

Configure Prime Collaboration Assurance (PCA) - Conference Diagnostics

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Limitation of Endpoints Set to Limited or Full Visibility Per OVA](#)

[Configure](#)

[Scenario 1. Conference with Video Endpoints Registered to Call Manager](#)

[Cisco Unified Communications Manager Set-Up](#)

[Enable HTTP](#)

[Enable SNMP](#)

[Start CTI Service](#)

[Create Application User for PCA CTI Control \(JTAPI User\)](#)

[Conference Relatable Alarms](#)

[Conference Relatable Reports](#)

[Conference Video Test Call](#)

[Scenario 2. Conference with Non Call Manager Registered Endpoints](#)

[Conference Relatable Alarms](#)

[Conference Video Test Call](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure and set-up your deployment for Conference Diagnostics within Prime Collaboration Assurance (PCA) to proactively monitor voice/video conference statistics.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Call Manager Admin log in
- PCA Log in
- Your Telepresence Monitor Server (TMS)
- Core/Expressway credentials, if applicable

Components Used

The information in this document is based on PCA versions 11.x - 12.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Cisco Prime Collaboration 11.x supports these types of visibility:

- Full Visibility - Call detection with the use of JTAPI/ HTTP feedback and real-time monitoring information such as conference statistics, and conference information is supported.
- Limited Visibility - Automatic call detection with the use of JTAPI/ HTTP feedback takes place, but real-time monitoring information such as conference statistics, and conference information is not supported. Endpoints with limited visibility are indicated with a half-dimmed icon in the Conference Topology.

Cisco Prime Collaboration 12.x supports these types of visibility:

- Full Visibility - Call detection with the use of JTAPI/ HTTP feedback and real-time monitoring information such as conference statistics, and conference information is supported.
- No Visibility - Call detection with the use of JTAPI/ HTTP feedback and real-time monitoring information are not supported. These endpoints are displayed on the Conference Monitoring page with a fully dimmed icon.

Limitation of Endpoints Set to Limited or Full Visibility Per OVA

- Small Open Virtualization Archive (OVA) supports up to 500 Endpoints
- Medium OVA supports up to 1000 Endpoints
- Large OVA supports up to 1800 Endpoints
- Very Large OVA supports up to 2000 Endpoints

A list of supported devices per PCA in regards to conferences and our supported sessions is as shown in the table image here.

Session Scenarios

The various session scenarios that are monitored in Cisco Prime Collaboration are as follows:

Table 1 Session Scenarios

Session Classification	Session Type	Session Structure	Session Topology Elements
Cisco Unified CM <i>intracluster</i> and <i>intercluster</i> sessions	Ad hoc,Scheduled	Point-to-point	Cisco TelePresence System 500, 1000, 3000, TX9000 Series.
Cisco Unified CM <i>intracluster</i> and <i>intercluster</i> sessions	Ad hoc,ScheduledStatic	Multipoint	Cisco TelePresence System 500, 1000, 3000, TX9000 Series, and CTMS.
Cisco VCS <i>intracluster</i> and <i>intercluster</i> sessions	Ad hoc,Scheduled	Point-to-point	Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20, Cisco Cius, and Cisco Jabber. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Cisco VCS <i>intracluster</i> and <i>intercluster</i> sessions (with MCU)	Ad hoc,ScheduledPermanent (displayed as static)	Multipoint	Cisco C series, EX Series, Cisco MCU, Cisco MSE ¹ , or Cisco TelePresence Server. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Cisco VCS <i>intracluster</i> and <i>intercluster</i> sessions (without MCU)	Ad hoc,Scheduled	Multisite	Cisco C series, EX Series, Cisco MX, Cisco MXP Series, Cisco IP Video Phone E20. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.

Sessions between Cisco Unified CM and Cisco VCS clusters ²	Ad hoc	Point-to-pointMultipoint	<ul style="list-style-type: none"> • Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20 • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • Cisco TelePresence Server • IX 5000 series TelePresence endpoints
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) <i>intracluster</i> sessions ³	Ad hoc	Point-to-point	<ul style="list-style-type: none"> • Cisco C series, EX Series, Cisco MX series • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • IX 5000 series TelePresence endpoints
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) <i>intracluster</i> sessions	Ad hoc,Scheduled Note Scheduler must be CTS-Manager 1.7, 1.8, or 1.9.	Multipoint	<ul style="list-style-type: none"> • Cisco C series, EX Series, Cisco MX series, Cisco IP Video Phone E20 • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • CTMS 1.8 or Cisco TelePresence Server
Sessions outside the enterprise firewall - Cisco VCS Expressway	Ad hocPermanent (displayed as static)	Point-to-point,Multipoint, Multisite	<ul style="list-style-type: none"> • Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20 • Cisco MCU or Cisco TelePresence Server • Cisco VCS Control and Cisco VCS Expressway

Endpoints in a call (with an MCU in the call) work as a conferencing bridge in Cisco Unified CM.	Ad hoc	Point-to-point When a call is put in a conference mode or when merged with another call, it becomes Multipoint. The session does not show the MCU. When the first participant leaves the call, the session shows it is connected to the MCU, while the second and third participants continue in the same call as a point-to-point call. Note This scenario is applicable when in-built video bridge capability is not present in the endpoint.	Multipoint conferencing devices and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance .
Sessions between MRA endpoints- Cisco Jabber or Cisco TelePresence MX Series or Cisco TelePresence System EX Series or Cisco TelePresence SX Series	Ad hoc, Scheduled	Point-to-point, Multipoint, Multisite Note Cisco Prime Collaboration does not monitor a Multisite session where an MRA endpoint acts as a conference bridge.	Cisco Jabber, Cisco TelePresence MX Series, Cisco TelePresence System EX Series, and Cisco TelePresence SX Series.

