisco Unified CM. You must enable web access in Cisco Unified CM for these. ■ These video phones require Cisco Unified CM application user to have the additional role <i>Standard CTI Allow Control of Phones supporting Connected Xfer and conf.</i> ■ Credentials are not required for HTTP access. ■ End-to-end troubleshooting is not supported. However, the path trace can be discovered from the first-hop-router (FHR) if router CLI access is provided for Cisco Prime Collaboration.
							<ul style="list-style-type: none"> ■ The Cisco Phone endpoints are

Cisco Android-Based Firmware for DX70 and DX80 (supported by Prime Collaboration Assurance 10.5.1 and later versions)	-	-	-	-	-	-	<p>discovered through Cisco Unified CM. You must enable web access in Cisco Unified CM for these.</p> <ul style="list-style-type: none"> ■ These phones require Cisco Unified CM application user to have the additional role Standard CTI Allow Control of Phones supporting Connected Xfer and conf. ■ Credentials are not required for HTTP access. ■ End-to-end troubleshooting is not supported. However, the path trace can be discovered from the first-hop-router (FHR) if router CLI access is provided for Cisco Prime Collaboration.
Border Element, Virtual Border Element, Gatekeeper, H323 Gateway, SIP Gateway, MGCP Gateway, SRST Device, Voice Gateway	-	-	-	-	-	-	

Configuring Call Controllers and Processors

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.

Note: The procedures described below are applicable for Cisco Unified CM 10.x. If you are using any other supported versions, see the [Cisco Unified CM guides](#) to understand how to create groups, users and assign roles to them.

Enable HTTP

You do not have to create a new user if you want to allow Cisco Prime Collaboration 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 can use to communicate.

To create a user:

1. Log in to the Cisco Unified CM Administration web interface using the administrator role.
2. Create a user group with sufficient privileges. Choose User Management > User Settings > Access Control Group and create a new user group with a suitable name, PC_HTTP_Users in this case. Now, click Save.
3. Choose User Management > User Settings > Access Control Group and click Find. Find the group you defined and click on the  icon on the right.
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, choose 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 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 (for example, PC_HTTP_Users).
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, choose 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.
6. Also make sure the Call Manager SNMP Service is running.

Start the CTI Service

Perform the following procedure for call processing Unified Communications Manager publishers or subscribers

1. Log in to the Cisco Unified Serviceability view in the Cisco Unified Communications Manager graphical user interface.
2. Choose Tools > Control Center - Feature Services.
3. Select a server from the drop-down list.
4. From the CM Services section, check the Cisco CTIManager check box.
5. Click Start.

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

To create a new JTAPI user (Non-Secure JTAPI Connection):

1. Log in to the Cisco Unified CM Administration web interface using administrator role.
2. Create a user group with sufficient privileges. Choose User Management > User Settings > Access Control Group and create a new user group with a suitable name, PC_HTTP_Users in this case. Now, click Save.
3. Choose User Management > User Settings > Access Control Group and click Find. Find the group you defined and click on the *i* icon on the right.
4. Click Assign Role to Group and select the following roles:

- a. Standard CTI Allow Call Monitoring
 - b. Standard CTI Enabled
 - c. Standard CTI Allow Control of Phones supporting Connected Xfer and conf.
5. Click Save.
 6. From the main menu, choose 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 to monitor all devices.
Note: The password must not contain a semicolon (;) or equals (=).
 7. In the Permission Information section, click Add to Access Control Group and select the group that was created in step 1. (for example, PC_HTTP_Users).
 8. Click Save. The page is refreshed and the right privileges are displayed.

To create a new JTAPI user (Secure JTAPI Connection):

Note:

*Ensure the following services are activated and started:

- **Cisco CTIManager
- **Cisco AXL Web Service
- **Cisco Tftp
- **Cisco Certificate Authority Proxy Function

See the Cisco Unified Communications Manager guide for details about how to configure the application user.

For Cisco Prime Collaboration Release 11.6 and earlier

1. You can access the log files to verify whether the endpoints are assigned with the CTI-controlled roles in the Unified CM and for the JTAPI-related issues using <https://<primecollaboration-ip>/emsam/log/SessionMon/CUCMJTAPIDdiag.log>.
2. Ensure that CUCM is in Mixed Mode.

1. Log in to the Cisco Unified CM Administration web interface using administrator role.
2. Create a user group with sufficient privileges. Choose User Management > User Settings > Access Control Group and create a new user group with a suitable name, PC_HTTP_Users in this case. Now, click Save.
3. Choose User Management > User Settings > Access Control Group and click Find. Find the group you defined and click on the i icon on the right.
4. Click Assign Role to Group and select the following roles:

- a. Standard CTI Allow Call Monitoring
 - b. Standard CTI Enabled
 - c. Standard CTI Allow Control of Phones supporting Connected Xfer and conf
 - d. Standard CTI Secure Connection (This is applicable only if you are planning to enable Secure JTAPI for CUCM clusters).
5. Click Save.
 6. From the main menu, choose 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 to monitor all devices.
Note: The password must not contain a semicolon (;) or equals (=).
 7. In the Permission Information section, click Add to Access Control Group and select the group that was created in step 1. (for example, PC_HTTP_Users).
 8. Click Save. The page is refreshed and the right privileges are displayed.
 9. Create a new application user CAPF profile associate it to the JTAPI user with a unique Instance ID. For more information, see the section on [“Certificate Authority Proxy Function”](#) in the [“Security Guide for Cisco Unified Communications Manager”](#).

Configure CDR (Add Prime Collaboration Assurance as a Billing Server)

You can monitor Call Detail Record (CDR) trunk utilization on your Unified CMs using Prime Collaboration Assurance. Ensure that the Unified CM publisher is discovered successfully and in Managed state in Prime Collaboration before you add Prime Collaboration as a billing server. To verify, check if the Unified CM publisher is listed under the Call Quality Data Source Management page (Administration > System Setup > Assurance Setup > Call Quality Data Source Management) in the Prime Collaboration UI. To monitor CDR-based trunk data using Prime Collaboration Assurance:

1. Log in to the Cisco Unified CM Administration web interface.
2. Choose System > Service Parameters. The Service Parameters Configuration page appears.
3. Select your CUCM server (the Publisher node) and the Cisco CallManager service.
4. 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.

