



Cisco Prime Collaboration Assurance - Advanced and Analytics Guide, 12.1 Service Pack 3

First Published: 2019-04-17

Last Modified: 2021-03-15

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I

Get Started with Cisco Prime Collaboration 21

CHAPTER 1

Overview of Cisco Prime Collaboration Assurance and Analytics 1

Overview of Cisco Prime Collaboration Assurance 1

Document Conventions 1

Cisco Prime Collaboration Assurance - Advanced 3

Cisco Prime Collaboration Assurance - Advanced Features 10

Voice and Video Unified Dashboard 10

Device Inventory/Inventory Management 10

Voice and Video Endpoint Monitoring 11

Diagnostics 12

Fault Management 12

Reports 12

Cisco Prime Collaboration Assurance Support for IPv6 13

Overview of Cisco Prime Collaboration Assurance—MSP Mode 15

Differences Between the Enterprise Mode and the MSP Mode 19

Cisco Prime Collaboration Assurance NBI 21

Cisco Prime Collaboration Assurance and Analytics Geo-Redundancy 22

New and Changed Information 22

What's New in Cisco Prime Collaboration Assurance 26

Overview of Cisco Prime Collaboration Analytics 34

Cisco Prime Collaboration Analytics NBI 35

CHAPTER 2

Concepts 39

Concepts 39

Event 39

Alarm	40
Event Creation	40
Alarm Creation	41
Event and Alarm Association	41
Event Aggregation	42
Event Masking	42
Alarm Status	42
Event Severity	43
Event and Alarm Database	44
Alarm Notifications	44

CHAPTER 3	Get Started with Cisco Prime Collaboration Assurance	45
	Get Started with Cisco Prime Collaboration Assurance	45
	Get Started with Cisco Prime Collaboration Assurance	45
	Get Started with Cisco Prime Collaboration Analytics	50

PART II	Set Up the Server	53
----------------	--------------------------	-----------

CHAPTER 4	Enable Third-Party CA Signed Certificate	55
	Enable Third-Party CA Signed Certificate	55
	Install CA signed certificate	55

CHAPTER 5	Manage Licenses	59
	Manage Licenses	59
	Cisco Prime Collaboration Assurance Licensing	59
	Cisco Prime Collaboration Analytics Licensing	60
	Adding Analytics License	60
	Enable and Disable Analytics	60
	Cisco Prime Collaboration Contact Center Assurance Licensing	61
	License Count	61
	Endpoint Count in Cisco Prime Collaboration Assurance	62
	View License Details	62
	Add and Delete a License File	64

Switch Between Advanced Evaluation to Advanced (Purchase License) in Cisco Prime Collaboration Assurance 64

CHAPTER 6

Manage Users 65

Manage Users 65

Cisco Prime Collaboration Assurance-Advanced User Roles 65

Single Sign-On for Cisco Prime Collaboration Assurance 67

Default User Accounts 69

User Roles and Tasks 69

Add a User 70

Modify User Roles 70

Configure an LDAP Server 71

LDAP Configuration Parameters 71

Configure Maximum Length for Password 74

Unlock Cisco Prime Collaboration Assurance Account 74

CHAPTER 7

Manage Customers 75

Manage Customers 75

Add Customers 75

Global Customer Selection 76

CHAPTER 8

Manage Domains 77

Manage Domains 77

Manage Domains 77

Add Domains 77

Global Domain Selection 78

CHAPTER 9

Configure System Parameters 79

Configure System Parameters 79

Global System Parameters 80

Configure SMTP Server 81

Configure Cisco Prime Collaboration Assurance Server Time Zone 81

PART III

Manage Devices in Cisco Prime Collaboration Assurance 83

CHAPTER 10**Manage Device Credentials 85**

- Manage Device Credentials 85
- Add a Device Credentials Profile 86
 - Credential Profiles Field Descriptions 87
- SSL Certificate Authentication for Device Discovery 97
- Modify Device Credentials 98
- Verify Device Credentials 98
 - Credential Verification Error Messages 99
- Delete a Device Credential Profile 101

CHAPTER 11**Set Up Clusters 103**

- Set Up Clusters 103
 - Manage Cisco TelePresence Manager or Cisco TMS Clusters 103

CHAPTER 12**Discover Devices 105**

- Discover Devices 105
 - Discovery Life Cycle 105
 - Removal of Devices from Cisco Prime Collaboration Assurance on Deletion 108
 - Discovery Methods 108
 - Prerequisites and Recommendations 115
 - Automatic Discovery of Devices 121
 - Discovery Filters and Scheduling Options 125
 - Manual Discovery of Devices 126
 - Import Devices 128
 - Export Device Lists and Credentials 129
 - Troubleshooting 130
 - Discovery of Cisco Unified Computing System (UCS) 130
 - Configure vCenter 132
 - Unified CM Cluster Data Discovery 133
 - Schedule Cluster Device Discovery 134
 - Rediscover Devices 135
 - Verify Discovery Status 136
 - Troubleshooting 136

CHAPTER 13	Manage Device Groups	139
	Manage Device Groups	139
	About Device Groups	139
	Create Groups	142
	Add Devices to a Group	142
	Remove Devices from a Group	143
	Device Group Selector	143

CHAPTER 14	Manage Inventory	145
	Manage Inventory	145
	View Inventory Details	145
	Inventory Pane	146
	Device 360° View	150
	Global Search Options for Cisco Prime Collaboration Assurance	155
	Inventory Summary	157
	Device Status Summary	157
	Troubleshooting	159
	Inventory Status Error Messages	160
	Device-Specific Inventory Details	161
	Update and Collect Inventory Details	175
	Update Inventory	176
	Job Schedule - Field Descriptions	177
	Inventory Details Collection	178
	Suspend and Resume Managed Devices	178
	Delete Devices	179
	Performance Graphs	180
	Unified CM Device Search	185
	SNMP Query	186

CHAPTER 15	Poll Devices	189
	Poll Settings	189
	Overview	189
	Polling Parameters— Settings	191

View Polling Parameters 191

Edit Polling Parameters 191

PART IV

Monitor Faults 193

CHAPTER 16

Configure Notifications 195

Configure Notifications 195

Notification Groups 196

Notification Criteria 197

Types of Notifications 197

SNMP Trap Notifications 199

Configure SMTP Server 205

Syslog Notifications 206

Notifications Limited to Specific Alarms 207

Add an Alarm Set 207

Add a Device Notification Group 208

General Information Field Descriptions 209

Set up Destinations Field Descriptions 210

CHAPTER 17

Set Threshold Rules 213

Set Threshold Rules 213

Threshold Rules 213

Configure TelePresence Endpoint Threshold—Device Level 215

Configure TelePresence Endpoint Thresholds—Global 216

Configure Thresholds for Conference Troubleshooting 216

Enable Automatic Troubleshooting for TelePresence Endpoints 217

Overview of Device Pool Thresholds 217

Edit Device Pool Thresholds 219

Overview of Voice Call Grade Settings 219

Add Dynamic Syslogs 220

Correlation Rules 222

Create Custom Alerts 225

Custom Alert Parameters 226

System 227

CHAPTER 18	Monitor Alarms and Events	229
	Monitor Alarms and Events	229
	Alarms and Alarm Summary	229
	Events	232
	View Call Events	233
	Notes for Alarms and Events	234

PART V	Monitor the Network	237
---------------	----------------------------	------------

CHAPTER 19	Monitor Video Endpoints	239
	Monitor Video Endpoints	239
	Endpoint Diagnostics Dashboard	239
	Troubleshooting	242
	View User 360 Details	243
	Manage a Video Test Call	244

CHAPTER 20	Monitor Conferences	247
	Monitor Conferences	247
	Data Collection for Video Conferences	249
	Import Conferences from Cisco TMS	251
	Conference Workflow and Scenarios	252
	Conference Diagnostics Dashboard	258
	Realtime Visibility of an Endpoint	262
	360° Conference View	265
	Conference Topology	265
	Endpoint Statistics	268

CHAPTER 21	Enable Cisco APIC-EM to Troubleshoot Conference	269
	Enable Cisco APIC-EM to Troubleshoot Conference	269
	Overview of Cisco APIC-EM	269
	Cisco APIC-EM Controller Integration Settings	270
	Conference Troubleshooting with Cisco APIC-EM	271

CHAPTER 22	Monitor the Cisco Prime Collaboration Assurance Server	273
	Monitor the Cisco Prime Collaboration Assurance Server	273
PART VI	Dashboards and Reports	279
CHAPTER 23	Cisco Prime Collaboration Assurance Dashboards	281
	Cisco Prime Collaboration Assurance Dashboards	281
	Ops View	284
	Summary	288
	Endpoint by Device Pool	290
	Topology—Cisco Unified Communications Manager or Cisco TelePresence Video Communication Server Cluster	290
	Connected Devices	295
	Performance	295
	Route Pattern Summary	295
	Device Search	296
	Endpoint Registration Summary	296
	Availability Summary	297
	Service Experience/Call Quality	297
	Top 5 Poor Voice Call Quality Locations	297
	Top 5 Call Failure Locations	298
	Top 10 TelePresence Endpoints with Call Quality Alarms	299
	Conference with Alarms	299
	Alarm Dashboard	299
	Top 10 TelePresence Endpoints with Alarms	299
	Top 10 Devices with Alarms	299
	Infrastructure Alarm Summary/Device Alarm Summary	300
	Utilization Monitor	300
	Trunk Utilization	300
	T1/E1 Trunks	302
	CUBE SIP Trunk	302
	UCM SIP Trunks	304
	Route Group Utilization	305

Trunk Group Utilization	306
Location CAC Bandwidth Usage	306
Conferencing Devices	307
Conductor Bridge Pool Utilization	308
TelePresence Endpoint	308
License Usage	311
Customer Summary Dashboard	314
Contact Center Assurance Dashboards	316
Contact Center Assurance Topology Dashboard	317
View Historical Trends	319
Customer Voice Portal (CVP)	320
Unified Contact Center Enterprise (Unified CCE)	329
Cisco Unified Intelligence Center	337
Cisco MediaSense	345
Cisco Unified Contact Center Express	350
Virtualized Voice Browser	354
Performance Dashboards	358
Unified CM and Unity Connection	359
View Historical Trends	372
Create Custom Performance Dashboards	373
Add a Customized Dashboard	375

CHAPTER 24

Cisco Prime Collaboration Assurance Reports	377
Cisco Prime Collaboration Assurance Reports	377
Prerequisites to Generate the Cisco Prime Collaboration Assurance Reports	377
Update Call Detail Records NAM Credentials	378
Add Credential for Prime NAM	378
Delete Credentials for Multiple Prime NAMs	379
Verify Credentials for Multiple Prime NAMs	379
Add Multiple NAM Credentials	380
Import Credentials for Prime NAMs	381
Credential Verification - Error Messages	381
Use NAM Credentials to Troubleshoot Problems and Verify Credentials	382
Call Classification	383

Understand OffNet and OnNet Calls	385
Call Category Creation	385
Create Custom Call Category	385
Dial Plan Addition	386
Understand the Default Dial Plan	386
Add a Dial Plan	390
Edit a Dial Plan	392
Delete a Dial Plan	392
Configure Gateway Codes	393
Configure SFTP Settings	393
SFTP Settings Page - Field Descriptions	394
Administrative Reports	396
CDR & CMR Call Report	397
Generate CDR & CMR Reports	404
Troubleshoot	407
NAM & Sensor Report	408
Understand Sensor Reports	413
View Sensor Stream Correlation Data	413
Session Reports/Conference Reports	416
All Session/Conference Summary Report	417
Session/Conference Detail Report	417
TelePresence Endpoint Reports	418
Endpoint Utilization Report	418
No Show Endpoint Summary Report	419
Launch CUCM Reports	419
Miscellaneous Reports	419
UCM/CME Phone Activity Reports	419
Endpoint Move Report	420
Endpoint Audit Report	420
Endpoint Remove Report	420
Endpoint Extension Report	420
Understand the Time Period Covered by Audio IP Phone Activity Reports	421
Track Phone Status when Cisco Unified CM Is Down	421
Voice Call Quality Event History Reports	421

Other Reports	422
CTI Applications Report	423
ATA Devices Report	423
Cisco 1040 Sensors Report	423
Conferencing Device Video Port Utilization Report	423
Scheduled Reports	424
Generate Scheduled Reports	426
Access Data for Reports that Contain More than 2,000 Records	427
Troubleshoot File Download Issues	427