¹ The codian software must be running on Cisco MSE.

² This scenario is supported on CTS 1.7.4, and TC 4.1 to 7.0.

³ The troubleshooting workflow is supported on TC 4.2, 5.0, and above.



Note

- Cisco Cius and Cisco Jabber devices support only ad hoc sessions.

Configure

Scenario 1. Conference with Video Endpoints Registered to Call Manager

Step 1. First you need to ensure the Call Managers are in a Managed state.

Navigate to **Inventory > Inventory Management > Manage Credentials > Create a profile** for the Call Manager cluster.

Note: Remember each credential profile uses the same credentials for every ip listed within the profile. So, if you list the Call Manager Publisher and Subscriber within the same Credential Profile, it uses those same credentials to discover both ip addresses. If you do have a conductor in your setup, discover the conductor first then the Cisco Call Manager as shown in the image.

<input checked="" type="radio"/>	CUCM	ANY	10.201.196.222 ...
<input type="radio"/>	CUE	ANY	10.201.196.209
<input type="radio"/>	CUSP	SIPPROXY	10.201.160.42
<input type="radio"/>	Default	ANY	
<input type="radio"/>	JoeCUBE	ROUTER/VOICEGATEWAY	10.201.196.210

* Indicates required field

*Profile Name

Device Type (Optional)

*IP Version

*Apply this credential to the given IP address

ⓘ

General SNMP Options

SNMP Timeout seconds

SNMP Retries

SNMP Version

Step 2. Ensure you have setup Hypertext Transfer Protocol (HTTP), Simple Name Management Protocol (SNMP) and Java Telephony API (JTAPI) Credentials

In addition, you have to enable the Cisco Computer Telephony Integration (CTI) Service in Call Manager Serviceability.

Cisco Unified Communications Manager Set-Up

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 into Cisco Unified Communications Manager, you must create a new HTTP user group and a correspondent user that Cisco Prime Collaboration can use to communicate.

In order to create a user follow these steps:

Step 1. Log into the Cisco Unified CM Administration web interface with your administrator account.

Step 2. Create a user group with sufficient privileges. Navigate to **User Management>User Settings>Access Control Group** and create a new user group with a suitable name, **PC_HTTP_Users** in this case. Now, select **Save**.

Step 3. Navigate to **User Management>User Settings>Access Control Group** and select **Find**. Find the group you defined and click on the icon on the right.

Step 4. Select **Assign Role to Group** and select these roles:

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

Step 5. Click **Save**.

Step 6. From the main menu, navigate to **User Management > Application Users > Create a new user**.

Specify a suitable password on the **Application User Configuration** page. You can select only certain type of devices from the Available Devices text area, or allow Cisco Prime Collaboration to monitor all devices

Step 7. In the **Permission Information** section, select **Add to User Group** and select the group that was created in Step 1. (for example, PC_HTTP_Users).

Step 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.

In order to enable SNMP:

Step 1. Log into the **Cisco Unified Serviceability** view in the Cisco Unified Communications Manager web GUI.

Step 2. Navigate to **Tools > Service Activation**.

Step 3. Select **Publisher Server**.

Step 4. Navigate to **Performance > Monitoring Services** and select the check box for **Cisco Call Manager SNMP Service**.

Step 5. Select **Save** at the bottom of the screen.

In order to Create a SNMP community string:

Step 1. Log into the **Cisco Unified Serviceability** view the Cisco Unified Communications Manager web GUI.

Step 2. From the main menu in the Cisco Unified Serviceability view, navigate to **SNMP > v1/v2c > Community String**.

Step 3. Select a Server and click **Find**.

If the community string is already defined, the Community String Name is displayed in the Search Results.

Step 4. Click **Add new** to add a new string if no results are displayed.

Step 5. Specify the required SNMP information and save the configuration.

Note: Only SNMP Read Only (RO) Access is needed.

Start CTI Service

Perform the procedure for the Cisco Unified Communications Manager node you desire, it is preferable to set on two nodes.

Step 1. Log into the Cisco Unified Serviceability, viewed in the Cisco Unified Communications Manager graphical user interface.

Step 2. Navigate to **Tools > Service Activation**.

Step 3. Select a server from the drop-down list.

Step 4. From the CM Services section, check the **Cisco CTI Manager** check box.

Step 5. Select **Save** at the top of the screen

Create Application User for PCA CTI Control (JTAPI User)

JTAPI is used to retrieve the session status information from the device. You must create an Application user for CTI Control 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 Application user to help Cisco Prime Collaboration get the required information.

In order to create a new JTAPI Application user follow these steps:

Step 1. Log into the Cisco Unified CM Administration web interface through your administrator account.

Step 2. Create a user group with sufficient privileges. Navigate to **User Management>User Settings>Access Control Group** and create a new user group with a suitable name, **PC_HTTP_Users** in this case. Now, select **Save**.

Step 3. Choose **User Management>User Settings>Access Control Group** and click **Find**. Find the group you defined and select the icon on the right.

Step 4. Click **Assign Role to Group** and select these roles:

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

Step 5. Select **Save**.

Step 6. From the main menu, navigate to **User Management>Application Users>Create a new user**.

Specify a suitable password on the **Application User Configuration** page. You can select 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 (=).

Step 7. In the **Permission Information** section, select **Add to Access Control Group** and select the group that was created in Step 1. (for example, PC_HTTP_Users).