5. To add Prime Collaboration as a billing server, you must ensure Prime Collaboration is up and running.
 1. Launch Cisco Unified Serviceability.
 2. Choose Tools > CDR Management.
 3. Scroll down to Billing Applications Server Parameters and click Add New.
 4. Enter the following:
 - Host Name / IP Address—Enter the IP address of the system where Prime Collaboration Assurance is installed.
 - User Name—Enter *smuser*.
Note: Do not enter any username other than *smuser*.
 - Password—Enter a password. The default password is *smuser*. To change this password:
 - Change it in Prime Collaboration Assurance first.
 - Enter the same password that you entered for *smuser* while configuring other settings in Prime Collaboration Assurance.

Note: If you changed the password in Prime Collaboration Assurance and Unified Communications Manager does not immediately accept the new password, wait one minute and enter the new password again.

- Protocol—Select SFTP Protocol.
- Directory Path—Enter */home/smuser/*.
Note: Do not enter any directory path other than */home/smuser*.
- Resend on Failure—Select this check box.

5. Click Add.

Note: In some cases, for CDR/CMR files to be delivered to a newly added billing server, it is necessary to first restart the CDR Repository Management Service.

1. From Cisco Unified Serviceability, choose Tools > Control Center - Network Services.
2. From the list of Unified Communications servers, select the publisher.
3. Scroll down to CDR Services.
4. Select the Cisco CDR Repository Manager radio button.
5. Click the Restart button.

Change the Password for smuser

The SFTP password for *smuser* in Prime Collaboration and the password for the Application Billing Server *smuser* in Cisco Unified Communications Manager must be identical. Any time you change one, you must change the other to match.

Use this procedure to change the password for the Application Billing Server smuser in Cisco Unified Communications Manager.

1. Log in to the Cisco Unified Serviceability view in the Cisco Unified Communications Manager web GUI.
2. Choose Tools > CDR Management.
3. Scroll down to Billing Application Server Parameters and double-click the link for Prime Collaboration. Enter a new password. If you changed the password in Prime Collaboration and Cisco Unified Communications Manager does not immediately accept the new password, wait one minute and enter the new password again. Do not change the values in any other fields; Host Name / IP Address, User Name, SFTP Protocol, and Directory Path must remain the same.
4. Click Update.

Activate the AXL Web Service

Perform this procedure for Unified Communications Manager versions.

1. Launch Cisco Unified Serviceability.
2. Choose Tools > Service Activation.
3. Select a server.
Note: Activate the AXL Web Service on the Publisher node.
4. Scroll down to Database and Admin Services and select Cisco AXL Web Service.
5. Click Save.

Start the RIS Collector Service

Perform this procedure for Unified Communications Manager versions.

1. Log in to the Cisco Unified Serviceability view in the Cisco Unified Communications Manager web GUI.
2. Choose Tools > Control Center - Network Services.
3. Select a server.
4. Select Cisco RIS Data Collector Service from Performance and Monitoring pane.
5. Click Start.

Configuration for CVTQ Data

For Prime Collaboration Assurance to obtain CVTQ data from a Unified Communications Manager, you first need to perform configuration tasks while logged in to Unified Communications Manager.

You might also need to perform some additional configuration on H.323 and SIPs gateways if voice activity detection (VAD) is enabled on them so that MOS is calculated properly and, therefore, reported correctly in CDRs.

Set Unified Communications Manager Service Parameters

Note: Set these parameters on each Unified Communications Manager in a cluster.

1. Log in to Unified CM Administration.
2. Choose System > Service Parameters. The Service Parameters Configuration page appears.
3. Select the server and the service:
 1. Select the name of the Unified Communications Manager server. This is a Unified Communications Manager from which Prime Collaboration Assurance will gather data.
 2. Select the Unified Communications Manager service.
4. Set these parameters:
 1. CDR Enabled Flag—Scroll down to System. Set to True.
 2. Call Diagnostics Enabled—Scroll down to Clusterwide Parameters (Device - General). Set to Enable Only When CDR Enabled Flag is True.

Note: It is recommended that you ensure that Call Diagnostics Enabled is set to Enable Only When CDR Enable Flag is True on the publisher and on each of the subscribers.
5. Click Update.

Caution: Do not enable the CDR Log Calls With Zero Duration Flag service parameter. Enabling it can adversely affect Prime Collaboration Assurance (and CDR Analysis and Reporting). Resources spent processing numerous zero-duration call records can take away from the number of non-zero-duration calls that Prime Collaboration Assurance can process.

Set Unified Communications Manager Enterprise Parameters

1. Log in to Unified CM Administration.
2. Choose System > Enterprise Parameters. The Enterprise Parameters Configuration page appears.
3. Select the Cluster ID. If the cluster ID is already present Prime Collaboration Assurance, change it.

Note: Each cluster that you add to Prime Collaboration Assurance must have a unique cluster ID.

4. Scroll down to CDR Parameters and set CDR File Time Interval to 1.
5. Click Update.

Configure Voice Gateways when VAD is Enabled

Enabling voice activation detection (VAD) can save bandwidth, but it can also impact Prime Collaboration Assurance MOS calculations for CVTQ reports and might cause noticeable or unacceptable clipping of words. VAD is enabled by default in Cisco IOS voice (under dial peer configuration), and disabled by default in Unified Communications Manager (under System > Service Parameters).

When VAD is enabled on a voice gateway in a cluster, you can see lower MOS values in CVTQ reports for calls between the voice gateway and a Cisco Unified IP Phones. You need to:

- Configure the comfort noise payload type to 13 (from the default of 19) on H.323, SCCP, and SIP gateways. Doing so enables Cisco Unified IP Phones and voice gateways to properly adjust the MOS calculation.