PART VII
Analyzing the Network 429

CHAPTER 25
Analytics Dashboards and Reports 431

Cisco Prime Collaboration Analytics Dashboards and Reports	431
Cisco Prime Collaboration Analytics User Roles	431
Global Customer Selection	432
Global Domain Selection	432
User Interface	432
Managing Customer Logo	436
Configure sFTP Server	437
Prerequisites for Data Population in the Cisco Prime Collaboration Analytics Dashlets	438
Technology Adoption	438
Deployment Distribution by Endpoint Model	439
Call Distribution by Endpoint Model	440
Call Distribution by Endpoint Types	441
Technology Usage	442
Asset Usage	442
Least Used Endpoint Types	443
Video TelePresence Rooms Utilization	443
No Show Video TelePresence Endpoint	443
Traffic Analysis	444
Top N Callers	445
Top N Dialed Numbers	445
Top N Off-Net Traffic Locations	445

Top N Call Traffic Locations	447
Call Traffic Analysis	447
Capacity Analysis	448
Analytics Group Management	448
Location CAC Bandwidth Utilization	449
Trunk Utilization	449
Busy-Hour Trunk Capacity	450
Route Group/Trunk Group Utilization	452
Busy-Hour Route-Group Capacity	453
DSP Utilization	454
Service Experience	454
Service Experience Distribution	455
Endpoints with Service Quality Issues	456
Top N Call Failure Locations	457
Users with Service Quality Issues	458
Call Grade for Locations	458
Video Conferences	459
Video Conference Statistics	459
Top N Video Conference Locations	460
Conferencing Devices Video Utilization	461
Conductor Bridge Pool Utilization	461
UC System Performance	462
License Usage	462
Contact Center Enterprise	463
Customer Voice Portal	463
My Dashboard	464
Custom Report	465
Creating Custom Reports	466
Scheduled Reports	466
Troubleshooting Prime Collaboration Analytics Dashboard	468

PART VIII
Perform Diagnostics 471

CHAPTER 26
Diagnostics for Voice Endpoints 473

Diagnostics for Voice Endpoints	473
Phone Status Test	473
Create a Phone Status Test	474
Import Phone Status Test	475
Synthetic Test	477
Prerequisites for Synthetic Tests	479
Create an Emergency Call Synthetic Test	479
Create a Message-Waiting Indicator Synthetic Test	481
Create a TFTP Download Synthetic Test	481
Create an HTTP Download Synthetic Test	482
Create an End-to-End Call Synthetic Test	482
Create Dial-Tone Synthetic Tests	484
Create a Phone Registration Test	484
Import Synthetic Tests	485
Manage Synthetic Tests	491
Synthetic Test Notes	492
IP SLA Voice Tests	493
Required Cisco IOS and IP SLA Versions	496
Create an IP SLA Voice Test	496
Import Multiple IP SLA Voice Tests	501
Manage IP SLA Voice Tests	503
IP SLA Voice Test Data	505
Create a Batch Test	512
Format Batch Test Import Files	512
Manage Batch Tests	513
Phone Tests—Batch and On Demand Tests	515
Create a Phone Test on Demand	517
Audio Phone Features Test	519
Troubleshooting	524
CME Diagnostics	524
Monitoring IP Phones Using Cisco Unified CME Syslog Messages	525
 CHAPTER 27	
Troubleshooting Workflow for Video Endpoints	527
Troubleshooting Workflow for Video Endpoints	527

Features of the Troubleshooting Workflow	529
Features of the Troubleshooting Workflow for Conferences	530
Features of the Troubleshooting Workflow for Endpoints	531
Support Matrix for Troubleshooting Source and Destination Endpoints	531
Start a Troubleshooting Workflow	533
Troubleshoot Data Analysis	534
Troubleshooting	534
Path Statistics	539
Export Troubleshooting Data	542
Understand the Export Troubleshooting Report	543
Cisco Prime Infrastructure Cross-Launch	544
Cross-Launch Cisco Prime Infrastructure	545

CHAPTER 28
Media Path Analysis 547

Media Path Analysis	547
Analyze Media Paths Using VSAA	547
VSA Agent Assessment Results	548

CHAPTER 29
Collect Logs 551

Collect Logs	551
Log Collection Center/Device Log Collector	552
Set the Trace Levels	554
Log Collection Template	555
Collect Call Logs	555

CHAPTER 30
Analyze Call Signaling 557

Analyze Call Signaling	557
Supported Call Flows	559
Create a Call Ladder Diagram	560
Filter a Message in the Call Ladder Diagram	563
Understand a Call Ladder Diagram	563

PART IX
Maintain the Server 565

CHAPTER 31	Manage Jobs 567
	Manage Jobs 567
	Schedule a Job 569
	Defining a Timetable 570
	Cancel a Job 571
	Predefined Quick Filters 571
CHAPTER 32	Purge Policies 573
	Purge Policies 573
	Purge Policies Table 573
CHAPTER 33	Perform Backup and Restore 575
	Perform Backup and Restore 575
	Overview of Backup and Restore 575
	Backup Time Period 576
	Create a Repository on FTP, Disk, SFTP, or TFTP Server 576
	Schedule Backup using Cisco Prime Collaboration Assurance and Analytics User Interface 578
	Troubleshooting 580
	Backup Cisco Prime Collaboration Assurance Data using CLI 580
	Check the Backup History 580
	Restore Data on the Same System 581
	Restore on a New System 581
CHAPTER 34	Set Log Levels 583
	Set Log Levels 583
	Log Levels 583
PART X	Unified Communication Operations Dashboard 585
CHAPTER 35	Getting Started with Unified Communication Operations Dashboard 587
	Unified Communication Operations Dashboard 587
	Introduction to Unified Communication Operations Dashboard 587
	Install Responder in PCA 587

Launch UC Operations Dashboard	588
Register the Master IP Address	588
Unified Communication Operations Landing page	588

CHAPTER 36 Threshold Settings 591

Introduction to Threshold Settings	591
Threshold Settings	591
Threshold Parameters	591

CHAPTER 37 System Settings 593

System Settings	593
Add or Delete Associated Responders	593
Set the Job Frequency	594
Set the Shared Secret Key	595

CHAPTER 38 Responder Settings 597

Introduction to Responder Settings	597
Enable Responder	597
Set the Shared Secret Key	597
Registration Status	598

CHAPTER References 599

APPENDIX A Synthetic Test Worksheet 601

Synthetic Test Worksheet	601
--------------------------	-----

APPENDIX B Cisco 1040 Sensor Management 605

Cisco 1040 Sensor Management	605
Overview of Cisco Prime NAM/vNAM	605
Perform Initial Configuration in Cisco Prime Collaboration Assurance	605
Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files	606
Add and Delete a TFTP Server	606
Set Up the Cisco 1040 Sensor Default Configuration	607
Configure Cisco 1040 Sensors in Cisco Prime Collaboration Assurance	608

Cisco 1040 Sensor Details	608
Add a Cisco 1040 Sensor	610
Edit Configurations for Multiple Cisco 1040s	611
Cisco 1040 Management - Field Descriptions	611
Reset Cisco 1040s	612
Delete a Cisco 1040 Sensor	612
View Diagnostic Information on a Cisco 1040	613
APPENDIX C Troubleshooting Secure JTAPI Connection	615
Troubleshooting Secure JTAPI Connection	615
APPENDIX D TLS Configuration for Jetty and Tomcat Server	617
Enable Minimum TLS Version for Cisco Prime Collaboration Assurance Client Connections	617
Enable TLS Protocol for Jetty Server	618
Enable TLS Protocol for Tomcat Server	618
APPENDIX E User Interface	621
Overview	621
Filters	622
Launch the Advanced Filter and Save Filter Criteria	623
Quick View	624
View About Details	624



PART I

Get Started with Cisco Prime Collaboration

- [Overview of Cisco Prime Collaboration Assurance and Analytics, on page 1](#)
- [Concepts, on page 39](#)
- [Get Started with Cisco Prime Collaboration Assurance, on page 45](#)



CHAPTER 1

Overview of Cisco Prime Collaboration Assurance and Analytics

This section provides an overview of Cisco Prime Collaboration Assurance and Analytics.

- [Overview of Cisco Prime Collaboration Assurance, on page 1](#)
- [Overview of Cisco Prime Collaboration Assurance—MSP Mode, on page 15](#)
- [Differences Between the Enterprise Mode and the MSP Mode, on page 19](#)
- [Cisco Prime Collaboration Assurance NBI , on page 21](#)
- [Cisco Prime Collaboration Assurance and Analytics Geo-Redundancy, on page 22](#)
- [New and Changed Information, on page 22](#)
- [What's New in Cisco Prime Collaboration Assurance, on page 26](#)
- [Overview of Cisco Prime Collaboration Analytics, on page 34](#)

Overview of Cisco Prime Collaboration Assurance

This document provides information on Cisco Prime Collaboration Assurance 11.0, 11.1, 11.5, 11.6, 12.1, and 12.1 SP1 features.

Cisco Prime Collaboration Assurance is a comprehensive video and voice service assurance and management system with a set of monitoring, and reporting capabilities that help you receive a consistent, high-quality video and voice collaboration experience.

Document Conventions

The following conventions are used in the document for different releases of Cisco Prime Collaboration Assurance:

- Renamed “Session” to “Conference” in all the relevant sections.



Note The word “Session” is still applicable to Cisco Prime Collaboration Assurance Release 11.1 and earlier.

- Renamed “Log Collection Center” to “Device Log Collector” in all the relevant sections.



Note The word “Log Collection Center” is still applicable to Cisco Prime Collaboration Assurance Release 11.1 and earlier.

- Renamed “Call Signalling Analyzer” to “SIP Call Flow Analyzer” in all the relevant sections.



Note The word “Call Signaling Analyzer” is still applicable to Cisco Prime Collaboration Assurance Release 11.1 and earlier.

- “Troubleshooting” is not supported in Cisco Prime Collaboration Assurance Release 11.5.



Note “Troubleshooting” is still applicable to Cisco Prime Collaboration Assurance Release 11.1 and earlier.

- The **Limited Visibility** option is not supported in any dashboards from Cisco Prime Collaboration Assurance 12.1 and later. Click on **Edit Visibility** to either switch on the **Full Visibility** option or switch it OFF.
- “FIPS Compliance” is not supported in Cisco Prime Collaboration Assurance Release 12.1.



Note “FIPS Compliance” is still applicable to Cisco Prime Collaboration Assurance Release 11.6 and earlier.

- “Credential Profile” feature is not supported in the Cisco Prime Collaboration Assurance Release 11.6 MSP Mode.



Note With this, the TelePresence endpoints are shown as Inaccessible.

- “Smart Licensing” feature is not supported in the Cisco Prime Collaboration Assurance Release 12.1.
- The “Video Test Call” feature is not supported for Endpoints registration through the Mobile and Remote Access (MRA) solution.
- LDAP configuration with SSL enabled is not supported in the Cisco Prime Collaboration Assurance Release 12.1.
- Additional tab like CUCM SFTP Credentials and Save are introduced in the User Interface. A field to change the smuser password and options to confirm password options are available. Change in Navigation from **Alarm & Report Administration** -> **CDR Source Settings** -> **CUCM SFTP Credentials** to **Inventory** -> **Inventory Management** -> **CUCM SFTP Credentials** in the Cisco Prime Collaboration Assurance Release 12.1 Service Pack 3.
- CDR Source Settings Dashlet along with Manage Call Quality Data Source Settings page is removed from the Cisco Prime Collaboration Assurance User Interface for Release 12.1 Service Pack 3.

Cisco Prime Collaboration Assurance - Advanced

Cisco Prime Collaboration Assurance is available in the following modes:

- Cisco Prime Collaboration Assurance Advanced—Enterprise and MSP mode

For installing Advanced Assurance, see the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#).

Cisco Prime Collaboration Assurance Advanced is a comprehensive video and voice service assurance and management system with a set of monitoring, and reporting capabilities that help ensure that you receive a consistent, high-quality video and voice collaboration experience.

- The Enterprise mode provides a single enterprise view or multiple domains view within your enterprise. This option is usually used in a standard single enterprise environment.
- The MSP mode provides multiple customer views. This option is used in managed service provider environments. This view allows you to view the devices of multiple customers that are being managed. For more information on the MSP mode, See the *Overview of Cisco Prime Collaboration Assurance—MSP Mode* section in [Cisco Prime Collaboration Assurance Guide - Advanced](#).

The following table lists the features available in Cisco Prime Collaboration Assurance - Advanced.

Feature	Advanced	See Cisco Prime Collaboration Assurance Guide - Advanced
Supported Modes	It supports both the Enterprise and MSP modes.	For more information on Advanced features, see the sections <i>Overview of Cisco Prime Collaboration Assurance—MSP Mode</i> and <i>Differences Between the Enterprise Mode and the MSP Mode</i> .
License Requirement	Requires license after evaluation expiry.	For more information on Advanced features, see the section <i>Manage Licenses</i> .