Step 8. Click **Save**. The page is refreshed and the right privileges are displayed.

Note: If the Call Manager was managed prior to the add of the JTAPI User, ensure the JTAPI user is added in the Credential Profile for the Call Manager and rediscover it.

Continued from Scenario 1. Steps:

Step 3. Navigate to the Call Manager JTAPI Application user you created, and move the supported endpoints from Available Devices to Controlled Devices.

You can perform this by the Device Association function as shown in the image.

The screenshot displays the 'Application User Configuration' interface. At the top, there is a header bar with the title 'Application User Configuration' and a toolbar containing 'Save', 'Delete', 'Copy', and 'Add New' icons. Below the header, the 'Status' section shows 'Status: Ready'. The 'Application User Information' section includes fields for 'User ID*' (JTAPIUser), 'Password', 'Confirm Password', 'Digest Credentials', 'Confirm Digest Credentials', and 'BLF Presence Group*' (Standard Presence group). There are also several checkboxes for 'Accept Presence Subscription', 'Accept Out-of-dialog REFER', 'Accept Unsolicited Notification', and 'Accept Replaces Header'. The 'Device Information' section features two lists: 'Available Devices' (Auto-registration Template, BAT205D23177001, Sample Device Template with TAG usage examples, TCTTEST, TCTTEST2) and 'Controlled Devices' (SEP00059A3B7700, SEP00506004ECB3, SEP0050600CF7EB, SEP00562B04CFA8, SEP005F8693E4A0). A 'Device Association' button and a 'Find more Route Points' button are also visible.

If you refer back to the limitation of Endpoints Set to Limited or Full Visibility Per OVA you can verify the amount of devices you have added to the OVA size.

Within this screen, you can filter by Device Name, Description or Directory Number to help you

manage and filter these devices as shown in the image.

It is useful to note these devices as it is added in Step 7.

User Device Association											
	Select All		Clear All		Select All In Search		Clear All In Search		Save Selected/Changes		Remove All Associated
User Device Association (1 - 14 of 14)											
Find User Device Association where Name begins with <input type="text"/> Find Clear Filter											
<input checked="" type="checkbox"/> Show the devices already associated with user											
<input type="checkbox"/>			Device Name								
<input checked="" type="checkbox"/>			SEP00059A3B7700	1000							
<input checked="" type="checkbox"/>			SEP00506004ECB3	1011							
<input checked="" type="checkbox"/>			SEP0050600CF7EB	1030							
<input checked="" type="checkbox"/>			SEP00562B04CFA8	1003							
<input checked="" type="checkbox"/>			SEP005F8693E4A0	1010							
<input checked="" type="checkbox"/>			SEP7426ACEF09C7	1005							
<input checked="" type="checkbox"/>			SEP7426ACF35AE7	1006							
<input checked="" type="checkbox"/>			SEPD0C789141410	1007							

Ensure as well the correct User Roles are added for this JTAPI User:

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf as shown in the image.

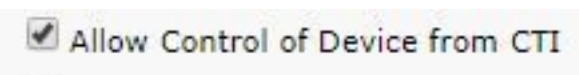
Permissions Information

Groups: JTAPIUser [View Details](#)

Roles: Standard CTI Allow Call Monitoring, Standard CTI Allow Control of Phones supporting Conne, Standard CTI Enabled [View Details](#)

For a list of supported devices per PCA, in regards to conferences and our supported sessions, refer back to Background Information section.

Note: Additionally, ensure that the devices controlled by the CTI Application User have the Allow Control of Device from CTI check box checked under device information as shown in the image.




Note: It is important to note before you proceed that if you do have the endpoints registered to Call Manager and Call Manager is integrated with VCS/TMS, then you discover your VCS/TMS first, then discover your Call Manager last. This way from the inventory


perspective, all of your infrastructure is mapped to the correct location. In addition, when you Discover the VCS/TMS ensure you change the default Discover tab to the respective device of TMS/VCS or Call manager.

Step 4. Next in PCA, select **Device Discovery** and input in the IP Addresses of your Call Managers, select the two check boxes on **Auto-Configuration** and select **Run Now** as shown in the image.

Discover Devices ✕

 Manage Credentials

→

 Device Discovery

i Ensure creating Cluster information using "Manage TMS Cluster" UI before discovering TMS cluster. * Indicates required field

Job Name

Check Device Accessibility

Discover

*IP Address i

Associate to Domain (Optional)

If you have SIP trunks configured between the desired "Communications Manager" cluster and other "Communications Manager" clusters, please exclude all the Destination IPs of those SIP trunks in the Discovery Filter while triggering Logical Discovery.

▼ Auto-Configuration

Add the Prime Collaboration server as a CDR Destination in the Unified CM servers i

Add the Prime Collaboration server as a Syslog Destination in the Unified CM servers i

▶ Filters

▶ Advanced Filters

BackScheduleRun Now

Step 5. After the Call Managers are in a Managed state, proceed to Step 6.

Note: If the Call Manager is not in a managed state, it is most of the time due to HTTP or SNMP, if further assistance is needed open a TAC case to get the call manager in a Managed state.

Step 6. Navigate to **Inventory > Inventory Schedule > Cluster Data Discovery Schedule** and select **Run Now**.

Note: This is dependant on how many registered/non-registered devices you have. This process may take anywhere from a few minutes to a few hours. Check throughout the day by a refresh of the page. As well, this maps your Call Manager cluster together and retrieves all of your endpoints. After this is complete, proceed to the next step.

Note: It is important to mention in the PCA inventory if there are any endpoints where you want to have conference statistics that are supported. Ensure that these are well managed for reports and all the statistics, to show the correct information.