Note: Sensors calculate MOS correctly for voice gateways when VAD is enabled.

- Be aware that low MOS will be reported for calls between Cisco Unified IP Phones and MGCP gateways on CVTQ reports. (Comfort noise payload type is not configurable on MGCP gateways.)

Note: Call Management Record (CMR) data will not be available in Prime Collaboration Assurance for Cisco Unified Border Element (CUBE), because Unified Communications Manager does not support CMR for SIP trunks.

Activate Enterprise License Management Resource API

Whenever the ELM and Unified CM co-resides, the service in Unified CM which provides the REST API to get license data needs to be activated manually.

1. SSH to Unified CM.
2. Enter the command.

If the license server is Enterprise License Manager:

```
license management service activate Cisco ELM Resource API
```

If the license server is Prime License Manager:

```
license management service activate Cisco Prime LM Resource API
```

After the configuration, the following message will be displayed:

```
Activating <License_Server> Resource API completed successfully
```

Configure Syslog Receiver

To successfully receive Cisco Unified Communications Manager syslog messages, you must add the syslog receiver from the device's serviceability web page. **Event Monitoring Service**

1. On your Cisco Unified Communications Manager, select Cisco Unified Serviceability from the Navigation pull-down in the top-right corner of the device's home screen.
2. Choose Alarm > Configuration.
Caution: Do not use the Unified CM enterprise service parameter to configure the syslog receiver for Prime Collaboration syslog integration. When the enterprise parameter is enabled, all syslog messages (with matching severity levels) are sent regardless of whether or not they are intended to be processed by Prime Collaboration.
3. Select Service Group and Service options based on the following table:
 - Service Group > CM Services > Service > Cisco CallManager
 - Service Group > CDR Service > Cisco CDR Agent
 - Service Group > CDR Service > Cisco CDR Repository Manager
 - Service Group > Database and Admin Services > Cisco Database Layer Monitoring
 - Service Group > Database and Admin Services > Cisco License Manager
 - Service Group > Performance and Monitoring Services > Cisco AMC Service
 - Service Group > Backup and Restore > Cisco DRF Master
 - Service Group > Backup and Restore > Cisco DRF Local

Note: If you are using Prime Collaboration 10.5 and later, you need to add the syslog receiver for CM Services (Service Group > CM Services > Service > Cisco CallManager) only.

1. Click on the Enable Alarm check box, select Alarm Event Level to "Error" for all listed services except for Cisco CallManager and Cisco License Manager, which should be set to "Informational" level..

2. Check Apply to All Nodes and click Save.

Note: Syslog messages have a limitation of 1,024 characters (including the heading). Any syslog-based event details may not contain the full information because of this syslog limitation. If the syslog message exceeds this limit, it is truncated to 1,024 characters by the syslog sender.

Exchange the Prime Collaboration Assurance and MSI Highgate Certificates

This procedure is for one Cisco Unified Communications Manager cluster for which you want to use the PCA-MSI Highgate feature. To use this for another CUCM cluster you need to repeat the procedure. Ensure that this task is completed after you have set up the server and have not managed the CUCM. To add the certificate for a CUCM already maintained in inventory or for a newly-added cluster, you have to restart the PC server.

Exchange the Prime Collaboration Assurance Self Signed Certificate

Download the Prime Collaboration Self Signed Certificate

Download the `primecollab-cer.cer` file from the Prime Collaboration server to your local system using an SFTP client for example Filezilla. The path is as follows: `/opt/emms/emsam/conf/msi_ca_certs/ primecollab-cer.cer`

Add the Prime Collaboration Self Signed Certificate to the Cisco Unified Communications Manager Publisher

1. Log in to the Cisco Unified CM OS Administration portal.
2. Click Security > Certificate Management.
3. In the Certificate page, click on the Upload Certificate/ Certificate chain button.
4. In the Upload Certificate/ Certificate chain dialog box, select the following:
 - a. Certificate: tomcat-trust
 - b. Description: You can add a reference description.
 - c. Browse: Add the certificate (`primecollab-cer.cer`) from the following path: `/opt/emms/emsam/conf/msi_ca_certs/ primecollab-cer.cer`
5. Click the Upload File button. A message notifies you that the certificate upload task is a success.

Exchange the Cisco Unified CM CAPF Certificate

Download the CAPF certificate from Cisco Unified Communications Manager

1. Log in to Cisco Unified CM OS Administration portal.
2. Click Security > Certificate Management.
3. **Search for keyword “CAPF” to find the CAPF.pem file.** Note: The keyword is case sensitive.
4. In the search results, click on the file CAPF.pem. The Certificate Configuration page appears.
5. Click the Download button. A dialog box appears prompting you to save the file on the local system.

Add the CAPF Certificate from Cisco Unified Communications Manager to Prime Collaboration Assurance

Add the CAPF.pem file using an SFTP client for example Filezilla to the following directory:

/opt/emms/emsam/conf/msi_ca_certs/ CAPF.pem

Standalone Enterprise/Prime Licensing Manager

Troubleshooting Enterprise/Prime Licensing Manager

Credential Verification

PLM access can be tested to verify access and credentials:

- Testing URL: <https://<plmIP>/elm-resources>

Verify Credentials using login request

- **Note:** If no Credentials appear to work, attempt use of the Credentials used to access the PLM CLI

PLM is listed as Non-Cisco Device

If PLM is listed as a non-cisco Device in the PCA Device Work Center the following Steps that can be performed:

1. Change PLM to a suspended state in the PCA Device Work Center
2. Delete PLM in the PCA Device Work Center
3. Delete the PLM Credential Profile in the Credential Manager Menu
4. Build a new PLM Credential Profile in the Credential Manager Menu after ensuring Credential Information.
5. Perform a Logical Discovery using PLM's IP as the seed IP for the discovery
6. Perform a Cluster Data Discovery once PLM is listed in a "Managed" State in the Device Work Center

Cisco Unity Connection HTTP User Role

HTTP User Role

You do not have to create a new user if you want Cisco Prime Collaboration to use administrator credentials to log in. Alternatively, if you want Cisco Prime Collaboration Manager to use the right credentials to log in to Cisco Unified Connection, you must create a new HTTP user group and a corresponding user that Cisco Prime Collaboration can use to communicate.