Role Based Access Control	<p>Supports five roles to provide multiple levels of authorization:</p> <ul style="list-style-type: none"> • Super Administrator • System Administrator • Network Administrator • Operator • Helpdesk <p>For Cisco Prime Collaboration Release 11.5 and later</p> <p>Supports six roles to provide multiple levels of authorization:</p> <ul style="list-style-type: none"> • Super Administrator • System Administrator • Network Administrator • Operator • Helpdesk • Report Viewer 	For more information on Advanced features, see the section <i>Manage Users</i> .
Single Sign-On Support	Yes	For more information on Advanced features, see the section <i>Manage Users</i> .
Cluster Management	Manages multiple clusters with mixes of cluster revisions and cluster associations.	For more information on Advanced features, see the section <i>Set Up Clusters</i> .

Discovery	<ul style="list-style-type: none"> You can discover and manage all endpoints that are registered to Cisco Unified CM (phones and TelePresence), Cisco VCS (TelePresence), and Cisco TMS (TelePresence). In addition to managing the endpoints, you can also manage multipoint switches, application managers, call processors, routers, and switches that are part of your voice and video collaboration network. Provides multiple discovery modes such as Auto Discovery, Import, and Add Device features. Supports Logical Discovery, Ping Sweep, CDP-based discovery for discovering devices. Provides the option to perform rediscovery. <p>For Cisco Prime Collaboration Release 11.5 and later</p> <p>Note CTS-Manager (TelePresence) device is not supported.</p>	For more information on Advanced features, see the section <i>Discover Devices</i> .
Inventory Management	<ul style="list-style-type: none"> Provides a concise summary information for a device through the Device 360 view. Provides exhaustive Inventory details. 	For more information on Advanced features, see the section <i>Manage Inventory</i> .
Fault Management	<ul style="list-style-type: none"> For Cisco Prime Collaboration Release 11.1 and earlier Support for initiating troubleshooting by using quick views. Supports Alarm Correlation rules. Supports customization of events at the device, and global level. Provides configuration of thresholds for: <ul style="list-style-type: none"> TelePresence Endpoints Infrastructure Device Call Quality Device Pool 	For more information on Advanced features, see the section <i>Monitor Alarms and Events</i> .

Voice and video Reports	<p>Provides the following predefined reports and customizable reports:</p> <ul style="list-style-type: none"> • Administrative Reports • Communications Manager Reporting • Interactive Reports • Scheduled Reports 	For more information on Advanced features, see the section <i>Dashboards and Reports</i> .
Dashboard	<p>Provides the following dashboards:</p> <ul style="list-style-type: none"> • Ops View - Provides high-level information about the Cisco Unified CM and VCS Clusters. • Service Experience - Provides information about quality of service. • Alarm - Provides information about alarm summaries. • Performance - Provides details on critical performance metrics of each managed element. • Contact Center Topology - Provides information about the Contact Center components such as CUIC, Finesse, MediaSense, CVP, and Unified CCE. <p>You can add customized dashboards in the Home page.</p>	For more information on Advanced features, see the section <i>Dashboards and Reports</i> .

Dashboards	<p>For Cisco Prime Collaboration Release 11.5 and later</p> <p>Provides the following dashboards:</p> <ul style="list-style-type: none"> • Ops View - Provides high-level information about the Cisco Unified CM and VCS Clusters. • Call Quality - Provides information about quality of service. • Alarm - Provides information about alarm summaries. • Performance - Provides details on critical performance metrics of each managed element. • Contact Center Topology - Provides information about the Contact Center components such as CUIC, Finesse, MediaSense, CVP, and Unified CCE. <p>You can add customized dashboards in the home page.</p> <p>You can also do the following:</p> <ul style="list-style-type: none"> • Add the existing dashlets to a different dashboard. • Move the dashlets around under a dashboard by dragging and dropping them. 	<p>For more information on Advanced features, see the section <i>Dashboards and Reports</i>.</p>
------------	--	--

Voice and Video Endpoint Diagnostics	<p>For Cisco Prime Collaboration Release 11.1 and earlier</p> <ul style="list-style-type: none"> • Provides a detailed analysis of the end-to-end mediapath, including specifics about endpoints, service infrastructure, and network-related issues. • Uses Cisco Medianet technology to identify and isolate video issues. • Provides mediapath computation, statistics collection, and synthetic traffic generation • Uses the IP SLA to monitor the availability of key IP phones in the network. • Predicts service outage using scheduled synthetic and IP SLA tests. <p>For Cisco Prime Collaboration Release 11.5 and later</p> <ul style="list-style-type: none"> • Uses the IP SLA to monitor the availability of key IP phones in the network. • Predicts service outage using scheduled synthetic and IP SLA tests. 	For more information on Advanced features, see the section <i>Perform Diagnostics</i> .
Job Management	Enables you to view, schedule, and delete jobs.	For more information on Advanced features, see the section <i>Manage Jobs</i> .
Cross Launch to UC Application	Yes	-
Cross Launch to Cisco Prime Collaboration Assurance Serviceability	Yes	-
Device Search	Global Search - Provides filtered search for TelePresence, endpoints, phones, other devices, locations, and users.	For more information on Advanced features, see the section <i>Global Search Options for Cisco Prime Collaboration Assurance</i> .

Cisco Prime Collaboration Analytics	<p>Helps you to identify the traffic trend, technology adoption trend, over used resources, and under used resources in your network. You can also track intermittent and recurring network issues and address service quality issues using the Analytics Dashboards. The Analytics dashboards are:</p> <ul style="list-style-type: none"> • Technology Adoption • Asset Usage • Traffic Analysis • Capacity Analysis • Call Quality • UC System Performance • Scheduled Reports • Video Conferences • Custom Report Generator <p>Note For Cisco Prime Collaboration Release 11.1 and earlier</p> <p>Cisco Prime Collaboration Analytics is not supported in MSP mode deployment.</p> <p>Cisco Prime Collaboration Analytics is a licensed software, which has to be purchased separately with Cisco Prime Collaboration Assurance.</p>	See Cisco Prime Collaboration Analytics Guide .
NB API	<p>NB API is supported for the following:</p> <ul style="list-style-type: none"> • Managing devices • Viewing and deleting device credentials • Listing all video conferences • For Cisco Prime Collaboration Release 11.1 and earlier <p>Troubleshooting video conferences</p>	<p>To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server with the administrator privilege and enter</p> <p><code>http://<pc-server-ip>/emsam/nbi/nbiDocumentation</code></p> <p>in the browser URL;</p> <p>where, pc-server-ip is the Cisco Prime Collaboration Assurance server IP address.</p> <p>For Cisco Prime Collaboration Release 11.6 and later</p> <p>To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server and select Assurance NB API documentation from Settings drop-down menu at the top right corner of the user interface.</p>

Cisco Prime Collaboration Assurance - Advanced Features

Cisco Prime Collaboration Assurance enables you to monitor your network and perform diagnostics. In addition, you can run reports that help you identify the source of problems.

Voice and Video Unified Dashboard

The Cisco Prime Collaboration Assurance dashboards enable end-to-end monitoring of your voice and video collaboration network. They provide quick summaries of the following:

Dashboard	Description	Cisco Prime Collaboration Assurance Options
Service Experience	Information about quality of service.	Cisco Prime Collaboration Assurance Advanced
Alarm	Information about Alarm summaries.	Cisco Prime Collaboration Assurance
Performance	Provides details on critical performance metrics of each managed element.	Cisco Prime Collaboration Assurance Advanced
Contact Center Topology	Information about the Unified Contact Center Topology View.	Cisco Prime Collaboration Contact Center Assurance

For Cisco Prime Collaboration Release 11.5 and later

Dashboard	Description	Cisco Prime Collaboration Assurance Options
Call Quality	Information about quality of service.	Cisco Prime Collaboration Assurance Advanced
Alarm	Information about Alarm summaries.	Cisco Prime Collaboration Assurance
Performance	Provides details on critical performance metrics of each managed element.	Cisco Prime Collaboration Assurance Advanced
Contact Center Topology	Information about the Unified Contact Center Topology View.	Cisco Prime Collaboration Contact Center Assurance

See “Prime Collaboration Dashboards” to learn how the dashlets are populated after deploying the Cisco Prime Collaboration Assurance servers.

Device Inventory/Inventory Management

You can discover and manage all endpoints that are registered to Cisco Unified Communications Manager (phones and TelePresence), Cisco Expressway (TelePresence), and Cisco TMS (TelePresence). In addition to managing the endpoints, you can also manage multipoint switches, application managers, call processors, routers, and switches that are part of your voice and video collaboration network.

As part of the discovery, the device interface and peripheral details are also retrieved and stored in the Cisco Prime Collaboration Assurance database.

After the discovery is complete, you can perform the following device management tasks:

- Group devices into user-defined groups.
- Edit visibility settings for managed devices.
- Customize event settings for devices.
- Rediscover devices.
- Update inventory for managed devices.
- Suspend and resume the management of a managed device.
- Add or remove devices from a group.
- Manage device credentials.
- Export device details.

See [Manage Inventory](#) to learn how to collect the endpoints inventory data and how to manage them.

Voice and Video Endpoint Monitoring

Service operators must quickly isolate the source of any service degradation in the network for all voice and video conferences in an enterprise.

For Cisco Prime Collaboration Release 11.1 and earlier

Cisco Prime Collaboration Assurance provides a detailed analysis of the end-to-end media path, including specifics about endpoints, service infrastructure, and network-related issues.

For video endpoints, Cisco Prime Collaboration Assurance enables you to monitor all Point-to-point, Multisite, and Multipoint video collaboration conferences. These conferences can be ad hoc, static, or scheduled with one of the following statuses:

- In-progress
- Scheduled
- Completed
- No Show

Cisco Prime Collaboration Assurance periodically imports information from:

- The management applications (Cisco TMS) and conferencing devices (CTMS, Cisco MCU, and Cisco TS) on the scheduled conferences.
- The call and conferences control devices (Cisco Unified CM and Cisco Expressway) shown on the registration and call status of the endpoints.

In addition, Cisco Prime Collaboration Assurance continuously monitors active calls supported by the Cisco Collaboration System and provides near real-time notification when the voice quality of a call fails to meet a user-defined quality threshold. Cisco Prime Collaboration Assurance also allows you to perform call classification based on a local dial plan.

See [Prerequisites for Setting Up the Network for Monitoring](#) in Cisco Prime Collaboration Network Monitoring, Reporting, and Diagnostics Guide, 9.x and later to understand how to monitor IP Phones and TelePresence.

Diagnostics

Cisco Prime Collaboration Assurance uses Cisco Medianet technology to identify and isolate video issues. It provides media path computation, statistics collection, and synthetic traffic generation.

When network devices are Medianet-enabled, Cisco Prime Collaboration Assurance provides:

- Flow-related information along the video path using Mediatrace.
- Snapshot views of all traffic at network hot spots using Performance Monitor.
- The ability to start synthetic video traffic from network devices using the IP Service Level Agreement (IP SLA) and Video Service Level Agreement Agent (VSAA) to assess video performance on a network.

For IP phones, Cisco Prime Collaboration Assurance uses the IP SLA to monitor the availability of key phones in the network. A phone status test consists of:

- A list of IP phones to test.
- A configurable test schedule.
- IP SLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the IP phones. Optionally, it also pings from the Cisco Prime Collaboration Assurance server to IP phones.

For Cisco Prime Collaboration Release 11.5 and later

Cisco Medianet technology is not supported.

Cisco Prime Collaboration Assurance enables you to collect call logs to identify faults in the calls for Cisco Voice Portal (CVP), Unified Contact Center Enterprise (Unified CCE), Cisco Unified Communications Manager (Unified CM), and IOS Gateways. This feature enables you to troubleshoot issues in the calls. You can use the SIP Call Flow Analyzer feature to further zoom in on the collected calls and isolate faults in the messages. It also helps you to recreate the issue as you can view the call ladder diagram that indicates faults in the call messages and provides the root cause and recommendations.

Fault Management

Cisco Prime Collaboration Assurance ensures near real-time quick and accurate fault detection. After identifying an event, Cisco Prime Collaboration Assurance groups it with related events and performs fault analysis to determine the root cause of the fault.

Cisco Prime Collaboration Assurance allows to monitor the events that are of importance to you. You can customize the event severity and enable to receive notifications from Cisco Prime Collaboration Assurance, based on the severity.

Cisco Prime Collaboration Assurance generates traps for alarms and events and sends notifications to the trap receiver. These traps are based on events and alarms that are generated by the Cisco Prime Collaboration Assurance server. The traps are converted into SNMPv2c notifications and are formatted according to the CISCO-EPM-NOTIFICATION-MIB.