Step 7. Navigate to **Diagnose > Endpoint Diagnostics**.

In order to obtain upto date statistics for your conference endpoints you need to set their visibility to the highest level possible that is allowed by the system.

Select all the endpoints you want to monitor in the Conference Diagnostics then click **Edit Visibility** and then select **Full Visibility** as shown in the image.

Limited Visibility only shows the device within the topology but no statistics and it is not able to retrieve applicable alarms for those devices related to Conference Diagnostics.

Endpoints

Run Tests Edit Visibility

Endpoint Name	Directo	Registration Status
SEP00562B04C...	1003	Registered [SIP]
Deskex90 Desk...	405733	Registered [SIP]
SEP7426ACEF...	1005	Registered [SIP]
SEP005F8693E...	1010	Registered [SIP]
SEP0050600CF...	1030	Registered [SIP]
Desk8945 Desk...	405733	Registered [SIP]
DeskDX80	405733	Registered [SIP]
SEPE4C722640...	1040	Registered [SIP]

Edit SEP00562B04CFA8 and 7 more

Full Visibility Limited Visibility Off

Full Visibility: Displays Conference Statistics in the Conference Diagnostics page
Limited Visibility: Does not display Conference Statistics in the Conference Diagnostics page
Off Visibility: Does not display the endpoint in the Conference Diagnostics page

Save Cancel

The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
<ul style="list-style-type: none"> • CTS 500, 1000, and 3000 Series • Cisco Codec • Cisco TelePresence SX20 • Cisco TelePresence MXP Series • Cisco IP Video Phone E20 	Full	Full
<ul style="list-style-type: none"> • Cisco Jabber Video for TelePresence (Movi) • Polycom 	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
<ul style="list-style-type: none"> • Cisco SX80 and Cisco SX10 • • Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800 	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: <ul style="list-style-type: none"> • Cisco Jabber • Cisco TelePresence MX Series • Cisco TelePresence System EX Series • Cisco TelePresence System SX Series 	Limited	Limited

Note: If you select, for example, 10 endpoints and select Full Visibility it selects the highest level of visibility support per device.

Step 8. In order to test, navigate to **Diagnose > Conference Diagnostics** and a Conference In progress or completed shows, as shown in the image.

The screenshot displays the Cisco Prime Collaboration Assurance interface for Conference Diagnostics. At the top, it shows the Cisco logo and 'Prime Collaboration Assurance' title. The main navigation bar includes 'Diagnose / Conference Diagnostics'. Below this, there are filters for 'Group' (All) and 'Time Range' (10/6/2017-10/6/2017). A table lists 'Video Collaboration Conferences' with columns for 'Conference Subject', 'Scheduler', and 'Start Time'. A specific conference is selected, showing its ID 'SEP7426ACF35AE7 - SEP7426ACEF09C7'. To the right, a topology diagram shows two devices connected: 'DX 70' and 'DX 80'. Below the table, 'Endpoint Statistics: SEP7426ACEF09C7' are shown, including 'System Information' (Physical Location, Device Model: DX80, IP Address: 10.201.196.207, Host Name: SEP7426ACEF09C7, Software Type: PHONE, Software Version: sipdx80.10-2-4-7dev, Last Discovered: 2017-Oct-06 11:25:36 CDT, Serial Number: FOC1825N7S3) and 'Conference Statistics' for Video and Audio.

Category	Metric	Value
Video	Avg Period Latency	203 ms
	Avg Period Jitter	3 ms
	Resolution	640 * 360
	DSCP In	NONE(0)
Audio	Avg Period Latency	1 ms
	Avg Period Jitter	0 ms
	DSCP In	NONE(0)

Within these conferences you are able to view the Average Packet loss, latency and Jitter for Audio and Video calls.

Also, obtain a topology of the Session and the devices involved.

Currently, the Conference Diagnostics pulls the information based off of DN and if your environment has shared DN's, PCA retrieves the first one it receives for the conference.

Conference Relatable Alarms

For Conference Diagnostics you are able to receive three different Alarms for any session and set their thresholds:

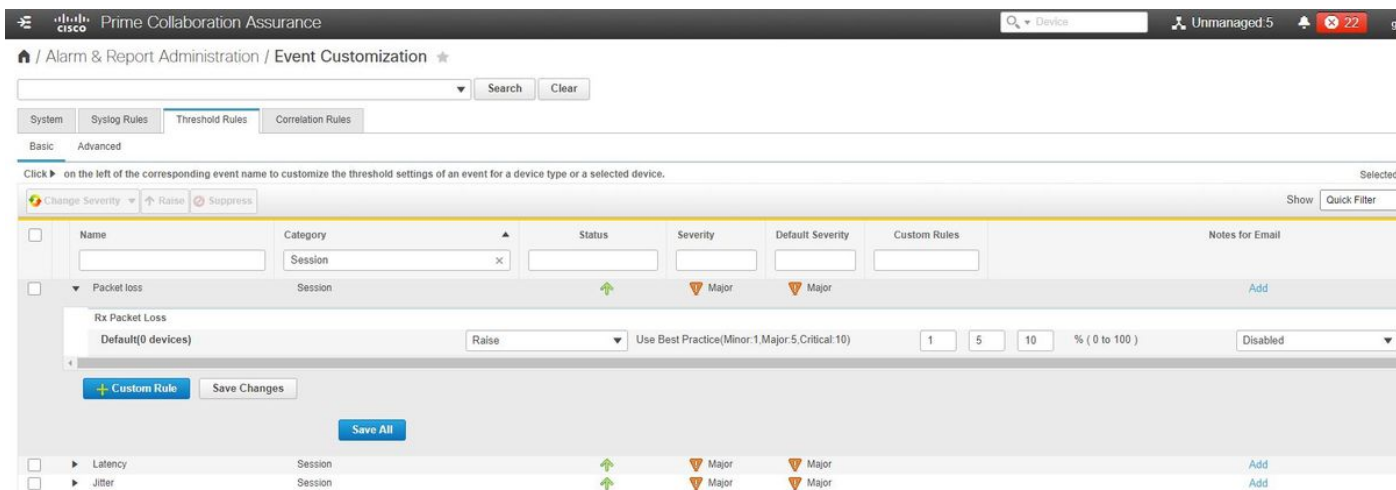
- Packet Loss
- Latency
- Jitter

For each of these, you can modify the default threshold, suppress it or define what devices you would like associated to this alarm.

Step 1. Navigate to **Alarm & Report Administration > Event Customization**.

Step 2. Select **Threshold Rules** and ensure you have **Basic** selected.

Step 3. Scroll down or filter to your right for the Category Named Session as shown in the image.



Step 4. Select the drop down arrow that is next to the alarm. You want to modify and you can modify the Minor, Major or Critical percentages for Packet Loss, Jitter or Latency.

Step 5. If you would like to surpress then switch the Raise to Surpress.

Step 6. If you would like to define the endpoints associated to the alarm you can select Custom Rule.

Step 7. Next, Select the **Device Type > Select All Devices** or **Selectable Devices** that you want for this alarm and click **Save**.

Conference Relatable Reports

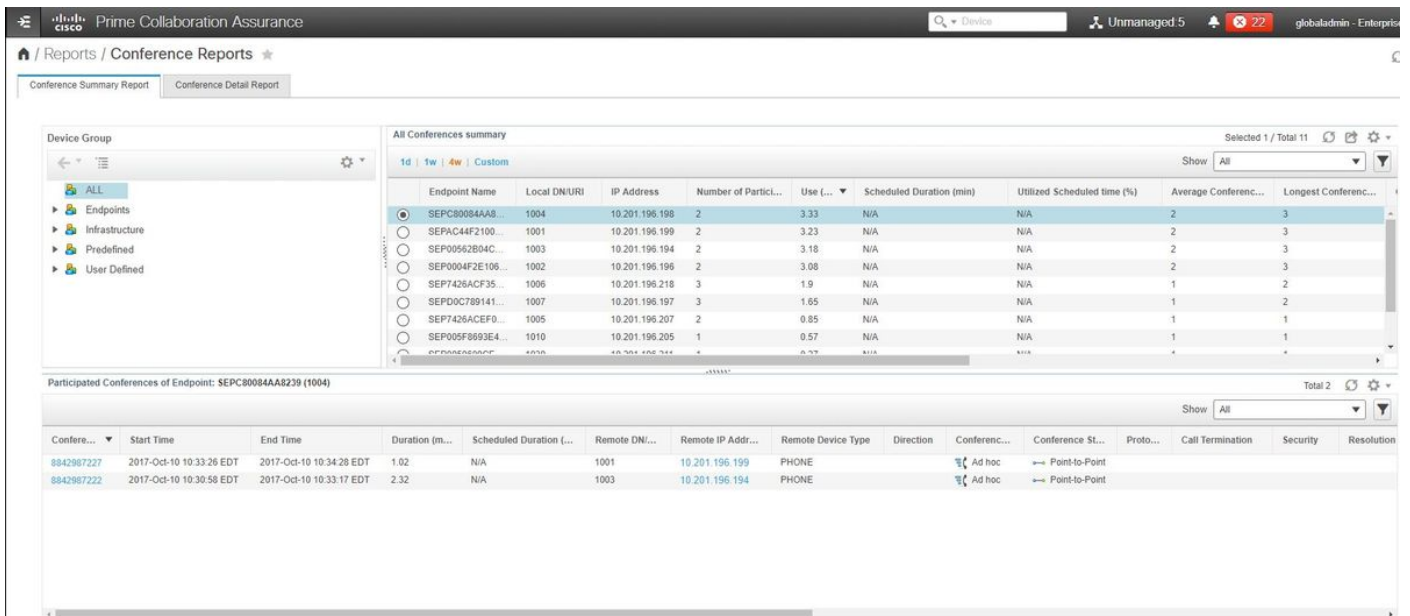
For the Conference Diagnostics reports can be retrieved and viewed.

There are two reports:

- Conference Reports
- Telepresence Endpoint Reports

For Conference Reports, you can view a list of all conferences within a time-frame from one to four weeks or a custom period of time as needed.

Step 1. Navigate to **Reports > Conference Reports** as shown in the image.



Conference Summary Reports

This reports delivers a view of every endpoint that you have selected as limited/full visibility and their conferences.

Statistics shown here are:

- Average Conference Usage
- Alarms related to the conference
- Average Packet Loss, Jitter and Latency
- Longest Conference

This can help you achieve a granular view into issues where you can have within your Voice/Video network to determine which endpoints have the most issues.

Also, you can utilize your bandwidth in correspondance per usage.

Conference Detail Report Tab

If you do encounter an alarm for a Conference you can navigate to the **Conference Detail Report** Tab.

Once you select the Conference, you can refine it to find the Endpoint name, Software version and other details you may be interested in.

For Telepresence Endpoint Reports, you can view per endpoint the:

- Number of conferences this device had
- Utilization percentage
- Endpoint Model
- Usage

In addition, you can change the Utilization Paramaters by the **Change Utilization** Tab as shown in the image.