Note: Before you add user accounts manually, you must select and define a template and class of service (COS) for each type of account that you want to add. For administrator accounts, you must also select the roles that are assigned to each account.

To create a user:

1. Log in to the Cisco Unity Connection Administration window using the administrator role.
2. In the left pane, expand Users, then click Users.
The Search Users window appears.
3. Select the applicable user account.
The Edit User Basics window appears.
4. Choose Edit > Roles.
5. On the Edit Roles window, in the Available Roles field, select Remote Administrator and System Administrator.
6. Select the Up arrow to move it to the Assigned Roles field.
7. Click Save.

You can log in to both the Cisco Unity Connection Administration and the Cisco Unity Connection Serviceability windows by using the same credentials.

Configure Syslog Receiver

To successfully receive Cisco Unity Connection syslog messages, you must add the syslog receiver from the **device's serviceability web page**. To configure syslog receiver on Cisco Unity Connection:

1. On your Cisco Unity Connection, select Cisco Unity Connection Administration from the Navigation drop-down in the **top-right corner of the device's home screen**.
2. Choose System Settings > Enterprise Parameters.
3. Go to Cisco Syslog Agent section and update the following required fields:
 - Remote Syslog Server Name with the IP address of *Prime Collaboration Assurance*.
 - Select *Informational* from the drop-down menu for Syslog Severity For Remote Syslog Messages.
4. Select Cisco Unity Connection Serviceability from the Navigation drop-down in the **top-right corner of the device's home screen**.
5. Choose Alarm > Configurations.

Select the correct alarm configuration elements for your particular machine:

- For Unity Connection 8.x:
 - Enable Informational Alarms for Local syslogs
 - Enable Informational Alarms for Remote Syslogs and enter the Server name as Prime Collaboration Assurance Server IP address
- 6. Click Save to save the configuration to complete syslog configuration.

Configure the Unity Event Monitoring Service

The Event Monitoring Service (EMS) should already be installed along with the Remote Serviceability Kit.

Configure the Event Monitoring Service to support these Unity events in Prime Collaboration Assurance:

- OutOfDiskSpace
- HardDiskError
- ExchangeLoginFailed

To configure the Event Monitoring Service:

- Open the Tools Depot on the Desktop and choose Diagnostic Tools > Event Monitoring Service.
- Double-click to run.
- Create a recipient to receive notifications by selecting File > New > Recipient, or select the Recipients node in the navigation tree and click Create New Recipient.
- Enter a Recipient Name to identify a single recipient (or a group as there can be multiple E-mail addresses under SMTP).

- Select the desired notification method tabs.
 - The SNMP trap tabs works with the Remote Serviceability Kit to send traps to a destination (defined under windows SNMP service properties).
 - The Syslog tab allows entry of a Syslog server address for the event.
 - The failover tab is not a notification, but can force a failover upon receipt of a specified event. The Test button at the top of the page sends a test event to the defined recipients. These can be:
 - Event Source: EMSTest
 - Event ID:10001
 - Description: Event Monitoring Service Test Message
- Create a monitored event by selecting File > New > Event, or select the Monitored Events node in the navigation tree and click Create New Event.

If the event exists currently in the Windows Event Viewer, to populate the event information in the Add New Event dialog:

- Select the event in Windows Event Viewer.
- Select Copy Event to Clipboard.
- Use Import Event From Clipboard in the Add New Event dialog.

To manually add the event:

1. Select Event Source from the pull-down menu
2. Select a specific Event ID and enter the desired ID. All Event IDs could also be used to obtain all events from a specified event source.
3. Select Type to filter what level notifications should be sent for.
4. Select Errors, Warnings, and Informational for all level events or if the Type is unknown.
5. Enter Notes that will be included with the notification, such as troubleshooting steps.

The content section allows you to record a custom WAV for the event used along with the Recipient Voicemail option.

The Email Subject and Body can be used to customize the formatting of the messages sent to Recipient Email and SMTP notification methods. If no customization is desired, leave default fields as is.
6. Select OK after adding the new event.

To activate the new event, one or more Recipients need to be added to it.

1. Select the newly added event and click on the Add Recipients icon. The Recipients and notification methods can be further defined with check boxes here.

2. Check the Active check box and Apply to activate the event.

You may also perform this step from the Monitored Events node in the navigation tree.

You can also exclude or ignore events that pass the other criteria by selecting File > New > Exclusion, or select the Exclusions node in the navigation tree and click Create New Exclusion.

If the event exists currently in the Windows Event Viewer, you can populate the event information in the Add Exclusion dialog by selecting the event in Windows Event Viewer and clicking Copy Event to Clipboard. Then use Import Event From Clipboard in the Add Exclusion dialog.

To manually exclude the event:

1. Select the event Source from the pull-down.
2. Select Specific Event ID and enter the desired ID. All Event Ids could also be used to obtain all events from a specified event Source.
3. Select OK when finished adding the new exclusion.

Cisco Unified Presence

Configure Syslog Receiver

To successfully receive Cisco Unified Presence syslog messages, you must add the syslog receiver from the **device's serviceability web page**. To configure syslog receiver on Cisco Unified Presence

1. On your Cisco Unified Communications Manager IM and Presence, select Cisco Unified IM and Presence Serviceability from the Navigation drop-down in the **top-right corner of the device's home screen**.
2. Choose Alarm > Configurations.
3. Select the correct alarm configuration elements (Server, Service Group, and Service) for your particular machine and then click Go. For example:
 - Enter the Prime Collaboration Assurance server name/address in Server text box.
 - Select CUP Services in the Service Group.
 - For Remote Syslogs, select Enable Alarms and set the Alarm Event Level to Informational.
4. Click Save to save the configuration to complete syslog configuration.