See [Monitor Alarms and Events](#) to learn how Cisco Prime Collaboration Assurance monitors faults.

Reports

Cisco Prime Collaboration Assurance provides the following predefined reports and customizable reports:

- Administrative Reports — Provides System Status Report, Who Is Logged On Report, and Process Status.

- CDR & CMR Reports — Provides call details such as call category type, call class, call duration, termination type, call release code, and so on
- Conference Reports — Provides the All Conference Summary Report and Conference Detail Report.
- TelePresence Endpoint Reports — Provides details on completed and in-progress conference, endpoint utilization, and No Show endpoints. TelePresence reports also provide a list of conferencing devices and their average and peak utilization in your network.
- Launch CUCM Reports — Enables you to cross launch to the reporting pages for the Cisco Unified Communications Manager clusters.
- Miscellaneous Reports — Provides Other Reports, UCM/CME Phone Activity Reports, and Voice Call Quality Event History Reports.
- Scheduled Reports — Provides utilization and inventory reports. You can generate the reports on the spot or enable scheduling to generate them on predefined days.

See [Cisco Prime Collaboration Assurance Reports](#) to learn the different types of reports and how to generate them.

Cisco Prime Collaboration Assurance Support for IPv6

Cisco Prime Collaboration Assurance supports IPv6 endpoints in IPv6 only and Dual Stack network. The following table details the Cisco Prime Collaboration Assurance feature support for IPv6 endpoints:

Table 1: Cisco Prime Collaboration Assurance Feature Support for IPv6 Devices

Features	Supported	Notes or Limitations
Device Inventory/Inventory - Credential Profile	Creation of IPv6 credential profiles.	—

Features	Supported	Notes or Limitations
Device Inventory/Inventory - Discovery	<ul style="list-style-type: none"> Accept IPv6 credential profiles and is able to match these profiles to IPv6 addresses Is able to ping and reach IPv6 devices When endpoints are registered to Unified CM using IPv4, IPv6, or dual stack, you can see only the active IP addresses (the IP address selected by the Unified CM configuration to communicate with the registered endpoint). When endpoints can be registered to a VCS through IPv4, IPv6, or dual stack, you can see the IP address with which the device has registered to the VCS. 	<ul style="list-style-type: none"> Unified CM, TMS, CTS, and other infrastructure devices can be managed using IPv4 only. Ping sweep discovery does not work on IPv6 subnet.
Device Inventory/Inventory - Inventory Management	Inventory Summary shows IPv6 addresses.	—
Conference Diagnostics	<p>Endpoint Statistics (System and Conference Information) shows IPv6 addresses.</p> <p>Endpoints Quick View shows IPv6 addresses.</p>	—
Endpoint Diagnostics	Endpoint Diagnostics dashboard shows IPv6 addresses.	—
Troubleshooting	—	No troubleshooting support for IPv6 devices.
Dashboards and Reports	Miscellaneous Reports—Voice Call Quality Event History Reports, UCM/CME Phone Activity Reports show IPv6 addresses.	By default the IPv6 addresses column is hidden. You can change the columns displayed by clicking on the Column Filter icon.
Topology	Search for endpoints with IPv6 addresses.	—
Alarm Browser	Alarm Summary shows IPv6 addresses.	—
Phone Search	Search for IPv6 phones.	—

Features	Supported	Notes or Limitations
For Cisco Prime Collaboration Release 11.5 and later		
Technology Adoption Dashboard	IP address filters supports endpoints with IPv6 addresses.	—
Asset Usage Dashboard	IP address filters supports endpoints with IPv6 addresses.	—
Traffic Analysis Dashboard	IP address filters supports endpoints with IPv6 addresses.	—
Service Experience Dashboard	IP address filters supports endpoints with IPv6 addresses.	—

**Note**

- For a dual stack device, only IPv4 IP addresses are shown in the IP address column mentioned earlier, except for UCM/UCE Phone Activity Reports.
- North Bound Interface (NBI) communication is supported only on IPv4 networks.
- Colon (:) cannot be used as a separator in the credential profile patterns or while adding multiple devices.

Overview of Cisco Prime Collaboration Assurance—MSP Mode

Cisco Prime Collaboration Assurance—MSP mode provides multiple customer views. This option is used in managed service provider environments. You can manage the networks of multiple customers better (including Static NAT environments) by implementing restricted access for each of the customers, and separate administration.

**Note**

You can select the MSP mode deployment only during installation.

NAT Environment - Deployment Scenarios

You can manage the customer's endpoints behind NAT in the following scenarios:

- Scenario - Voice endpoints

Audio Phones registered to the Call Controller (configured with the private IP Address of the endpoints) in a NAT environment - Managed in Cisco Prime Collaboration Assurance with Public IP address also referred to as the Managed IP Address.

- Scenario - Voice and Video endpoints

Audio and Video/TelePresence endpoints registered to Call Controller (configured with the private IP Address of the endpoints) in the customer premise in a NAT environment - Managed in Cisco Prime Collaboration Assurance with Public IP address also referred to as the Managed IP Address.

- **For Cisco Prime Collaboration Release 11.1 and earlier**

Scenario - TelePresence provisioned to Cisco TelePresence Exchange (CTX)

TelePresence endpoints provisioned to CTX in a NAT environment - Managed in Cisco Prime Collaboration Assurance with Public IP address also referred to as the Managed IP Address.



Note Cisco Unified Communications Manager processing node (publisher of UCM cluster) query on any call manager returns the publisher IP address or hostname. In NAT environment, you must ensure that the public hostname returned as publisher query output should not be resolved by private DNS configuration in Cisco Prime Collaboration Assurance.

For example: If Public hostname is FQDN, then the Private DNS should be hostname without FQDN or hostname with different FQDN than the public domain.



Note For Cisco Prime Collaboration Release 11.5 and later

The Private IP address of a device for one customer may overlap with the Public IP address of a device for another customer. However, the Public IP address is unique across different customers that are managed in Cisco Prime Collaboration Assurance.

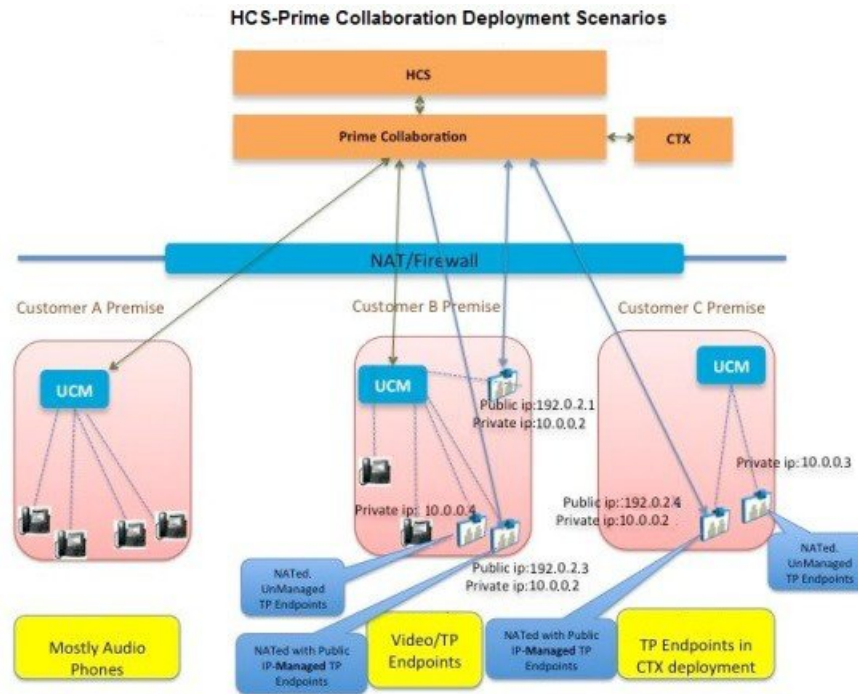
For example, the Private IP address (192.168.1.12) of an IP phone for “Customer A” overlaps with the Public IP address (192.168.1.12) of Unified Communications Manager for “Customer B”. Hence, the NAT IP address may cross-launch to Unified Communications Manager application because of the same Public IP address.

The following diagram displays the HCS-Cisco Prime Collaboration Assurance deployment scenarios in a NAT environment.

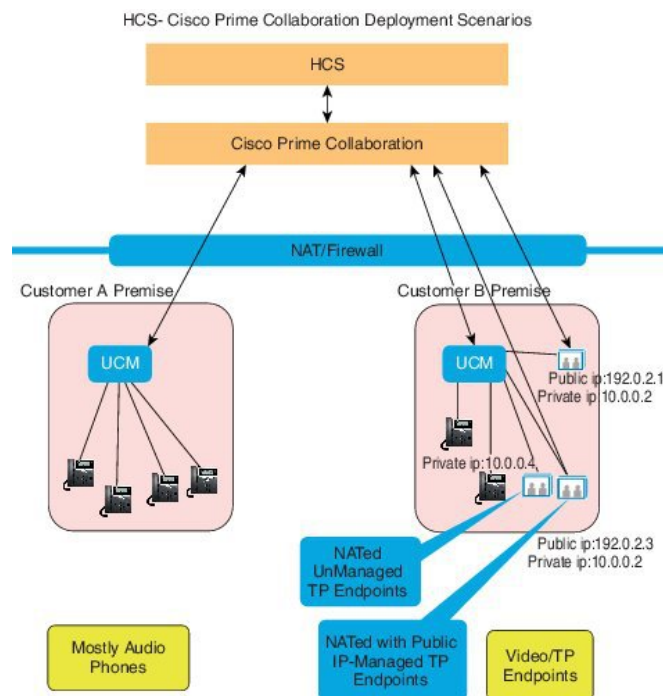


Note The following diagram is applicable to Cisco Prime Collaboration Assurance Release 11.1 and earlier.

Figure 1: Cisco Prime Collaboration Deployment Scenarios



Note The following diagram is applicable to Cisco Prime Collaboration Assurance Release 11.5 and later.



Voice and Video Unified Dashboard

You can do end-to-end monitoring of the voice and video collaboration network of each of your customers separately.

You can view the detailed and exclusive summary for each of your customer's network on the following:

- High-level information about the Cisco Unified Communications Manager and Cisco Video Communication Server clusters
- Conferences and Alarms
- Details about the devices
- Performance of each managed device
- Information about the Contact Center components such as Cisco Unified Intelligence Center (CUIC), Cisco Finesse, Cisco MediaSense, Cisco Unified Customer Voice Portal (Cisco CVP), and Cisco Unified Contact Center Enterprise (Unified CCE)

Device Inventory/Inventory Management

For HCS-specific discovery details, see the [HCS documents](#).

You can view and manage each customer's inventory separately.

You can select the customer for which you want to discover the device. In a non-NAT environment, the Public IP (Managed IP) is populated with the discovered IP Address, and the Private IP is populated as Public IP (Managed IP) by default.

You can discover devices and clusters, and associate them to specific customers. You can choose if you want all existing managed endpoints or subscribers registered to a publisher inherit the customer name from the publisher.

You can discover and manage all endpoints that are registered to Cisco Unified Communications Manager (phones and Cisco TelePresence), Cisco Expressway (Cisco TelePresence), and Cisco TMS (Cisco TelePresence). In addition to managing the endpoints, you can also manage multipoint switches, application managers, call processors, routers, and switches that are part of the customer's voice and video collaboration network.

As part of the discovery, the device interface and peripheral details are also retrieved and stored in the Cisco Prime Collaboration Assurance database.

Voice and Video Endpoint Monitoring

For video endpoints, Cisco Prime Collaboration Assurance enables you to monitor all point-to-point, multipoint, and multipoint video collaboration conferences for individual customers. These conferences can be ad hoc, static, or scheduled with one of the following statuses:

- In-Progress
- Scheduled
- Completed
- No Show

Diagnostics

You can run multiple diagnostics tests to identify issues related to UC phone network of individual customers.

In a NAT environment, Medianet is only supported for endpoints with Public IP addresses. In a NAT environment, video conferences diagnostics is only supported for endpoints with Public IP addresses.

For Cisco Prime Collaboration Release 11.5 and later

Cisco Medianet Technology is not supported.

Fault Management

You can monitor the alarms and events for different customers separately. You can customize the event severity and enable to receive notifications from Cisco Prime Collaboration Assurance, based on the severity.

You can also create customer-specific device notification groups.

Reports

All predefined reports and customizable reports for individual customers are available except the sensor-based reports such as NAM and Sensor reports.

See [Differences Between the Enterprise Mode and the MSP Mode, on page 19](#) for more information on the Enterprise and the MSP modes.

