# CISCO™

# Configure Devices for Cisco Prime Collaboration Assurance

Published On: December 8, 2020
Modified On  : January 20, 2021

## Release History

| First Customer Shipment (FCS)/Service Pack(s) (SP) | Release Date |
|---|---|
| Release: 12.1 SP4 | |
| SP4 Republished, to include the latest SNMP commands | 20-JAN-2021 |
| SP4 | 08-DEC-2020 |

## 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 - Manage video test call and analyze call signaling.

■ JTAPI - Retrieve the conference status information from the Cisco Unified CM.

■ CDP - Discover neighboring devices.

Note: For supported software versions, see Supported Devices for Cisco Prime Collaboration Assurance.

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Analog Gateway | Yes | - | - | - | - | - | |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| 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 Center | Yes | Yes | – | – | – | – | If you are using Cisco Prime Collaboration 10.5 or later versions, you must configure 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. |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| 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 | – | | – | |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Cisco Unified CM | Yes | Yes | – | Yes | – | – | ■ 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 > Enterprise Parameters) on Cisco Unified CM publisher (for every cluster). <br><br> ■ The same credentials must be created for all devices in the cluster whenever clustering is used. <br><br> ■ The JTAPI user needs to have these roles Standard AXL API Access, CCM Admin Users, SERVICEABILITY Administration, CTI Enabled, and CTI Allow Call Monitoring. <br><br> ■ The conference monitoring feature is supported only from Cisco Unified CM 8.5 release onwards. |

4

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Cisco Unified Communications Manager Business Edition | Yes | Yes | – | Yes | – | – | |
| Cisco Unified Customer Voice Portal | Yes | Yes | – | – | – | – | 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 *ServiceabilityAdministrationUserRole* privileges. The default username *wsmadmin* has this privilege. |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| ■ Cisco Codec EX series<br><br>■ Cisco TelePresence System Integrator C Series<br><br>■ Cisco TelePresence MX Series<br><br>■ Cisco TelePresence System Profile Series<br><br>■ Cisco TelePresence SX20 Quick Set<br><br>■ Cisco TelePresence MX700 and MX800 (supported by Cisco Prime Collaboration | Yes | Yes | Yes | – | Yes | – | The HTTP user requires Admin privilege. |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| ■ Cisco TelePresence MX300 G2 and MX200 G2 (supported by Cisco Prime Collaboration Assurance 10.5.1 and later versions) <br><br> ■ Cisco TelePresence SX10 and SX80 (supported by Cisco Prime Collaboration Assurance 10.5.1 and later versions) | | | | | | | |
| Emergency Responder | 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. |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Cisco MCU | Yes | Yes | - | - | - | - | ■ The HTTP user requires Admin privilege. <br><br> ■ 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 | - | - | - | - | - | |
| Personal Assistant | - | - | - | - | - | - | |
| Cisco TelePresence System MXP series | Yes | Yes | Yes | | | | |
| Cisco Unified Presence | Yes | Yes | - | - | - | - | |
| Network devices (routers and switches) | Yes | - | Yes | - | - | Yes | |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|--------|------|------|-----|-------|-----|-------|---|
| Cisco TelePresence Management Suite (Cisco TMS) | Yes | Yes | – | – | – | – | ■ Requires Booking API license (TMS software version 13.1 or below).<br><br>■ The HTTP user for Cisco Prime Collaboration needs to be generated through the Booking API on the Cisco TMS windows server.<br><br>■ Cisco Prime Collaboration supports only the default e-mail template for the Booking Confirm e-mail in Cisco TMS. The conference import feature will not work, if the default e-mail template is not used. |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Cisco Telepresence Server<br><br>Cisco Telepresence Server on Virtual Machine (supported by Cisco Prime Collaboration Assurance 10.5.1 and later versions)<br><br>Cisco TelePresence Server on Multiparty Media 310 and 320 (supported by Prime Collaboration Assurance 10.5.1 and later versions) | – | Yes | – | – | – | – | ■ The HTTP user account should have the API Access privilege.<br><br>■ 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 Connection | Yes | Yes | – | – | – | – | |
| Cisco Unity Express | Yes | – | – | – | – | – | |
| Cisco TelePresence Video Communication Server (Control and Expressway) | Yes | Yes | – | – | – | – | The HTTP user requires Admin privilege. |
| Third party devices | Yes | – | – | – | – | – | |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Cisco Jabber Video for Telepresence (Movi) | – | – | – | – | – | – | ■ The Cisco Jabber endpoints are discovered either through Cisco Unified CM or Cisco VCS (access credentials are not required).<br><br>■ End-to-end troubleshooting is not supported. |
| Cisco Cius | – | – | – | – | – | – | ■ The Cisco Cius endpoints are discovered either through Cisco Unified CM or Cisco VCS (access credentials are not required). You must enable web access in Cisco Unified CM for these.<br><br>■ Credentials are not required for HTTP access.<br><br>■ End-to-end troubleshooting is not supported. |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Cisco IP phones (89xx, 99xx) | – | – | – | – | – | – | ■ The Cisco IP Phones endpoints are discovered through Cisco Unified CM. You must enable web access in Cisco Unified CM for these.<br><br>■ These video phones require Cisco Unified CM application user to have the additional role Standard CTI Allow Control of Phones supporting Connected Xfer and conf.<br><br>■ Credentials are not required for HTTP access.<br><br>■ End-to-end troubleshooting is not supported. |