Media Servers

Configure a Media Server's SNMP Services Community String Rights

Use this procedure on media servers running voice application software. Prime Collaboration Assurance installation ensures that the SNMP service is installed and enabled on that server.

Prime Collaboration Assurance cannot monitor supported voice applications running on a media server if community string rights for SNMP services are set to *none*. The SNMP queries will not succeed unless the rights for the community string are changed to *read-only*, *read-write*, or *read-create*.

To set a media server's SNMP services community string right:

1. On the media server system, choose Start > Settings > Control Panel > Administrative Tools > Services.

The Services window appears.

2. Double-click SNMP Service.

The SNMP Services Properties window appears.

3. Select the Security tab.

4. Select Community String and click Edit.

5. Change the rights from NONE to READ ONLY.

Prime Collaboration Assurance requires read-only rights. You are not required to set the rights to read-write or read-create.

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 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: Choose System > SNMP and enter the SNMP information.

Cisco Expressway Core/Edge

Follow the same procedure mentioned under Cisco TelePresence Video Communication Server, to enable HTTP, and enable SNMP for Cisco Expressway - Core or Cisco Expressway - Edge.

Cisco TelePresence Exchange

Create New User with API role in Primary CTX Admin server

If you are using Prime Collaboration 10.5 and later, you can monitor the Cisco TelePresence Exchange (CTX) nodes in Prime Collaboration Assurance (PCA) without using Cisco Hosted Collaboration Mediation Fulfillment.

To do this you need to create a new user with API role in the primary CTX Admin Server as follows:

1. Log in as Admin user in the graphical user interface of the primary CTX Admin server.
2. Click "Users" on the left control panel, under the "System" tab.
3. Create a new user, select "API" as its role from the drop-down menu, and then click "Save".

For complete information on how to monitor Cisco TelePresence Exchange(CTX)nodes in Prime Collaboration Assurance (PCA) without using Cisco Hosted Collaboration Mediation Fulfillment, see the Cisco Prime Collaboration Assurance Guide - Advanced, 10.5.

Configuring Unified Contact Center Enterprise Devices

If you have deployed Prime Collaboration 10.5 and later, you need to configure the Unified Contact Center Enterprise Devices mentioned below.

Unified Contact Center Enterprise

Enable SNMP

1. Add the Cisco SNMP Agent Management Snap-in. See section How to add the Cisco SNMP Agent Management Snap-in and Saving the Snap-in View in the [SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted](#). Note: If you are using Windows server 2008, type mmc/32.
2. Configure the Community Name for SNMP version 1 or version 2c – See the section Configuring Community Names for SNMP V1 and V2c in the [SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted](#). Note: At least one community string must be configured on each UCCE server to be managed.
3. (Optional) Configure User Name for SNMP v3 – See the section Configuring User Names for SNMP v3 in the [SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted](#).
4. Configure General properties – See the section Configuring General Information Properties for Cisco SNMP Agent Management in the [SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted](#).

Configure Debug Level 3 for UCCE Using System CLI

If you want to use the Log Collection Center and Call Signaling Analyzer features, you need to set the debug level on the UCCE as follows:

1. Click the Unified System CLI icon, then log in with domain, username and password. For example: cisco/JDoe where cisco is the domain name and JDoe is the username.
2. Press Enter and skip the instance name in which case it will default to the single instance used in Enterprise environment.
3. After the welcome message, enter this command:

```
debug level 3 component cvp:CallServer subcomponent cvp:SIP
```

Configure UCCE to send Traps

1. To access the Cisco SNMP Agent Management settings, refer to the section: How to add the Cisco SNMP Agent Management Snap-in, in the [SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted](#).
2. Expand Cisco SNMP Agent Management in the left pane of the MMC plugin.

3. Highlight Trap Destinations in the left pane under Cisco SNMP Agent Management.
Trap Entity Name and SNMP Version columns appear in the right pane.
4. Right click on the white space in the right pane and choose Properties.
A dialog box appears.
5. Click Add Trap Entity. Under Trap Entity Information, select the SNMP version radio box for the version of SNMP used.
6. Provide a name for the trap entity in the Trap Entity Name field. Select the SNMP Version Number, and the User Name/Community Name that you want to associate with this trap. This list is auto-populated with existing users/community names that have already been configured.
7. Enter one or more IP addresses in the IP Address entry field (containing " dots") and click Insert to define the destination(s) for the trap(s).
8. Click Save to save the new trap destination.
The Trap Entity Name appears in the Trap Entities section at the top of the dialog box.
Note: You can remove the Trap Entity by highlighting the name in the Trap Entities section and clicking Remove Trap Entity.
9. Click OK to save the changes.

Cisco Finesse

Enable SNMP

1. Launch the serviceability page and configure SNMP for Cisco Finesse by entering the following in a web browser:
For Cisco Finesse Release 11.x and earlier
<http://<IP Address>/ccmservice>. Here IP address is the address of the device.
For Cisco Finesse Release 11.x and later
<https://<FinesselP>:8443/ccmservice>
2. Follow procedure mentioned for Enable SNMP under Cisco Unified Communications Manager on this page. To enable SNMP v3, on the serviceability page go to SNMP > v3 > Users and configure a user.

Cisco MediaSense

Enable SNMP

1. Launch the serviceability page and configure SNMP for Cisco MediaSense by entering the following in a web browser: <http://<IP Address>/ccmservice>. Here IP address is the address of the device.
2. Follow procedure mentioned for Enable SNMP under Cisco Unified Communications Manager on this page. To enable SNMP v3, on the serviceability page go to SNMP > v3 > Users and configure a user.

Cisco SocialMiner

Enable SNMP

1. Launch the serviceability page and configure SNMP for Cisco SocialMiner by entering the following in a web browser: <http://<IP Address>/ccmservice>. Here IP address is the address of the device.
2. Follow procedure mentioned for Enable SNMP under Cisco Unified Communications Manager on this page. To enable SNMP v3, on the serviceability page go to SNMP > v3 > Users and configure a user.