Cisco Prime Collaboration Analytics

For Cisco Prime Collaboration Release 11.5 and later

Following are the new features supported in Cisco Prime Collaboration Analytics:

- **Global Customer Selection**—On the Cisco Prime Collaboration Analytics home page, you can select customers and filter information accordingly.
- **Scheduled Reports**—Multiple customer selection is supported in Scheduled reports. The generated report contains multiple customer data.
- **Logo Management**—Customers can upload, replace, and delete logo. The uploaded logo will be included in the scheduled report.
- **Role Based Access Control**—Report viewer role is supported to all the dashboards except Capacity Analysis, License Usage, and My Dashboard. Report viewer cannot schedule reports and do not have access to the Scheduled Reports menu.

Differences Between the Enterprise Mode and the MSP Mode

The features provided for Cisco Prime Collaboration Assurance are the same for both Enterprise and MSP modes, except for the differences, described in the following table:

Managed Service Provider (MSP) Mode	Enterprise Mode
Comes with Advanced mode only.	Comes with both Advanced mode .

Managed Service Provider (MSP) Mode	Enterprise Mode
Enables you to create customers and add specific devices to them.	Enables you to create logical units in your enterprise called domains. This is an optional feature in the Advanced mode.
Filters information, by customer, Inventory Management, phone inventory reports, conference diagnostics, and endpoint diagnostics.	Filters information, by domains, in the inventory table, Inventory Management, conference diagnostics, and endpoint diagnostics.
Provides dashboards and dashlets on Customer Summary. For Cisco Prime Collaboration Release 11.5 and later Cisco TelePresence Exchange (CTX) is no longer available.	Does not provide dashboards and dashlets on Customer Summary.
IP SLA testing can be performed for a specific customer's routers and switches also.	IP SLA testing is available for all IP SLA-enabled routers and switches.
Provides support for CTX clusters and meeting types supported by CTX. For Cisco Prime Collaboration Release 11.5 and later Cisco TelePresence Exchange (CTX) is no longer available.	Does not support CTX.
Provides Role Based Access Control (RBAC) for customer groups.	Provides Role Based Access Control (RBAC) for assurance device pools and endpoints.
Supports Static NAT.	Does not support NAT.
Supports CTX manageability for both hosted and non-hosted deployment models. For Cisco Prime Collaboration Release 11.5 and later Cisco TelePresence Exchange (CTX) is no longer available.	Does not support CTX.
RTP-based diagnostics tests (for example, Synthetic tests) are only supported in a non-NAT environment.	All functionalities are supported.
In a NAT environment, for phones, the data from Phone XML discovery is not available. Video conference stats and conference information will not be available for phones even if they are set to full visibility.	All functionalities are supported.
Sensor-based call quality reports are not available.	All reports are available.

Managed Service Provider (MSP) Mode	Enterprise Mode
In a NAT environment, the Cisco TelePresence endpoint health monitoring is only supported for Cisco TelePresence endpoints with Public IP addresses.	All functionalities are supported.
In a NAT environment, video conference diagnostics is only supported for endpoints with Public IP addresses.	All features of video conference diagnostics are supported.
Auto Discovery is not supported.	Auto Discovery is supported.
For Cisco Prime Collaboration Release 11.5 and later FIPS Compliance is not supported. For Cisco Prime Collaboration Release 12.1 and later FIPS Compliance is not supported.	For Cisco Prime Collaboration Release 11.5 and later FIPS Compliance is supported. For Cisco Prime Collaboration Release 12.1 and later FIPS Compliance is not supported.
For Cisco Prime Collaboration Release 11.5 and later Perimeta Session Border Controller (SBC) is supported.	Perimeta Session Border Controller (SBC) is not supported.
In a NAT environment, Medianet is only supported for endpoints with Public IP addresses. For Cisco Prime Collaboration Release 11.5 and later Cisco Medianet Technology is not supported.	All features of Medianet are supported. For Cisco Prime Collaboration Release 11.5 and later Cisco Medianet Technology is not supported.
For Cisco Prime Collaboration Release 11.5 and later For Scheduled Reports uploaded in sFTP server, the access to the reports are restricted to the users who created the scheduled reports.	For Cisco Prime Collaboration Release 11.5 and later For Scheduled Reports uploaded in sFTP server, all the users can view the reports.
For Cisco Prime Collaboration Release 11.6 and later Credential Profile feature is not supported.	Credential Profile feature is supported.

Cisco Prime Collaboration Assurance NBI

Cisco Prime Collaboration Assurance NBI support is available for the following:

- Managing devices
- Viewing and deleting device credentials.

- Listing all video sessions based on the filtering criteria.
- Troubleshooting video sessions.
- Get the endpoint count from the Unified CM cluster
- Lists the alarms based on the filtering criteria.

For Cisco Prime Collaboration Release 11.5 and later

Troubleshooting is not supported.

To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server with the administrator privilege and enter the following in the browser URL.

```
http://<pc-server-ip>/emsam/nbi/nbiDocumentation
```

The *<pc-server-ip>* is the Cisco Prime Collaboration Assurance server IP address.

For Cisco Prime Collaboration Release 11.6 and later

To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server and select **Assurance NB API documentation** from Settings drop-down menu at the top right corner of the user interface.

For Cisco Prime Collaboration Release 12.1 and later

```
https://<pc-server-ip>:<port-number>/emsam/nbi/nbiDocumentation
```

Where, *<pc-server-ip>* is the server IP address and *<port-number>* is the HTTP port number.

For example:

```
https://<pc-server-ip>:8443/emsam/nbi/nbiDocumentation
```

In addition to these NBIs, you can configure to send SNMP traps (CISCO-EPM-NOTIFICATION-MIB) to the trap receiver, whenever an alarm or event is raised.

Cisco Prime Collaboration Assurance and Analytics Geo-Redundancy

Cisco Prime Collaboration Assurance and Analytics support Geo-Redundancy through the VMware vSphere replication. You do not need an extra Cisco Prime Collaboration Assurance and Analytics license to configure Geo-Redundancy. For more information on Geo-Redundancy, see [Geo Redundancy for Cisco Prime Collaboration Assurance and Analytics](#).

New and Changed Information

The following table describes the information that has been added or changed in this guide for 12.1 Service Pack 3 update release. A few defects have also been addressed.

Table 2: New and Changed Information

Date	Update
June 06, 2019	You can schedule Endpoints Audit, Endpoints Move, Endpoints Remove, and Endpoints Extension Audit reports and send the generated reports through email notification to the specified email ID.

The following table describes the information that has been added or changed in this guide for 12.1 Service Pack 3 release. Many defects have also been addressed.

Table 3: New and Changed Information

Date	Updates
October 30, 2018	There is a change in the navigation with respect to sFTP Credentials User Interface. Changes are made in the section on "Configure System Parameters" > in the "Table: on System Parameters" and corresponding section on "Configure sFTP Settings".
November 28, 2018	Change in NAM Configuration Screen.
November 02, 2018	Change in CUCM SFTP Server Screen.
November 28, 2018	Change in Set Call Category Screen.
November 28, 2018	Change in Dial Plan Configuration Screen - Create.
December 06, 2018	Change in Dial Plan Configuration Screen - Edit/Delete.
December 05, 2018	CDR Source Settings Removal.
February 14, 2019	Allow password up to 127 characters - not bytes.

The following table describes the information that has been added or changed in this guide for 12.1 Service Pack 2 release.

Table 4: New and Changed Information

Date	Updates
August 21, 2018	New Endpoint Support

Date	Updates
August 24, 2018 September 05, 2018 September 19, 2018	Conference Diagnostics - Following User Stories are addressed - <ul style="list-style-type: none"> • Default Visibility Off • Assurance-Analytics Dashlets for Session Monitoring Off • TC/CE Endpoints Call Feedback Subscription registered to Cisco Unified Communications Manager
September 04, 2018	Section on “Prerequisites” is created for each of the following Cisco Prime Collaboration Assurance and Analytics Reports/Dashlets for Session Monitoring.

The following table describes the information that has been added or changed in this guide for 12.1 Service Pack 1 release.

Table 5: New and Changed Information

Date	Updates
April 10, 2018	Support of TLS v1.2 communication protocol
May 14, 2018	New fields to support secured JTAPI communication with CUCM
July 04, 2018	Secure JTAPI Communication for Session Monitoring

The following table describes the information that has been added or changed in this guide for 12.1 release.

Table 6: New and Changed Information

Date	Updates
July 21, 2017	Added What's New in Cisco Prime Collaboration Assurance section.
March 13, 2017	Updated information on Device Status Summary.
March 14, 2017	Made changes to the existing content on TMS Cluster in the chapter "Set Up Cluster".
March 27, 2017	Audio Phone and Video Phone Audit Reports are merged to a single report "Endpoint Audit Report".
March 31, 2017	Audio Phone and Video Phone Move Reports are merged to a single report "Endpoint Move Report".
April 24, 2017	Removed IP Phone and Removed Video Phone Reports are merged to a single report "Endpoint Remove Report".

Date	Updates
May 30, 2017	Audio Extension and Video Extension Reports are merged to a single report "Endpoint Extension Report".
April 05, 2017 April 17, 2017	There are a few changes with respect to user interface. 1. Handling dependencies for removal of device 2. CUBE SIP Trunk - changes for session server group configuration
March 23, 2017	Updated information in the section "Rediscover Devices" with respect to removal of devices from Cisco Prime Collaboration Assurance on deletion.
June 06, 2017	As part of PIFServer process removal, the following are removed "IP Phone Inventory Collection and IP Phone XML Collection" from Inventory Schedule Page. This change addresses the following aspects: 1. Updated information in the following sections "Configure System Parameters", "Schedule Cluster Data Discovery", "Update and Collect Inventory Details", "Inventory Details Collection", and table "Global System Parameters". 2. Removed sections on "IP Phone Discovery Schedule" and "Schedule IP Phone XML Discovery Schedule".
July 06, 2017	A new section "Monitoring IP Phones Using Cisco Unified CME Syslog Messages" is added that explains the configuration of the syslogs in CME.
July 06, 2017	Updated the section on "License Count" to address the changes made in "Licensing of Registered Endpoints in Inventory".
June 18, 2017	Revamped the section on "Schedule a Job" and added a new section "Defining a Timetable" to address the issue on "Fixing Settings button on Job Management page".
June 18, 2017	The changes related to all audit reports should be purged for data older than 30 days on daily basis are addressed in the section on "Perform Backup and Restore" and to the table on "Purge Policies".
June 18, 2017	Added information to the section on "Manage Licenses > View License Details" to address the change related to "Cisco Prime Collaboration Assurance Licensing User Interface should restrict the maximum license you can import based on each profile (Small/Large/BE6k)".
June 01, 2017	Added a note in the section on "Upgrade Cisco Prime Collaboration Assurance" to address the issue on handling schema changes through Data Migration Assistant Tool.
June 01, 2017	All the occurrences of FIPS Compliance is hidden. As part of Cisco Prime Collaboration Assurance 12.1 Enterprise mode, FIPS compliance is not certified. The entire section on "Enable FIPS Compliance" is hidden.

Date	Updates
May 21, 2017	There is a change in the navigation with respect to sFTP Credentials User Interface. Changes are made in the section on "Configure System Parameters" > in the "Table: on System Parameters" and corresponding section on "Configure sFTP Settings".

What's New in Cisco Prime Collaboration Assurance

You can access the Cisco Prime Collaboration Assurance 12.1 Service Pack 3 features from [Cisco.com](https://www.cisco.com).

Many defects are also addressed along with the Features listed in the table below.

Table 7: Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Features

Feature Name	Feature Description
sFTP Credentials User Interface Implementation	Additional tab like CUCM SFTP Credentials and Save are introduced in the User Interface. A field to change the smuser password and options to confirm password options are available. Change in Navigation from Alarm & Report Administration -> CDR Source Settings -> CUCM SFTP Credentials to Inventory -> Inventory Management -> CUCM sFTP Credentials
Removal of CDR Source Settings	CDR Source Settings Dashlet along with Manage Call Quality Data Source Settings page is removed from the Cisco Prime Collaboration Assurance User Interface.
User Interface Changes	Following are the changes with respect to user interface: <ol style="list-style-type: none"> 1. NAM Configuration Screen. 2. CUCM SFTP Server Screen. 3. Set Call Category Screen. 4. Dial Plan Configuration Screen - Create/Edit/Delete.
Configuration of maximum passphrase of upto 127 characters	Enable users to have strong passwords. Lack of password complexity, particularly password length, significantly reduces the search space when attackers try to guess user passwords, making brute-force attacks much easier. To avoid this, the feature is implemented.