| Device | SNMP | HTTP | CLI | JTAPI | CDP | Notes | |
|---|---|---|---|---|---|---|---|
| Cisco DX70 and DX80 (supported by Prime Collaboration Assurance 10.5.1 and later versions) | – | – | – | – | – | – | ■ The Cisco Phone endpoints are discovered through Cisco Unified CM. You must enable web access in Cisco Unified CM for these.<br><br>■ These phones require Cisco Unified CM application user to have the additional role Standard CTI Allow Control of Phones supporting Connected Xfer and conf.<br><br>■ Credentials are not required for HTTP access.<br><br>■ End-to-end troubleshooting is not supported |
| 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.

### Discovery

#### 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 i icon on the right.

4. Click Assign Role to Group and select the following roles:

   a. Standard AXL API Access.

   b. Standard CCM Admin.

   c. 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.

### 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 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.

# Conference Monitoring

## Enable JTAPI

JTAPI (Java Telephony API) is used to retrieve the conference 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:

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:

   ■ Standard CTI Allow Call Monitoring

   ■ Standard CTI Enabled

   ■ 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.

   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.

   For Cisco Prime Collaboration Release 11.6 and earlier

   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/ConferenceMon/CUCMJTAPIDiag.log

## Configure CDR (Add Cisco 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 is displayed.

1. Select your CUCM server (the Publisher node) and the Cisco CallManager service.

2. 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.

3. 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.

## 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 Cisco Voice Transmission Quality (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 is displayed.

1. 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. Set these parameters:

   ■ CDR Enabled Flag—Scroll down to System. Set to True.

   ■ 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.

3. Click Update.

   Caution: Do not enable the CDR Log Calls With Zero Duration Flag service parameter. Enabling it can adversely impact 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 is displayed.

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.

## View Dashlets

### 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

# 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

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 is displayed.

3. Select the applicable user account.

   The Edit User Basics window is displayed.

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.

# 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 is displayed.

2. Double-click SNMP Service.

The SNMP Services Properties window is displayed.

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.

### Discovery

#### 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.

## 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

### Discovery

#### 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 mustbe 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.

## Log Collection Center

### Configure Debug Level 3 for Unified CCE 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:

   admin:debug level 3 comp "icm:Router A" sub "icm:rtr"

## 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 are displayed in the right pane.

4. Right click on the white space in the right pane and choose Properties.

   A dialog box is displayed.

5. Click Add Trap Entity. Under Trap Entity Information, select the SNMP version radio box for the version of SNMPused.

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 Insertto define the destination(s) for the trap(s).

8. Click Save to save the new trap destination.

   The Trap Entity Name is displayed 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 sectionand clicking Remove Trap Entity.