Cisco Unified Intelligence Center

Enable SNMP

1. Launch the serviceability page and configure SNMP for Cisco Unified Intelligence Center by entering the following in a web browser: <http://<IP Address>/ccmservice>. Here IP address is the address of the device.
2. Follow procedure mentioned for Enable SNMP under Cisco Unified Communications Manager on this page. To enable SNMP v3, on the serviceability page go to SNMP > v3 > Users and configure a user.

Cisco Voice Portal

Enable HTTP

In the Cisco Prime Collaboration Assurance User Interface, when we add CVP devices under "Manage Credentials", we need to add userID/pwd for the "wsmadmin" user that has been configured in CVP, as the HTTP credentials. If not, the HTTP test for the device fails.

Enable SNMP

Follow the procedure mentioned under the section "SNMP V1/V2c Community String Setup" in the document [Operations Console User's Guide for Cisco Unified Customer Voice Portal Release 9.0\(1\)](#). Ensure that this configuration is performed in the CVP OAMP server.

Configure Debug Level 3 for CVP Using System CLI

If you want to use the Log Collection Center and Call Signaling Analyzer features, you need to set the debug level on CVP as follows:

1. Click the Unified System CLI icon, then log in with username ["wsmadmin" is the default username added during installation] and password as the Operations Console Administrator password configured during CVP installation.
2. (Optional) Enter the instance name. The instance name is the first part of the service name. To find the instance name, look at the services that are running on the server. Note: This step is not required if you run the System CLI from CVP server because it would not ask for instance name.
3. After the welcome message, enter this command:

```
admin:debug level 3 comp "cvp:CallServer" sub "cvp:SIP"
```

Note:

1. Before using the System CLI on a CVP device, the device must be deployed by the CVP Operations Console.
2. To be able to login to the System CLI on CVP, WSM service must be up and running. By default, WSM service is always running.
3. Leave the Instance field empty unless you have a hosted environment with multiple instances.

Configuring Endpoints

Cisco TelePresence System Video Endpoints

Enable HTTP

You can access Cisco TelePresence system 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 system video endpoint.

Enable SNMP

SNMP for Cisco TelePresence system devices is configured using Cisco Unified Communications Manager phone configuration. To change the SNMP community string:

1. Launch Cisco Unified Communications Manager Administration.
2. Choose Device > Phone and search for Cisco TelePresence system 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 system 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.

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 Prime Collaboration IP address to configure the trap receiver: <PrimeCollaboration_ip_addr>
- Enter the Prime Collaboration IP address and port number 20514 to configure syslog receiver.: <PrimeCollaboration_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).

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 from the web interface:

Choose 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 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. 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 Prime Collaboration to accurately discover the troubleshooting path.

Configuring Call Management Applications

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 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 choose 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 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 uses this information to display the location of Cisco TMS in the inventory.
7. Restart the SNMP Service after the necessary modifications.

Configure Reporting API in Cisco CTS-Manager

For Prime Collaboration server to retrieve scheduled meetings from from CTS-Manager, 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.

Note: The procedures described below are applicable for CTS-Manager 1.8. If you are using any other supported versions, see the CTS-Manager Reporting API related documents.

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

1. In the LDAP server, create a user group. For example, create a group named pc_group.
2. In the group that you created in the LDAP server, create a user. For example, create a user named pc_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, pc_group created in *Step 1*.
4. Discover the CTS-Manager in Prime Collaboration with the user that you created in the LDAP server. For example, use pc_user.

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

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

Note:

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

Configure Third Party Booking API User in Cisco TMS

For the Prime Collaboration server to retrieve scheduled meetings from Cisco TMS server, you will require an Application Integration License for each server that uses the API. For details see the following note.

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.

*For Cisco Prime Collaboration Assurance 9.5 and later, if you want to use the frequent polling of TMS (versions 13.2 and later) feature for session monitoring, you will require a booking API license for the GetTransactionSince TMS API.

To enable Prime Collaboration 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 Remote Setup Service 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, pc_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 Prime Collaboration will be polling from Cisco TMS.
4. Click Invoke.
5. In the Cisco TMS application, verify the user name configured in Step 3 is listed in the Users page.
6. In the Cisco TMS application, create a user group. For example, create a group named pc_group.
7. Add the user created in Step 3 to the group created in Step 6. For example, add pc_user to pc_group.
8. In the Groups page, for the group created in Step 6, hit the drop down and select Set Permissions. Now check the Read permission check box for List Conferences-All (under the Booking pane). For example, pc_group must have the read permission to List Conferences-All.

9. Discover the Cisco TMS in Cisco Prime Collaboration with the user that you created in Step 3. For example, use `pc_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 *Cisco Telepresence Management Suite Administrator Guide*.

Disable the GetTransactionSince Cisco TMS API

To disable the GetTransactionSince TMS API (applicable for Prime Collaboration 10.0 and later) :

1. Log in as a root user in the Prime Collaboration Assurance server through SSH (port 26).
2. Run the following command:

```
1. goemsam
```

3. Go to `/opt/emms/emsam/conf` and open file `emsam.properties`
4. Change the value of `com.cisco.nm.emms.access.tms.frequent.polling` to `false`.
5. Restart the Prime Collaboration Assurance server by running the command:

```
bin/cpcmcontrol.sh start
```

then the following command:

```
bin/cpcmcontrol.sh stop
```

To see the status of the server

Note: Make sure all the processes are not running.

```
Start  
/cpcmcontrol.sh status | wc -l
```

```
29 (Number of processes)

Stop
cd bin
./cpcmcontrol.sh status | wc -l
2 (Number of processes)
```

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 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. Choose 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. Choose 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 Collaboration application. This user can be configured in the Multipoint Switch web user interface when logged in as admin. After the dedicated HTTP user has been created, you must login to CTMS web UI using this user credential and then change the password (the same password can be entered).