You can access the Cisco Prime Collaboration Assurance 12.1 Service Pack 2 features from [Cisco.com](https://www.cisco.com).

Table 8: Cisco Prime Collaboration Assurance 12.1 Service Pack 2 Features

Feature Name	Feature Description
New Endpoint Support	<p>Supports six new Cisco Endpoints for Cisco Prime Collaboration Assurance.</p> <ul style="list-style-type: none">• ciscoWebExRoom-55• ciscoWebExRoom-70• ciscoWebExRoomKit• ciscoWebExRoomKitPlus• 7832• 8832 <p>For more information, see Supported Devices for Cisco Prime Collaboration Assurance.</p>

Feature Name	Feature Description
Conference Diagnostics	Conference Diagnostics support for Cisco Unified Communications Manager registered Telepresence endpoints (TC/CE).
	The default visibility settings for endpoints is turned to OFF state for new installations (Cisco Prime Collaboration Assurance 12.1 SP2). During upgrade from the previous versions (Cisco Prime Collaboration Assurance 11.6, Cisco Prime Collaboration Assurance 12.1 FCS/ES1/ES2/ES3/ES4/SP1/...) to Cisco Prime Collaboration Assurance SP2, the Installation routine will retain the default visibility settings of the already managed endpoints.
	<p>Section on “Prerequisites” is created for each of the following Cisco Prime Collaboration Assurance and Analytics Reports/Dashlets for Session Monitoring. During configuration, this will help you get the required information from the integrated online help system.</p> <ul style="list-style-type: none"> • Monitor -> Utilization Monitor -> Telepresence Endpoint • Diagnose -> Conference Diagnostics • Reports -> Conference Reports • Reports -> Telepresence Endpoint Reports • Analytics -> Asset Usage -> No Show Video Telepresence Endpoint • Analytics -> Video Conference Analysis -> <ul style="list-style-type: none"> • Video Conference Statistics • Top N video Conference Location

You can access the Cisco Prime Collaboration Assurance 12.1 Service Pack 1 features from [Cisco.com](https://www.cisco.com).

Table 9: Cisco Prime Collaboration Assurance 12.1 Service Pack 1 Features

Feature Name	Feature Description
TLS v1.2	Support of TLS v1.2 communication for both server and client interfaces of Cisco Prime Collaboration Assurance.

Feature Name	Feature Description
New fields to support Secure JTAPI communication with CUCM	JTAPI section for Add Device, Modify Credentials, and Manage Credentials dialog on Inventory management page has been modified. This section has seven new fields to support Secure JTAPI communication with CUCM over TLS v1.2.
Secure JTAPI Communication for Session Monitoring	Secure JTAPI Communication with CUCM over TLS v1.2 protocol option has been introduced for Session Monitoring feature (Conference Monitoring) in Cisco Prime Collaboration Assurance.
Secure JTAPI Communication for Synthetic Tests	Secure JTAPI Communication with CUCM over TLS v1.2 protocol option has been introduced for Synthetic Tests feature in Cisco Prime Collaboration Assurance.



Note For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 SP1.

You can access the Cisco Prime Collaboration Assurance 12.1 features from [Cisco.com](https://www.cisco.com).

Table 10: Cisco Prime Collaboration Assurance 12.1 Features

Feature Name	Feature Description
Inventory - Device Status Summary	Fixing Unmanaged count: The unmanaged count in header must match the count in the Device Status Summary page. Count for both categories must meet this criteria.
Inventory - TMS Cluster	TMS discovery discovers all TMS provisioned devices (CUCM/VCS/endpoint/MCU/TPS/TP_Conductor) even though Cisco Prime Collaboration Assurance does not manage the CUCM/VCS devices. However, TMS discovery does not logically discover CUCM/VCS/endpoints.

Feature Name	Feature Description
Reports	<p>Following reports are merged into a single report:</p> <ol style="list-style-type: none"> 1. The Endpoint Audit Report is a single report that merges Audio Phone and Video Phone Audit Reports. Navigation - Reports -> Miscellaneous Reports -> Endpoint Audit Report 2. The Endpoint Move Report is a single report that merges Audio Phone and Video Phone Move Reports. Navigation - Reports -> Miscellaneous Reports -> Endpoint Move Report 3. The Endpoint Remove Report is a single report that merges Removed IP Phone and Removed Video Phone Reports. Navigation - Reports -> Miscellaneous Reports -> Endpoint Remove Report 4. The Endpoint Extension Report is a single report that merges Audio Extension and Video Extension Reports. Navigation - Reports -> Miscellaneous Reports -> Endpoint Extension Report
User Interface Changes	<p>Following are the changes with respect to user interface:</p> <ol style="list-style-type: none"> 1. Handling dependencies for removal of device - Devices like CUCM that includes Publisher and Subscriber, VCS, TMS, ESX, VCENTER, TPS, UNITY CONNECTION, MULTIPOINT Controller, IM&P and other infrastructure devices and their associated endpoints are removed from the database when the State is Deleted. 2. CUBE SIP Trunk - changes for session server group configuration A Collaboration Network Administrator access the Utilization Monitor -> CUBE SIP Trunk tab to view the CUBE SIP Trunk with "session server group configuration". In case of server group, this screen provides information about its limitation in supporting many-to-one configuration of Dialpeer to SIP Trunk. There is also an option to raise/suppress events for the server group configuration.
	<p>Removal of devices from Cisco Prime Collaboration Assurance on deletion</p> <p>The update explains that the Administrator must add a device first before rediscovering it. Remove the devices from Cisco Prime Collaboration Assurance when you delete them.</p>

Feature Name	Feature Description
	<p>Remove IP Phone Inventory Schedule and IP Phone XML Inventory Schedule from Inventory Schedule Page.</p> <p>PIFServer removal from the Cisco Prime Collaboration Assurance Enterprise/MSP mode also removes the IP Phone Inventory Collection and IP Phone XML Collection discoveries. This change addresses the following aspects:</p> <ol style="list-style-type: none"> 1. Removed Inventory Schedule -> IP Phone Inventory Schedule and Inventory Schedule -> IP Phone XML Discovery pages. 2. Renamed Inventory Schedule to Cluster Data Discovery Schedule under Inventory tab.
CME Syslog	The steps explain configuration of the syslogs in CME. This syslogs help monitor IP Phones using Cisco Unified CME Syslog messages.
Licensing of Registered Endpoints in Inventory	First, purge the latest registered endpoints within a particular cluster. Sort the registered endpoints by clustername, identify their clusters and purge them to meet licensing requirements. Port the phone licenses to the inventory module while removing the PIFServer from Cisco Prime Collaboration Assurance.
Fixing Settings button issue on Job Management page	Use the Schedule and Settings tab under the Job Details pane to schedule a job and set options.
30 day purge for Audit reports	Call quality event history and endpoint related (audio/video phone is now replaced with endpoint related) Audit report data older than 30 days are purged.
Cisco Prime Collaboration Assurance Licensing User Interface should restrict the maximum licenses one can import based on each profile like Small, Large, and BE6k	<p>Cisco Prime Collaboration Assurance licensing allows uploading of a license file with a count more than it supports. For instance, Small - 3K endpoints. An error message must notify the user when a Cisco Prime Collaboration Assurance accepts a license file with an endpoint count lesser than the maximum count supported per profile.</p> <p>This is applicable for Assurance Mass, Contact Center Assurance and Analytics Licensing and supports all the profiles such as Small/Medium/Large/Very Large/BE6k/BE7K.</p>

Feature Name	Feature Description
Handling Schema changes through DMA	<p>There will be schema changes around Inventory while upgrading from 11.x (11.0, 11.1, 11.5 and 11.6) to 12.1. During the upgrade, a few Database related table columns available in 11.x will be removed. There will be no impact on the overall Cisco Prime Collaboration Assurance functionality.</p> <p>The Deleted state devices/endpoints will be purged and after the upgrade these (the devices/endpoints) will not be available.</p>
FIPS User Interface has to be hidden	As part of Cisco Prime Collaboration Assurance 12.1 Enterprise mode, FIPS compliance is not certified. Hence, in the System Administration page, the FIPS enable/disable setup menu is hidden.
sFTP Credentials User Interface Implementation	<p>Additional buttons like CUCM/sFTP Credentials and Save are introduced in the User Interface. A check box to change the smuser password and options to confirm password options are available.</p> <p>Change in Navigation from Alarm & Report Administration -> CDR Source Settings -> CUCM SFTP Credentials to Inventory -> Inventory Management -> CUCM/sFTP Credentials</p>
Implementation of RTMT Polling Inconsistency - Notes for Alarms and Events	In a multi-node call manager cluster, if the same alert exists on more than one node at the same time, Cisco Prime Collaboration Assurance displays one latest alert.
Phone to Endpoint unregistered threshold	"Phone unregistered" is changed to "Endpoint unregistered".
Process Description Column - Serviceability	The process description column is added that describes each process to know the status of the processes in the output.
Prime License Manager does not show License Usage in Prime Collaboration Assurance	Provide both CLI and HTTP credentials in Monitor -> Utilization Monitor -> License Usage while managing co-resident PLM. Administrators can use CLI credentials to access the license information and HTTP credentials to manage Prime License Manager in Cisco Prime Collaboration Assurance.
Inaccessible status reason is shown as SNMP timeout	A note is added indicating that only HTTP credentials are required when a VMware vCenter Server or UCS Manager is added through Inventory -> Inventory Management -> Manage Credentials tab. The Inaccessible State column shows "SNMP timeout" where SNMP is not required for these devices.

Feature Name	Feature Description
Standalone PLM gets discovered as non-Cisco in PCA 11.6	A troubleshooting section is added to address this defect. This is likely to happen when PLM has a SNMP community string configured. If you want to discover PLM correctly, do not configure the community string. If configured to a community string, delete it and proceed to discover PLM in Cisco Prime Collaboration Assurance. Cisco Prime Collaboration Assurance does not support SNMP community string configuration for PLM discovery.
PCA BACKUP job status shows failure even after generating reports in SFTP	A troubleshooting section is added to address this defect. The troubleshooting section explains the method to generate the GPG key in the user folder.
The OpsView Dashlet page do not load due to corrupted globaladmin user	The troubleshooting section explains the Recommended Action and Path A new script (opsview_globaladmin.sh) and the recommended path (/opt/emms/emsam/bin) addresses this defect.
Ampersand is not allowed in LDAP parameter value	A Note is added to address this defect. A new LDAP parameter value (?CN=hq-prime,OU=Service Access Groups,DC=Megafon,DC=ru?) is defined to connect to LDAP.
CME Discovery & Phone XML Discovery job need to be restricted to be scheduled	A Note is added to address this defect. CMEPhoneDiscovery and PhoneXML Discovery Job is scheduled to execute at every regular four-hour intervals. These jobs can be modified to run once without re-occurrence. After the discovery, you cannot change it back to schedule.
Full Octets is not showing properly	During the deployment of Cisco Prime Collaboration Assurance 12.1 OVA, only three octets appear to IP address, IP Default Gateway, IP Default Netmask, and Backup Server IP. The fourth octet is invisible. Press the Tab button to display all octets.
Remove auto refresh of Device Status Summary from documentation	There is a change in the behavior of the Device Status Summary page. The page does not refresh automatically in every 30 seconds.
Execute this script on the server to generate and export CDR_CMV reports	Only an administrator can export CDR/CMR reports. Create a script to automate the task of exporting on the server.
NBI API Documentation	Reviewed and corrected Sample Input codes.

Feature Name	Feature Description
Performance data for Device 360	The performance data can no longer be viewed in Device 360 view. Instead, click the link 'Click here for performance data' to view the same data.
Performance data for Ops View Cluster Summary	A column is added to Call Health Summary tab.
Features or Devices Not Supported From This Release	<ol style="list-style-type: none"> 1. Cisco TelePresence-Manager (CTS-Manager/CTS-MAN) device is not supported. Hence, removed all occurrences of the device from the document. 2. FIPS Compliance is not supported. Hence, removed all occurrences from the document. 3. Content specific to CTX is removed from the document. 4. Enable Logical Discovery button - Content specific to enabling logical discovery button is removed from the document. 5. CLI is not supported. Hence, removed content specific to CLI from the document.
General	<ol style="list-style-type: none"> 1. Renamed "Cisco Prime Collaboration" to "Cisco Prime Collaboration Assurance". 2. Renamed "PhoneUnregThresholdExceeded" to "EndpointUnregThresholdExceeded".
Support UCM in Mixed mode	<p>Cisco Prime Collaboration Assurance supports Cisco Unified CM cluster in Mixed mode.</p> <p>However, the following features on Cisco Prime Collaboration Assurance will only support non-secure way of communication to CUCM:</p> <ul style="list-style-type: none"> • Session Monitoring will continue to use non-secure JTAPI communication to monitor sessions. • Synthetic Test: Does not support secure signaling (TLS) and secure media (SRTP) connections to CUCM and endpoints registered to CUCM in secure mode.