9. Click OK to save the changes.

# Cisco Virtualized Voice Browser

## Discovery

### 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](#).

# Cisco Finesse

## Discovery

### 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://<FinesseIP>: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

## Discovery

### 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

## Discovery

### 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

## Discovery

### 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

## Discovery

### 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.

## Log Collection Center

### 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"

Notes:

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

### Discovery

#### 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

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

2. Launch Cisco Unified Communications Manager Administration.

3. Choose Device > Phone and search for Cisco TelePresence system endpoints.

4. Click the Device Name link to go to the phone configuration page.

5. Edit the SNMP Configuration Parameters.

6. 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.

Notes:

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

## Discovery

### 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. 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.

# Configuring Call Management Applications

## Cisco TelePresence Management Suite

HTTP and SNMP access are required to successfully monitor Cisco TMS.

### Discovery

#### 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 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.

Notes:

*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 conference 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 RemoteSetupService page is displayed. 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 3is 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 Ciso 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:

    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

# 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.

## Discovery

### 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 VMware ESX Server

## Discovery

### Configure SNMP

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

- Using  vSphere Management Assistant (vMA)

To configure SNMP 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 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.

## Monitor Alarms

### 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 |

| VMware vCenter Server Alarm Name | VMware vCenter Server Trigger Name | Prime Collaboration Assurance Alarm Name |
|---|---|---|
| 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 | NA |
| 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 On | 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 |
| Host Connection Failure | LostStorageConnectivity | Lost Storage connectivity |

# Configuring Cisco Network Analysis Module

## Discovery

### 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 is displayed.

1. Click the Monitoring Enabled check box.

2. 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 is displayed.

    1. Select the NTP Server radio button.

    2. 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.

    3. Select the Region and local time zone from the lists.

    4. 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

## Enable Cisco IOS Devices to Send SNMP Traps

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

(config)# snmp-server [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).

# Log Collection Center

## 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 adress

   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

Warning:  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

## Discovery

### 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)

## Discovery

### 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.

# Configuring Perimeta Session Border Controller (SBC)

## Discovery

### Enable SNMP

SNMP is not enabled in Perimeta SBC by default.

To enable SNMP:

1.  Log in to Perimeta ISC in the Cisco C-Series server.

    The command prompt window with a list of commands is displayed.

2.  Enter 1 from the list of commands to open the command line interface.

3.  Enter the following commands to open the SNMP configuration page:

    META-A#configuration

    META-A(config)#sbc

    META-A(sbc)#diagnostics

    META-A(diagnostics)#snmp

■   In the SNMP window, enter the following commands:

    show config here

    Your existing SNMP configuration is displayed.

    Note: You must note down the Prime Collaboration Assurance IP address that appears in the following configuration line- authorized-client <IP address>

    snmp-client <IP address>

    where <IP address> is the address of Cisco Prime Collaboration Assurance.

    client-address ipv4 <IP address>

    allow-stats-requests

    community communityString

    where communityString is the community string you want to use for authentication of the client, for example 'cisco'.

    allow-system-mib-requests

Note: You must use communityString if you want the client to use a particular community string (SNMP password) to authenticate itself. If you do not configure a community string, the Session Controller uses the string public.

# Configuring Cisco Unified Attendant Console

## Discovery

### Enable SNMP

SNMP is not enabled in Cisco Unified Attendant Console by default.

To enable SNMP:

1. Log in to Windows Server 2012 box where Cisco Unified Attendant Console is running.

2. Open the Server Manager and go to Manage > Add Roles and Features.

3. Select Features and check the SNMP Service check box from the list to install SNMP Service.

4. From the Administrative Tools, go to the Services tab.

5. Right click on SNMP Service and select Properties.

6. In the Security tab, create a community string and add Cisco Prime Collaboration Assurance IP address as a host to receive the SNMP packets.

# Configuring Cisco Prime Collaboration Assurance Server

## Discovery

### Enable SNMP

#### Enable SNMP v1/v2c using admin access

Note: Enabling SNMP v1/v2c using admin access is the preferred method.