Change Utilization Settings for Endpoint Model: DX70



Work Hours per Day

Work Days per Week

This sets the parameters for that device so the system knows from the usage what percentage to display.

The No Show Endpoint Summary Report displays the Endpoints that had missed scheduled Conferences.

Within this graph, you can also view the Endpoint and how many Total Scheduled Conferences and how many of these did occur and were no shows.

Conference Video Test Call

You can create point-to-point video test calls between two video endpoints in managed state, to test your network. You can see events and alarms, session statistics, endpoint statistics, and network topology with statistics like other calls. Only the CTS, C and EX series codecs are supported for this call.

In addition, this can be used to validate everything is functional with conference diagnostics.

Prerequisites

- This feature is not supported for E20 codec series.
- In order to use this feature, CLI credentials must be added for the endpoints.
- Ensure that the endpoints are registered and JTAPI is enabled for endpoints (if they are registered to Unified CM).
- The Video Test Call feature is not available, if you have deployed Cisco Prime Collaboration in MSP mode.

Step 1. Navigate to **Diagnose > Endpoint Diagnostics**.

Step 2. Select two applicable endpoints as per the prerequisites mentioned.

Step 3. Select **Run Tests > Video Test Call**.

Step 4. You can schedule the Video Test Call to run Now or on a re-occurrence schedule.

Step 5. This Video Test Call then shows in the Conference Diagnostics Screen.

Scenario 2. Conference with Non Call Manager Registered Endpoints

Step 1. Ensure that the Telepresence Management Suite (TMS) and Video Communications

Server(s) (VCS) credentials are available.

Note: When you discover your VCS/TMS in this scenario, the discovery process is important. If you do have a call manager in your setup, discover the conductor first then the Cisco Call Manager.

Step 2. Navigate to **Inventory > Inventory Management > Manage Credentials > Select Add** and then enter the information for your TMS, while you create a separate credential Profile for your VCS's as shown in the image.

Discover Devices

Manage Credentials → Device Discovery

VCS-C-E VCS/EXPRESSWAY 10.201.202.56|1...

*Profile Name VCS-C-E * Indicates required field

Device Type VCS/EXPRESSWAY (Optional)

*IP Version v4

*Apply this credential to the given IP address 10.201.202.56|10.201.202.57

General SNMP Options

SNMP Timeout 10 seconds

SNMP Retries 2

*SNMP Version 2c

SNMP V2

*SNMP Read Community String

*Re-enter SNMP Read Community String

SNMP Write Community String


Re-enter SNMP Write Community String

Save Next


Step 3. Once the credential profile is created, select **Device Discovery**, enter the **ip addresses** and in the Discovery tab select **VCS** and discover the VCS devices. Also, select **TMS** for the TMS and enter in it's ip address. Click **Run Now** as shown in the image.

Discover Devices



 Manage Credentials

→

 Device Discovery

i Ensure creating Cluster information using "Manage TMS Cluster" UI before discovering TMS cluster. * Indicates required field

Job Name

Check Device Accessibility

Discover

***IP Address** **i**

Associate to Domain (Optional)

If you have SIP trunks configured between the desired "Communications Manager" cluster and other "Communications Manager" clusters, please exclude all the Destination IPs of those SIP trunks in the Discovery Filter while triggering Logical Discovery.

▶ **Filters**

▶ **Advanced Filters**

▼ **Schedule**

Start Time Date: (yyyy/MM/dd hh:mm AM/PM)

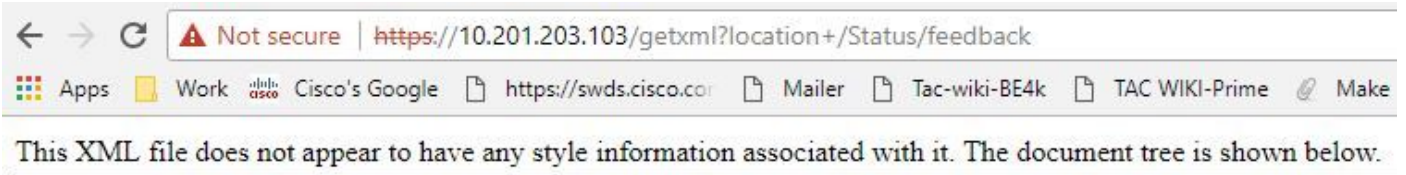
Recurrence None Hourly Daily Weekly Monthly

Step 4. Ensure the VCS and TMS are in a Managed state.

Note: If the VCS or TMS is not in a managed state, it is most of the time due to HTTP or SNMP, if further assistance is needed open a TAC case to get the VCS/TMS in a Managed state.

Note: Use this url and replace the IP_Address_of_VCS_Server with the appropriate IP Address once the VCS is in a Managed state. The PCA server must be registered as a feedback server to VCS, this ensures that when a conference session ends there is no issue with the data VCS sends back to PCA.