Overview of Cisco Prime Collaboration Analytics

This document provides information on Cisco Prime Collaboration 11.0, 11.1, 11.5, 11.6, 12.1, 12.1 SP1, 12.1 SP2, and 12.1 SP3 features.

Cisco Prime Collaboration Analytics helps you to identify the traffic trend, technology adoption trend, over-and-under-utilized resources, and device resource usages in your network. You can also track intermittent and recurring network issues and address service quality issues using the Cisco Prime Collaboration Analytics Dashboards.

Cisco Prime Collaboration Analytics is installed with the Cisco Prime Collaboration Assurance application, by default. You can disable Analytics or wait for Analytics evaluation license to expire. However, the only exception is for very large OVA (150 K) installation, where you can either install Cisco Prime Collaboration Assurance only or Cisco Prime Collaboration Assurance with Cisco Prime Collaboration Analytics.

For details on installation and system requirements, see [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#).

Cisco Prime Collaboration Analytics NBI

Following are the NBI supporting features for Cisco Prime Collaboration Analytics 11.5 SP1, 11.6, 12.1, and 12.1 SP1:

- NBI API support is available for the following dashboards:
 - Capacity Analysis
 - UC System Performance
 - Video Conference Analysis
 - License Usage
- **For Cisco Prime Collaboration Release 11.6 and later**
Video Communication Server / Expressway



Note As part of Cisco Prime Collaboration Analytics Release 11.5, NBI API is already supported for the following dashboards:

- Technology Adoption
- Asset Usage
- Traffic Analysis
- Service Experience

For Cisco Prime Collaboration Release 11.6 and later

NBI API is now available for Video Communication Server / Expressway dashlet which is present in License Usage dashboard.

- Following are the supported naming conventions:
 - For Dashlet:
`https://<PC Server>/emsam/nbi/<dashboard>/<dashletname>/summary/parameters`
 - For Details View:

```
https://<PC Server>/emsam/nbi/<dashboard>/<dashletname>/details/dvparameters
```

- NBI API documentation includes parameter descriptions and sample NBI URLs. To access the NBI API documentation, log in to the Cisco Prime Collaboration Analytics server with the administrator privilege and enter one of the following URL in the browser:

- `https://<pc-server-ip>/emsam/nbi/nbiAnalyticsDoc/`

Where, *<pc-server-ip>* is the server IP address.

- Or,

```
https://<pc-server-ip>:<port-number>/emsam/nbi/nbiAnalyticsDoc/
```

Where, *<pc-server-ip>* is the server IP address and *<port-number>* is the HTTP port number.

For example:

```
https://<pc-server-ip>:8443/emsam/nbi/nbiAnalyticsDoc/
```

- Acceptable parameters to the NBI URL are similar to the parameters on the GUI filters, check the NBI API documentation for the parameter names and values.



Note Case insensitive parameter values are not supported in the NBI API for Cisco Prime Collaboration Analytics 11.5.

- Call Detail Records (CDR) NBI Support:

- NBI is also supported to query the records for the CDR based dashlets:

```
https://<PC Server>/emsam/nbi/fetchCDR/fetchTableDetails
```

- Result provides information similar to the pop-up table displayed in the **Details View** when a legend is selected for CDR based dashlets.
- Search criteria can be one or combination of the following filters:
 - **Call**—status, grade, cluster, class, and type
 - **Origination Endpoint**—dn, ip, uri, cluster/location, cluster/device pool, username, codec, endpoint model, and endpoint type
 - **Destination Endpoint**—dn, ip, uri, cluster/location, cluster/device pool, username, codec, endpoint model, and endpoint type
- Case insensitive parameter values are supported in the NBI API. For example, parameter *timePeriod* accepts *last7days*, *Last14Days*, *last7DAYS*, and so on as values.
- As part of Cisco Prime collaboration Analytics Release 11.5, NBI API is supported to query Call Detail Records(CDR) for the CDR based dashlets. For more information, refer [Call Detail Records \(CDR\) NBI Support](#).

For Cisco Prime Collaboration Release 11.6 and later

To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server and click **Assurance NB API documentation** under Settings drop-down menu at the top right corner of the user interface.



CHAPTER 2

Concepts

This section provides information on the following topics:

- [Concepts, on page 39](#)

Concepts

This chapter explains the concepts that are key to Cisco Prime Collaboration Assurance.

Event

An event is a distinct incident that occurs at a specific point in time.

An event is a:

- Possible symptom of a fault that is an error, failure, or exceptional condition in the network. For example, when a device becomes unreachable, an Unreachable event is triggered.
- Possible symptom of a fault clearing. For example, when a device state changes from unreachable to reachable, an event is triggered.

Examples of events include:

- Port status change
- Node reset
- Node becoming reachable for the management station
- Connectivity loss between routing protocol processes on peer routers

Events are derived from incoming traps and notifications, detected status changes (by polling), and user actions.

It is important to understand that an event, once it occurs, does not change its status even when the conditions that triggered the event are no longer present.

Choose **Monitor > Alarms & Events** to view the list of events.

Alarm

The life cycle of a fault scenario is called an alarm.

An alarm:

- Is a Cisco Prime Collaboration Assurance response to events it receives.
- Is a sequence of events, each representing a specific occurrence in the alarm life cycle (see below example). In a sequence of events, the event with the highest severity determines the severity of the alarm.
- Represents a series of correlated events that describe a fault occurring in the network.
- Describes the complete event life cycle, from the time that the alarm is raised (when the fault is first detected) until it is cleared and acknowledged.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

Cisco Prime Collaboration Assurance constructs alarms from a sequence of correlated events. A complete event sequence for an alarm includes a minimum of two events:

- Alarm active (for example, an interface down event raises an alarm).
- Alarm clear (for example, an interface up event clears the alarm).

The lifecycle of an alarm can include any number of correlated events that are triggered by changes in severity, updates to services, and so on.

When a new related event occurs, Cisco Prime Collaboration Assurance correlates it to the alarm and updates the alarm severity and message text based on the new event. If you manually clear the alarm, the alarm severity changes to cleared.

You can view the events that form an alarm in the Alarms and Events browser.

Choose **Monitor > Alarms & Events** to view the list of alarms.

Event Creation

Cisco Prime Collaboration Assurance maintains an event catalog and decides how and when an event has to be created and whether to associate an event with an alarm. Multiple events can be associated to the same alarm.

Cisco Prime Collaboration Assurance discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.
- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when the status of the alarm is changed; for example, when the user clears an alarm.

Cisco Prime Collaboration Assurance allows you to disable monitoring of events that may not be of importance to you. The events that are disabled are not listed in the Alarms and Events browser. Also, Cisco Prime Collaboration Assurance does not trigger an alarm.

Incoming event notifications received as syslogs or traps are identified by matching the event data to predefined patterns. An event is considered supported by Cisco Prime Collaboration Assurance if it has matching patterns and can be properly identified. If the event data does not match with predefined patterns, the event is considered as unsupported and it is dropped.

The following table illustrates the Cisco Prime Collaboration Assurance behavior while it deals with event creation:

Time	Event	Cisco Prime Collaboration Assurance Behavior
10:00AM PDT June 7, 2012	Device A becomes unreachable	Creates a new Unreachable event on device A.
10:30AM PDT June 7, 2012	Device A continues to be in the unreachable state.	No change in the event status.
10:45AM PDT June 7, 2012	Device A becomes reachable.	Creates a new Reachable event on device A.
11:00AM PDT June 7, 2012	Device A stays reachable	No change in the event status.
12:00AM PDT June 7, 2012	Device A becomes unreachable.	Creates a new Unreachable event on device A.

Alarm Creation

An alarm represents the life cycle of a fault in a network. Multiple events can be associated with a single alarm.

An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after checking if there is no active alarm corresponding to this event.

An alarm is associated with two types of events:

- Active events: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- Historical events: Events that have been cleared. An event changes its state to an historical event when the fault is cleared. See [Alarm Status](#) to know how an alarm is cleared.

The alarm life cycle ends after an alarm is cleared. A cleared alarm can be revived if the same fault recurs within a preset period of time.

For Cisco Prime Collaboration Assurance, the preset period is 60 minutes.

Event and Alarm Association

Cisco Prime Collaboration Assurance maintains a catalog of events and alarms. The catalog contains the list of events managed by Cisco Prime Collaboration Assurance, and the relationship among the events and alarms. Events of different types can be associated to the same alarm type.

When a notification is received:

1. Cisco Prime Collaboration Assurance compares an incoming notification against the event and alarm catalog.
2. Cisco Prime Collaboration Assurance decides whether an event has to be raised.
3. If an event is raised, Cisco Prime Collaboration Assurance decides whether the event should trigger a new alarm or associate it to an existing alarm.

A new event is associated with an existing alarm, if the new event triggered is of the same type and occurs on the same source.

An active interface error alarm is an example. All interface error events that occur on the same interface, are associated to the same alarm.

If any event is cleared, its severity changes to informational.


Note

Some events have default severity as informational. For these events, alarms will not be created. If you want Cisco Prime Collaboration Assurance to create alarms for these events, you must change the severity of these events.

Event Aggregation

If the number of same event received from a set of elements exceeds a specified threshold, Cisco Prime Collaboration Assurance creates an alarm.

Example use cases:

- Number of unregistered phones on a device pool / Unified CM location is more than 5%.
- Number of service quality issues experienced on a device pool / Unified CM location is more than 5%
- All the call quality events raised against a single poor-quality call are grouped.

Event Masking

Cisco Prime Collaboration Assurance automatically masks the hierarchy of events when the top-level component is the cause for the issue, and raises an alarm against the top level component while masking all the downstream events.

Example use cases:

- When a Unified CM goes down, Cisco Prime Collaboration Assurance masks all its component (such as powersupply, interface, fan) events.
- When a switch card goes down, Cisco Prime Collaboration Assurance masks all the contained port level events.

Alarm Status

The following are the supported statuses for an alarm:

Table 11: Alarm Status

Status	Description
Not Acknowledged	When an event triggers a new alarm or an event is associated with an existing alarm.
Acknowledged	When you acknowledge an alarm, the status changes from Not Acknowledged to Acknowledged
Cleared	<ul style="list-style-type: none"> • System-clear from the device—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable alarm. • Alarms are also triggered during the conference because of packet loss, jitter, and latency. These alarms are auto-cleared after the conference ends. • Manual-clear from Cisco Prime Collaboration Assurance users: You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and this event clears the alarm. • If the fault continues to exist in the network, a new event and alarm are created subsequently based on the polling. • Auto-clear from the Cisco Prime Collaboration Assurance server—Cisco Prime Collaboration Assurance clears all conference-related alarms, when the conference ends. <p>If there are no updates to an active alarm for 24 hours, Cisco Prime Collaboration Assurance automatically clears the alarm.</p> <p>Note Certain alarms might get cleared automatically before 24 hours. See Supported Events and Alarms for Prime Collaboration.</p>

Event Severity

Each event has an assigned severity, and can be identified by its color in Cisco Prime Collaboration Assurance.

Events fall broadly into the following severity categories:

- Flagging — Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational — Info (blue). Some of the Informational events clear the flagging events.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

Cisco Prime Collaboration Assurance allows you to customize the settings and severity of an event. The events that are of importance to you can be given higher severity.

The event settings and severity predefined in the Cisco Prime Collaboration Assurance application is used if you have not customized the event settings and severity.

Event and Alarm Database

All events and alarms, including active and cleared, are persisted in the Cisco Prime Collaboration Assurance database.

The relationships between the events are retained. The Alarm and Event Browser allows you to review the content of the database. The purge interval for this data is four weeks.



Note

Events are stored in the form of the Cisco Prime Collaboration Assurance event object. The original notification structure of incoming event notifications (trap or syslog) is not maintained.

Alarm Notifications

Cisco Prime Collaboration Assurance allows you to subscribe to receive notifications for alarms. Cisco Prime Collaboration Assurance sends notifications based on user-configured alarm sets and notification criteria.



CHAPTER 3

Get Started with Cisco Prime Collaboration Assurance

This section provides the following:

- [Get Started with Cisco Prime Collaboration Assurance, on page 45](#)
- [Get Started with Cisco Prime Collaboration Analytics, on page 50](#)

Get Started with Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance is available in the following modes:

- Cisco Prime Collaboration Assurance Enterprise mode
- Cisco Prime Collaboration Assurance MSP mode



Note

You *must* complete the tasks mentioned in the section *Install Prime Collaboration Assurance* in the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#) before you start the tasks mentioned in the following sections.