1. Log in as an admin user in the Prime Collaboration Assurance server.

2. Type configure terminal.

3. Set SNMP V2 community by running the following command:

snmp-server contact jane

snmp-server location bangalore

snmp-server community public ro

4. Save the configuration using the following command:

write memory

## Enable SNMP v1/v2c using root access

1. Log in as a root user in the Prime Collaboration Assurance server.

2. Go to /etc/snmp and open snmpd.conf file.

3. Add rocommunity public in snmpd.conf file, and save the configuration.

4. Restart the snmpd by running the command:

   For Cisco Prime Collaboration Assurance 11.6 and earlier

   /etc/init.d/snmpd stop

   then the following command:

   /etc/init.d/snmpd start

   For Cisco Prime Collaboration Assurance 12.1 and later

   service snmpd stop

   then the following command:

   service snmpd start

   To test SNMP v1/v2c:

1. Execute the following command:

   # snmpwalk -v2c -c public <PCA IP> .1

## Enable SNMP v3 using root access

Note: The supported authentication algorithms are MD5 or SHA; and the supported privacy algorithms are AES, DES, and AES128. The FIPS compliant setup does not support MD5 authentication algorithm and DES privacy algorithm.

Note: You can enable SNMP v3 only using root access.

To enable SNMP v3 using MD5 algorithm:

1. Log in as a root user in the Prime Collaboration Assurance server.

2. Go to /etc/snmp and open snmpd.conf file.

3. Add the entries in snmpd.conf file as in the following example:

   #For SNMP V3

   com2sec snmpv3test <PCA IP>    public

   com2sec snmpv3test zen42        public

   group snmpv3group     usm    snmpv3test

   access snmpv3group      " "     usm    priv   exact  all    all   all

   rwuser jane authPriv .1

Note: In this example, jane is the rwuser with security mode authPriv. You can also change the security level to authNoPriv or noAuthNoPriv.

To configure SNMP v3 using MD5 algorithm:

1. Stop the snmpd by running the following command:

   /etc/init.d/snmpd stop

2. Create SNMP v3 user by running the following command:

   net-snmp-config --create-snmpv3-user -A authpassword -X privpassword -x AES -a MD5 jane

   /var/lib/net-snmp/snmpd.conf file is modified with hidden encryption key and rwuser jane is added to /etc/snmp/snmpd.conf file. Note: You need to specify a password for authentication (-A) and a password for encryption (-X), along with the algorithms to be used for authentication and encryption.

   To test SNMP v3 using MD5 algorithm:

1. Start the snmpd by running the command:

   /etc/init.d/snmpd start

2. Execute the following command:

   # snmpwalk -v 3 -a MD5 -A authpassword -X privpassword -l authPriv -u jane <PCA IP> .1

   To view SNMP v3 in tabular format:

   Execute the following command:

   #snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u jane <PCA IP> [OID of tables]

   To enable SNMP v3 using SHA algorithm:

1. Log in as a root user in the Prime Collaboration Assurance server.

2. Go to /etc/snmp and open snmpd.conf file.

3. Add the entries in snmpd.conf file as in the following example:

   #creat**eUser jane SHA "authpassword" AES "privpassword"**

   To configure SNMP v3 using SHA algorithm:

1. Restart the snmpd by running the command:

   /etc/init.d/snmpd stop

   then the following command:

   /etc/init.d/snmpd start

2. Create SNMP v3 user with the following command:

   # net-snmp-config --create-snmpv3- -A authpassword -X privpassword -x AES -a SHA jane

   /var/lib/net-snmp/snmpd.conf file is modified with hidden encryption key and rwuser jane is added to /etc/snmp/snmpd.conf file. Note: You need to specify a password for authentication (-A) and a password for encryption (-X), along with the algorithms to be used for authentication and encryption.

To test SNMP v3:

Execute the following command:

 # snmpwalk -v 3 -a SHA -A authpassword -X privpassword -l authPriv -u jane <PCA IP> .1

To view SNMP v3 in tabular format:

Execute the following command:

 #snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u jane –a SHA <PCA IP> [OID of tables]

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.