https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedback , the http credentials are requested and once input, you must receive a response as shown in the image.



```
<Status xmlns="http://www.tandberg.no/XML/CUIL/1.0" product="TANDBERG VCS" version="X8.9">
  <SystemUnit item="1">
    <Product item="1">TANDBERG VCS</Product>
    <Uptime item="1">935228</Uptime>
    <SystemTime item="1">2017-10-27 16:50:05</SystemTime>
    <TimeZone item="1">US/Central</TimeZone>
    <LocalTime item="1">2017-10-27 11:50:05</LocalTime>
  <Software item="1">
    <Version item="1">X8.9</Version>
    <Build item="1">oak_v8.9.0_rc_2</Build>
    <Name item="1">s42700</Name>
    <ReleaseDate item="1">2016-11-24</ReleaseDate>
    <ReleaseKey item="1">5026834098101150</ReleaseKey>
  <Configuration item="1">
    <NonTraversalCalls item="1">750</NonTraversalCalls>
    <TraversalCalls item="1">100</TraversalCalls>
    <Registrations item="1">0</Registrations>
    <TPRoom item="1">50</TPRoom>
    <UserDevice item="1">50</UserDevice>
    <Expressway item="1">False</Expressway>
    <Encryption item="1">True</Encryption>
    <Interworking item="1">True</Interworking>
    <FindMe item="1">True</FindMe>
    <DeviceProvisioning item="1">True</DeviceProvisioning>
    <DualNetworkInterfaces item="1">False</DualNetworkInterfaces>
    <AdvancedAccountSecurity item="1">True</AdvancedAccountSecurity>
    <StarterPack item="1">False</StarterPack>
    <EnhancedOCSCollaboration item="1">False</EnhancedOCSCollaboration>
    <ExpresswaySeries item="1">True</ExpresswaySeries>
  </Configuration>
</SystemUnit>
</Status>
```

Note: If Prime Collaboration is not subscribed to VCS through HTTP feedback subscription, it is not to be notified by the VCS when a registered endpoint joins or leaves a session, or registers or unregisters to VCS. In this case, set the visibility of those endpoint(s) to full or limited as required and ensure your VCS is in a Managed state.

Step 5. Navigate to **Inventory > Inventory Schedule > Cluster Data Discovery Schedule** and select **Run Now**.

Note: This process can take some time as it performs this function across all infrastructure devices. Therefore, if it does not complete after a few minutes, re-check after 1-2 hours. Very large systems can take up to 4 hours. It is important to mention in the PCA inventory if there are any endpoints where you want to have conference statistics that are supported and that you also ensure these as well are managed for reports and all statistics to show the proper information.

For a list of supported devices as per PCA in regards to conferences and our supported sessions, refer to the Background Information section.

Step 6. Navigate to **Diagnose > Endpoint Diagnostics**.

In order to obtain correct statistics for the conference endpoints, you need to set their visibility to the highest level possible allowed by the system.

Select all the endpoints you want to monitor in the Conference Diagnostics then click **Edit**

Visibility and then select the maximum visibility.

The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
<ul style="list-style-type: none">• CTS 500, 1000, and 3000 Series• Cisco Codec• Cisco TelePresence SX20• Cisco TelePresence MXP Series• Cisco IP Video Phone E20	Full	Full
<ul style="list-style-type: none">• Cisco Jabber Video for TelePresence (Movi)• Polycom	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
<ul style="list-style-type: none">• Cisco SX80 and Cisco SX10• • Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: <ul style="list-style-type: none">• Cisco Jabber• Cisco TelePresence MX Series• Cisco TelePresence System EX Series• Cisco TelePresence System SX Series	Limited	Limited

Note: If you select, for example, 10 endpoints and select Full Visibility it selects the highest level of visibility support per device.

Step 7. In order to test, navigate to **Diagnose > Conference Diagnostics** and a Conference In progress or completed is as shown in the image.

Within these conferences you are able to view the Average Packet loss, latency and Jitter for Audio and Video calls.

Also, you obtain a topology of the Session and the devices involved.

Conference Relatable Alarms

For Conference Diagnostics, you are able to receive three different Alarms any session and set their thresholds:

- Packet Loss
- Latency
- Jitter

Each of these you can modify the default threshold, disable it entirely or define what devices you would like associated to this alarm.

Step 1. Navigate to **Alarm & Report Administration >Event Customization**.

Step 2. Select **Threshold Rules** and ensure you have **Basic** selected.

Step 3. Scroll down or filter to your right for the Category Named Session as shown in the image.

Step 4. Select the drop down arrow next to the alarm you want to modify and you can modify the Minor, Major or Critical percentages for Packet Loss, Jitter or Latency.

Step 5. If you would like to suppress it then switch the Raise to Suppress.

Step 6. If you would like to define the endpoints associated to the alarm you would select Custom Rule.

Step 7. Next, Select **Device Type** > Select **All devices** or **Selectable devices** that you want for this alarm and click **Save**.

Conference Relatable Reports

For the Conference Diagnostics reports can be retrieved and viewed.

There are two reports:

- Conference Reports
- Telepresence Endpoint Reports

For Conference Reports, you can view a list of all conferences within a time-frame from one to four weeks or a custom period of time as needed.

Step 1. Navigate to **Report > Conference Reports** as shown in the image.

The screenshot shows the Cisco Prime Collaboration Assurance interface for Conference Reports. The main view is titled 'All Conferences summary' and displays a table with the following data:

Endpoint Name	Local DN/URI	IP Address	Number of Partic...	Use (...)	Scheduled Duration (min)	Utilized Scheduled time (%)	Average Conferenc...	Longest Conferenc...
SEPC80084A8...	1004	10.201.196.198	2	3.33	N/A	N/A	2	3
SEPAC44F2100...	1001	10.201.196.199	2	3.23	N/A	N/A	2	3
SEP00562B04C...	1003	10.201.196.194	2	3.18	N/A	N/A	2	3
SEP0004F2E106...	1002	10.201.196.196	2	3.08	N/A	N/A	2	3
SEP7426ACF35...	1006	10.201.196.218	3	1.9	N/A	N/A	1	2
SEPD0C789141...	1007	10.201.196.197	3	1.65	N/A	N/A	1	2
SEP7426ACEF0...	1005	10.201.196.207	2	0.85	N/A	N/A	1	1
SEP005F8693E4...	1010	10.201.196.205	1	0.57	N/A	N/A	1	1