An admin user is not required by Cisco Prime Collaboration 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 2 To configure NAM as an https server, from the command line on the NAM, enter this command under this section c 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 Collaboration application, we recommend

that you log in with this account in CTMS at least once before you enter the credentials in the Prime Collaboration server.

Configuring VMware ESX Server

Configure SNMP

You can configure SNMP using one of the procedures mentioned below:

- Using vSphere Management Assistant (vMA)
 1. To configure SNMP on ESX:
 2. Install vSphere Management Assistant (vMA) on the VMware ESX server. See the sections *Hardware Requirements*, *Software Requirements*, *Required Authentication Information*, and *Deploy vMA*, in the chapter *Getting Started with vMA*, in the [vSphere Management Assistant Guide](#).
 3. Create network settings with a username, password, and port Number (22). See the section *Configure vMA at First Boot*, in the chapter *Getting Started with vMA*, in the [vSphere Management Assistant Guide](#).
 4. Follow the procedure to configure SNMP for ESX mentioned in the section *Configure SNMP for ESXi*, in the [VMware vSphere ESXi and vCenter Server 5 Documentation](#).
- Using SSH

You can also configure SNMP on ESX by enabling SSH on the ESXi host. For details on the procedure, see <http://blogs.vmware.com/vsphere/2012/11/configuring-snmp-v1v2cv3-using-esxcli-5-1.html>.

Configure HTTP

You can configure HTTP using the procedure mentioned below:

- Using vSphere Management Assistant (vMA)

To configure HTTP on ESX:

1. Install vSphere Management Assistant (vMA) on the VMware ESX server. See the sections *Hardware Requirements*, *Software Requirements*, *Required Authentication Information*, and *Deploy vMA*, in the chapter *Getting Started with vMA*, in the [vSphere Management Assistant Guide](#).

2. Create network settings with a username, password, and port Number (22). See the section *Configure vMA at First Boot*, in the chapter *Getting Started with vMA*, in the [vSphere Management Assistant Guide](#).
3. Follow the procedure to configure HTTP for ESX mentioned in the section *Configure HTTP for ESXi*, in the [VMware vSphere ESXi and vCenter Server 5 Documentation](#).

Triggers for Alarms of VMware vCenter Server

Do not disable or modify the VMware vCenter Server (vCenter) triggers as this blocks generation of the vCenter alarms.

VMware vCenter Server Alarm Name	VMware vCenter Server Trigger Name	Prime Collaboration Assurance Alarm Name
Host Connection and Power state	Host Connection State	HostDisconnected
Host Connection and Power state	Host Power State	HostPoweredOff
Host Hardware Power Status	Hardware Health Changed	HostPowerNotOk
Host Storage Status	Hardware Health Changed	HostStorageCritical
Host Error	Host Error	Host Error
Host Error	Host Warning	Host Warning
vSphere HA Virtual Machine Failover failed	Not enough resource for vSphere HA to start VM	NotEnoughResoucetoStartVM
vSphere HA Virtual Machine Failover failed	vSphere HA Virtual Machine failover unsuccessful	VMFailoverUnsuccessful
vSphere HA Virtual Machine Failover failed	vSphere HA Restarted Virtual machine	N/A
Cannot Connect to storage	Lost Storage path redundancy	LostStoragePathRedundancy
Cannot Connect to storage	Degraded Storage Path redundancy	DegradedStoragePathRedundancy
Datastore capability alarm	N/A	Datastorecapability
Virtual Machine Error	VM Powered On	VMDown
Virtual Machine Error	VM Powered Off	VMDown
Host Connection Failure	Network Error	HostConnectionFailure
Host Connection Failure	Host Connection Lost	HostConnectionFailure
Host Connection Failure	Cannot Connect Host -time out	HostConnectionFailure
Host Connection Failure	Host Connected	HostConnectionFailure
Cannot Connect to Storage	Lost Storage Connectivity	Lost Storage connectivity

Configuring Cisco Network Analysis Module

Enable http or https Server and Configure a Web Administrator User

To access a NAM, the NAM must be configured as an http or http secure (https) server and you must configure an http or https port. The first time that you enable an http or https server on NAM, you are prompted for a web administrator username and password. The username and password of a web administrator user must be entered into Prime Collaboration Assurance.

To configure NAM as an http server, from the command line on the NAM, enter this command:

```
ip http server {enable | disable}
```

To configure NAM as an https server, from the command line on the NAM, enter this command:

```
ip http secure server {enable | disable}
```

If this is the first time that NAM has been configured as an http or https server, you are prompted for a web Administrator username and password as shown in the following example.

```
ip http server enable
Enabling HTTP server...

No web users are configured.
Please enter a web administrator user name [admin]:
New password:
Confirm password:

User admin added.
Successfully enabled HTTP server.
```

Note the username and password; you must enter it in Prime Collaboration Assurance.

To configure the http or https port, use the appropriate one of these commands:

```
ip http port <port number>
ip http secure port <port number>
```

For complete instructions, including how to reset the web administrator password, see the installation and configuration guide or note for the particular NAM hardware.

Enable RTP Stream Monitoring

Ensure that RTP stream monitoring is enabled on each NAM that you add to Prime Collaboration Assurance.

1. Log into NAM using the web interface.
2. Choose Setup > Monitor. The Core Monitoring Functions table displays.
3. Click RTP Stream Monitoring. The RTP Stream Setup window appears.
4. Click the Monitoring Enabled check box.
5. Click Apply.

For more information, see *User Guide for the Cisco Network Analysis Module Traffic Analyzer*.

Configure NAM to Use the NTP Server

To correlate information from sensors and Unified Communications Managers, timing is very important.

Therefore:

- Prime Collaboration Assurance must be configured to use the NTP server that Unified Communications Manager uses.
- Cisco strongly recommends that you also configure each NAM to use the same NTP server that Prime Collaboration Assurance uses.
 1. Log into NAM using the web interface.
 2. Choose Admin > System > NAM System Time. The NAM System Time Configuration dialog box appears.
 3. Select the NTP Server radio button.
 4. Enter the DNS name or IP address for the NTP server that Prime Collaboration Assurance uses in the first set of NTP server name and IP address text boxes.
 5. Select the Region and local time zone from the lists. Click Apply.