Below the main table, there is a section for 'Participated Conferences of Endpoint: SEPC80084A8239 (1004)' showing a detailed table of conference records:

Confere...	Start Time	End Time	Duration (m...	Scheduled Duration (...)	Remote DN/...	Remote IP Addr...	Remote Device Type	Direction	Conferec...	Conference St...	Proto...	Call Termination	Security	Resolution
8842987227	2017-Oct-10 10:33:26 EDT	2017-Oct-10 10:34:28 EDT	1.02	N/A	1001	10.201.196.199	PHONE		Ad hoc	Point-to-Point				
8842987222	2017-Oct-10 10:30:58 EDT	2017-Oct-10 10:33:17 EDT	2.32	N/A	1003	10.201.196.194	PHONE		Ad hoc	Point-to-Point				

Conference Summary Reports

This reports delivers a view of every endpoint you have selected as limited/full visibility and their conferences.

Statistics shown here are:

- Average Conference Usage
- Alarms related to the conference
- Average Packet Loss, Jitter and Latency
- Longest Conference

This can help you achieve a granular view into issues you may have within your Voice/Video network to determine which endpoints have the most issues.

As well utilize your bandwidth in correspondance per usage

Conference Detail Report Tab

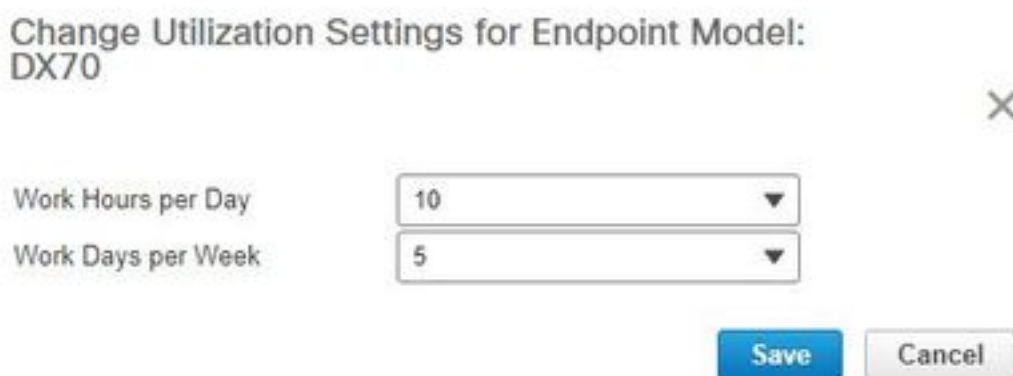
If you do encounter an alarm for a Conference, you can navigate to the Conference Detail Report Tab.

Once you select the Conference you can refine to find the Endpoint name, Software version and other details you may be interested in.

For Telepresence Endpoint Reports you can view per endpoint the-

- Number of conferences this device had
- Utilization percentage
- Endpoint Model
- Usage

In addition, you can change the Utilization Paramaters by the Change Utilization Tab as shown in the image.



Change Utilization Settings for Endpoint Model:
DX70

Work Hours per Day: 10

Work Days per Week: 5

Save Cancel

This sets the parameters for that device so the system knows from the usage what percentage to display.

The No Show Endpoint Summary Report displays the Endpoints that had missed scheduled Conferences.

Within this graph, you can view the Endpoint and how many Total Scheduled Conferences and how many of these did occur and were no shows.

Conference Video Test Call

You can create point-to-point video test calls between two video endpoints that are in a managed state, to test your network. You can see events and alarms, session statistics, endpoint statistics, and network topology. Only the CTS, C and EX series codecs are supported for this call.

In addition, this can be used to validate all functionality is correct with conference diagnostics.

Prerequisites

- This feature is not supported for E20 codec series.
- In order to use this feature, CLI credentials must be added for the endpoints.
- Ensure that the endpoints are registered and JTAPI is enabled for endpoints (if they are registered to Unified CM).
- The Video Test Call feature is not available if you have deployed Cisco Prime Collaboration in MSP mode.

Step 1. Navigate to **Diagnose > Endpoint Diagnostics**.

Step 2. Select two applicable endpoints as per the prerequisites.

Step 3. Select **Run Tests > Video Test Call**.

Step 4. You can schedule the Video Test Call to run Now or on a re-occurrence schedule.

Step 5. This Video Test Call then shows in the Conference Diagnostics Screen.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Logs to Collect for Troubleshooting

Step 1. Navigate to **System Administration > Log Management**.

Step 2. Scroll down to the module and select **Session Monitoring** and select **Edit** as shown in the image.

🏠 / System Administration / Log Management ★

✎ Edit ↶ Reset to Default 📄 Download Log		
	Module	Log Level
37	Sensor Keep alive	Error
38	Sensor Registration	Error
39	Sensor Skinny	Error
40	Sensor TopN	Error
41	Service Level View Server	Error
42	Service Quality Manager	Error
43	Session Monitoring	Debug

Step 3. Change the log level to debug and click **Save**.

Step 4. Reproduce the issue then come back to the Log Management Screen.

Step 5. After you reproduce the issue, select **Session Monitoring** and select **Download Log**.

Step 6. After you download, extract the zip file.

Step 7. Open up the zip file and navigate to the locations for useful logs:

`/opt/emms/emsam/log/SessionMon/`

- CUCMJTAPI.log
- CUCMJTAPIDiag.log
- CSMTracker
- CSMTrackerDiag.log
- CSMTrackerDataSource.log
- PostInitSessionMon.log