For more information, see *User Guide for the Cisco Network Analysis Module Traffic Analyzer*.

Configuring Cisco Virtual Network Analysis Module

Configure Cisco Prime Collaboration to Receive SNMP Traps from Prime vNAM

1. Log in to the Cisco Prime Virtual Network Analysis Module (Prime vNAM) using the web user interface.

2. Choose Administration > System > SNMP Trap Setting, and click Create.
3. Enter values in the Community (SNMP Community), IP Address (of Prime Collaboration where the traps will be sent) and UDP Port (Default Port - 162) fields, and click Submit. The SNMP Trap Setting page shows the newly added information.

Network Devices

Configure Cisco Mediatrace, Cisco IOS IP SLA, and Performance Monitoring

If you have enabled [Cisco Mediatrace](#) on your network nodes, Prime Collaboration 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 Prime Collaboration Inventory (Operate > Device Work Center > Current Inventory table).

For Performance Monitoring (PM) Configuration:

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

Supported Software Versions for the Cisco Medianet Feature

Platform	Minimum IOS Release	Minimum Package	Feature Support
Catalyst 3560	15.0(1)SE2	IP Base	Mediatrace, Performance Monitor, IPSLA-VO
Catalyst 3750	15.0(1)SE2	IP Base	Mediatrace, Performance Monitor, IPSLA-VO
Catalyst 4500E Supervisor 7-E/7L-E	XE 3.3.0SG	IP Base	Mediatrace, Performance Monitor, IPSLA-VO
Catalyst 4500E Supervisor 6-E/6L-E	15.1(1)SG	IP Base	Mediatrace, Performance Monitor, IPSLA-VO
Catalyst 6500 Supervisor 2T	15.0(1)SY	IP Services	Mediatrace, Performance Monitor
	15.2(2)T	UC and DSP	IPSLA-VO Sender
	15.2(2)T	15.2(2)T	IPSLA-VO Responder
ISR 1900	15.1(3)T	UC and Data	Mediatrace, Performance Monitor
	15.2(2)T	IP Base	IPSLA-VO Responder
ISR 880 and 890	15.1(3)T	Universal	Mediatrace, Performance Monitor
ASR 1000	XE 3.5	IP Base	Performance Monitor

Enable Cisco IOS Devices to Send SNMP Traps

For devices running Cisco IOS software, provide the following commands:

```
(config)# snmp-server community [community string] ro
```

```
(config)# snmp-server enable traps
(config)# snmp-server host [trap receiving host ip address] traps [community string]
```

Where *[community string]* indicates an SNMP read-only community string and *[trap receiving host ip address]* indicates the SNMP trap receiving host (the Prime Collaboration server). For more information, see the appropriate command reference guide.

Enable Catalyst Devices to Send SNMP Traps

For devices running Catalyst software, provide the following commands:

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [trap receiving host ip address] [community string]
```

Where *[community string]* indicates an SNMP read-only community string and *[trap receiving host ip address]* indicates the SNMP trap receiving host (the Prime Collaboration server).

Configure IOS Gateway

If you have deployed Prime Collaboration 10.5 and later, you can use the Log Collection Center and Call Signaling Analyzer features. To use those feature you need to do the following using the router command line:

1. Login to gateway using the username, password and enable password.
2. At the Router prompt, enter the following commands:

- Enable SIP Messages

```
Gateway#debug ccsip messages
```

- Set the Time stamp

```
Gateway(config)#service timestamps debug datetime msec localtime
Gateway(config)#service sequence-numbers
```

- Set the Time Zone

```
Gateway(config)#clock timezone <timezone name> <hours offset from UTC>
Gateway(config)#clock summer-time <timezone name> recurring
```

For example

```
Gateway(config)#clock timezone EST -5 0
Gateway(config)#clock summer-time EDT recurring
```

- Add NTP Server IP address

```
Gateway(config)#ntp server <NTP server IP address>
```

Configuring MGCP Voice Gateways to Support CVTQ

This configuration is applicable for voice gateways running Cisco IOS 12.4(4)T or later.

TIC5510 DSP supports the DSP/KF voice quality metric that Prime Collaboration needs. For more information, see [DSP Voice Quality Metrics Guide](#).

To confirm that a voice gateway has TIC5510 DSP, look for 5510 in the output of this command:

```
show voice dsp detailed
```

For more information, see [Cisco IOS Voice Command](#).

To enable voice quality statistics on the voice gateway, use the following command:

```
mgcp voice-quality-stat all
```

Note: A warning message might be displayed advising that "enable voice stats might impact performance".

For more information, see [Cisco IOS Voice Command](#).

Configuring Unified Contact Center Express

Enable SNMP

SNMP is not enabled in Cisco Unified Contact Center Express by default.

To enable SNMP:

1. Log in to the Cisco Unified Serviceability view in the Cisco Unified Contact Center Express web GUI.
2. From the main menu in the Cisco Unified Serviceability view, choose SNMP > v1/v2c > Community String.
3. Select a server from the Server drop-down list and click Find.
If the community string is already defined, the Search Results section displays the Community String Name.
4. Click Add new to add a new string, if no results are displayed.
5. Specify the required SNMP information and save the configuration.

Configuring Cisco Integrated Management Controller (CIMC)

Enable SNMP

Cisco Prime Collaboration generates traps for alarms and events of Cisco Integrated Management Controller (CIMC) devices and sends notifications to the trap receiver. SNMP is not enabled in CIMC by default.

To enable SNMP:

1. Log in to the Cisco Integrated Management Controller web GUI.
2. Select the Admin tab on the left pane and click Communications Services.
3. Select the SNMP tab and enter the details in the Trap Community String field.
4. In the SNMP Version field, select v1 or v2 from the drop-down list.
5. Under Trap Destinations, specify the Prime Collaboration Assurance IP addresses where the CIMC traps are received, and save the configuration.