Get Started with Cisco Prime Collaboration Assurance

After you install the Cisco Prime Collaboration Assurance, perform the tasks listed in the following table:

Table 12: Get Started with Cisco Prime Collaboration Assurance

Before Upgrade	After Upgrade
	Home > Getting Started

Before Upgrade	After Upgrade
Home > Network Health Overview <ul style="list-style-type: none"> • OPSView • Call Quality • Alarm • Performance • Contact Center Topology 	Network Health Overview <ul style="list-style-type: none"> • OpsView • Call Quality • Alarm • Performance • Contact Center Topology
Network Health Overview	In MSP mode, ONLY Customer Summary is available.
	Monitor <ul style="list-style-type: none"> • Alarms and Events <ul style="list-style-type: none"> • Alarm Summary • Alarms • Events • Utilization Monitor <ul style="list-style-type: none"> • T1/E1 Trunks • CUBE SIP Trunk • UCM SIP Trunk • Route Group • Trunk Group • Location CAC Bandwidth • Conferencing Devices • Conductor Bridge Pool • Telepresence Endpoint • License Usage
Call Quality	NA

Before Upgrade	After Upgrade
Inventory	Inventory <ul style="list-style-type: none"> • Inventory Management • Device Status Summary • UC Device Search • Cluster Device • Discovery Schedule <p>For Cisco Prime Collaboration Assurance 12.1 Service Pack 3</p> <p>Cluster Device Discovery Schedule</p> <ul style="list-style-type: none"> • SNMP MIB Query Tool
Inventory > UC Device Search	
Diagnose > Conference Diagnostics	
Diagnose > SIP Call Flow Analyzer	Diagnose <ul style="list-style-type: none"> • Endpoint Diagnostics • Conference Diagnostics • SIP Call Flow Analyzer • CME Diagnostics • Device Log Collector
Diagnose > Device Log Collector	
Synthetic Tests <ul style="list-style-type: none"> • UC Application Synthetic Test • Audio Phone Features Test • IP SLA Voice Test • Video Test • Phone Status Test • Batch Test 	Synthetic Tests <ul style="list-style-type: none"> • UC Application Synthetic Test • Audio Phone Features Test • IP SLA Voice Test • Video Test • Phone Status Test • Batch Test

Before Upgrade	After Upgrade
Reports <ul style="list-style-type: none"> • Administrative Reports • Launch CUCM Reports • Miscellaneous Reports • Conference Reports • Telepresence Endpoint Reports • NAM & Sensor Reports • CDR & CMR Reports • Scheduled Reports 	Reports <ul style="list-style-type: none"> • CDR & CMR Reports • NAM & Sensor Reports • Conference Reports • Telepresence Endpoint Reports • Scheduled Reports • Administrative Reports • Launch CUCM Reports • Miscellaneous Reports
	Analytics <ul style="list-style-type: none"> • Technology Adoption • Asset Usage • Traffic Analysis • Capacity Analysis • Service Experience • UC System Performance • Video Conference Analysis • License Usage • My Dashboard • Custom Report Generator • Scheduled Reports
Assurance Reports > Conference Reports <ul style="list-style-type: none"> • Conference Summary Report • Conference Detail Report 	

Before Upgrade	After Upgrade
Alarm & Report Administration <ul style="list-style-type: none"> • Event Customization • E-mail Setup for Alarms & Events • Notification Setup • CDR Source Settings • CDR Analysis Settings • 1040 Sensors Setup • Polling Settings • Customer Management 	Alarm & Report Administration <ul style="list-style-type: none"> • Event Customization • E-mail Setup for Alarms & Events • Notification Setup • CDR Analysis Settings • 1040 Sensors Setup • Conference Path Threshold Settings • Polling Settings • APIC-EM & Prime Integration <p>For Cisco Prime Collaboration Assurance 12.1 Service Pack 3</p> <p>APIC-EM & NAM</p> <ul style="list-style-type: none"> • For Cisco Prime Collaboration Assurance 12.1 Service Pack 2 and earlier <p>CDR Source Settings</p> <p>In MSP mode, ONLY Customer Management is available.</p>
System Administration > Domain Setup	
	Analytics Administration <ul style="list-style-type: none"> • sFTP Settings • Group Management • Trunk Traffic Max Capacity Settings <p>In MSP mode, ONLY Upload Customer Logo is available.</p>

Before Upgrade	After Upgrade
System Administration <ul style="list-style-type: none"> • License Management • User Management • LDAP Settings • Single Sign-On • Backup Settings • Log Management • Job Management • Certificate Management 	System Administration <ul style="list-style-type: none"> • Domain Setup • License Management • User Management • LDAP Settings • For Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Security Settings • Single Sign-On • Backup Settings • Log Management • Job Management • Certificate Management
	UC Operations Dashboard <ul style="list-style-type: none"> • UC Operations Dashboard • Responder Settings
	Serviceability

Get Started with Cisco Prime Collaboration Analytics

Table 1 describes the usage scenarios for Cisco Prime Collaboration Analytics dashboards.

Table 13: Get Started with Cisco Prime Collaboration Analytics Dashboards

Usage Scenario	Dashlet Name (Navigation from Analyze)
Track the progress of deployment of voice-only phones, video phones and TelePresence endpoints.	For Cisco Prime Collaboration Release 11.1 and earlier Deployment Distribution by Endpoint Model(Technology Adoption) For Cisco Prime Collaboration Release 11.5 and later Endpoints Deployment Summary(Technology Adoption)

Understand the endpoint usage to validate investments made so far and to make future investment decisions.	<ul style="list-style-type: none"> • For Cisco Prime Collaboration Release 11.1 and earlier Call Distribution by Endpoint Model (Technology Adoption) • For Cisco Prime Collaboration Release 11.5 and later Call Volume by Endpoint Model (Technology Adoption) • For Cisco Prime Collaboration Release 11.1 and earlier Call Distribution by Endpoint Types (Technology Adoption) • For Cisco Prime Collaboration Release 11.5 and later Call Volume by Endpoint Types (Technology Adoption)
Count the number of endpoints that are heavily or lightly used.	Technology Usage (Technology Adoption)
Identify the least used endpoints to effectively plan and allocate resources across an organization.	Least Used Endpoint Types (Asset Usage)
Track endpoints that did not participate in the scheduled sessions.	For Cisco Prime Collaboration Assurance 11.0 and earlier No Show Video Conference (Asset Usage) For Cisco Prime Collaboration Release 11.1 and later No Show Video TelePresence Endpoint
Enables you to identify the most utilized and least utilized endpoints.	Video TelePresence Rooms Utilization (Asset Usage)
Within the Cisco Prime Collaboration Assurance managed deployment, find the top N directory numbers sorted by the most number of calls placed or by total duration of all calls placed.	Top N Callers (Traffic Analysis)
Within the Cisco Prime Collaboration Assurance managed deployment, find the top N directory numbers receiving the most number of calls or to find the top N directory numbers having the most call minutes.	Top N Dialed Numbers (Traffic Analysis)
Find the locations with most number of incoming and outgoing OffNet calls.	Top N OffNet Traffic Locations (Traffic Analysis)

Identify the top N locations from which the highest number of calls were placed or received.	Top N Call Traffic Locations (Traffic Analysis)
Understand the trend of various types of calls between sites, locations, endpoints, clusters, or device pools.	Call Traffic Analysis (Traffic Analysis)
Track the utilization of TelePresence conferencing devices to optimize their usage across the organization.	Conferencing Devices Video Utilization (Capacity Analysis)
Evaluate the bandwidth allocated to each location by looking at the Call Admission Control (CAC) bandwidth usage for locations with the most number of failed calls.	Location CAC Bandwidth Utilization (Capacity Analysis)
Evaluate and optimize trunk and route group utilization across the organization. Also, you can define and track custom trunk/route group utilization.	<ul style="list-style-type: none"> • Trunk Utilization (Capacity Analysis) • Route Group Utilization (Capacity Analysis)
Decide on the capacity (lines) after measuring trunks and route group Average Bouncing Busy Hour (ABBH) traffic.	<ul style="list-style-type: none"> • Busy-Hour Trunk Capacity (Capacity Analysis) • Busy-Hour Route Capacity (Capacity Analysis)
Optimize the DSP resources for gateways	DSP Utilization (Capacity Analysis)
Analyze the service quality experienced by users in your organization.	Service Experience Distribution (Service Experience)
Identify the top N endpoints experiencing service quality issues.	<p>For Cisco Prime Collaboration Release 11.1 and earlier</p> <p>Endpoints with Service Quality Issues(Service Experience)</p> <p>For Cisco Prime Collaboration Release 11.5 and later</p> <p>Endpoints with Call Quality Issues(Service Experience)</p>
Analyze the trend of call failures in your organization and identify the locations where call failure rates are high.	Top N Call Failure Locations (Service Experience)
Identify users with service quality issue.	Users with Service Quality Issue (Service Experience)
Analyze the UC applications system performance in your organization.	UC System Performance
Get visibility into conference statistics (number of conferences and durations)	<ul style="list-style-type: none"> • Video Conference Statistics (Video Conference) • Top N Video Conference Locations (Video Conference)



PART II

Set Up the Server

- [Enable Third-Party CA Signed Certificate, on page 55](#)
- [Manage Licenses, on page 59](#)
- [Manage Users, on page 65](#)
- [Manage Customers, on page 75](#)
- [Manage Domains, on page 77](#)
- [Configure System Parameters, on page 79](#)



CHAPTER 4

Enable Third-Party CA Signed Certificate

This section explains the following:

- [Enable Third-Party CA Signed Certificate, on page 55](#)

Enable Third-Party CA Signed Certificate

You can import your company signed certificate for the secured data transmission. SSL must be enabled on the browser to use this certificate.

Install CA signed certificate

Steps to install CA signed certificate for secure data transmission:

Before you begin

The following factors will be validated to protect information assets for strong security, easy administration, and hands-on control of certificate management.

For Cisco Prime Collaboration Release 12.1 SP3 and later

The CA Signed Certificate must meet the following list of requirements. It must

- Contain “primecollab” alias.
- Allow importing with the right password.
- Stay valid for more than 30 years.
- Have the valid validity period. The validity must not
 - Expire
Ex: If Current Date is 20/9/2019, Validity period (20/8/1970-20/8/2000) is invalid.
 - Have a future date
Ex: If Current Date is 20/9/2019, Validity period (20/12/2020-20/12/2025) is invalid.
- A “Sample valid” validity period
Ex: If Current Date is 20/9/2019, Validity period (20/9/2019-20/9/2025) is valid.

- CN (common name) or SAN (Subject Alternative Name) specified in the certificate must match with FQDN (Fully Qualified Domain Name) of the PCA server.
 - If FQDN of the PCA server does not match with the CN, it is matched with the list of SANs.
 - Users must either generate CSR (Certificate Signing Request) with CN as FQDN or include FQDN in the list of SANs. Ex: pctest.cisco.com (FQDN).
- Signature algorithm must match with the Signature Algorithm Identifier present in the TBSCertificate sequence.
- Not have any duplicate extensions.
- Not have any un-supported critical extensions.
 - Check applies only on extensions marked as critical.
 - Extensions supported are BC or BasicConstraints, KU or KeyUsage, EKU or ExtendedkeyUsage, SAN or SubjectAlternativeName, IAN or IssuerAlternativeName, SIA or SubjectInfoAccess, AIA or AuthorityInfoAccess.
- Have a valid critical KeyUsage (KU)
 - Check applies if KU extension is marked as critical.
 - Valid KUs are keyCertSign, cRLSign, digitalSignature.
- Have a valid critical ExtendedKeyUsage (EKU).
 - Check applies if EKU extension is marked as critical.
 - Valid EKUs are serverAuth , clientAuth, OCSPSigning.

If any of the above requirements are not satisfied, the certificate is rejected and user is alerted with an appropriate error message.

**Note**

We recommend that you use Google Chrome, or Microsoft Edge to install the certificate.

For Cisco Prime Collaboration Release 11.5 and later

- The Root Certificate is part of the Signed Certificate.
- SSL is enabled on the browser to use CA signed certificate.

-
- Step 1** Choose **System Administration > Certificate Management > Cisco Prime Collaboration Certificate Management**.
- Step 2** Browse through the CA signed Certificate (in PKCS12 format) from your local system.
- Step 3** (Optional) Enter and verify the certificates password of PKCS#12 file, if you have configured the password while generating the certificate, otherwise it can be left empty.
- Step 4** Click **Import**.
- A warning message indicating that "The services will be restarted" appears.

Step 5 Click **Continue** on receiving the warning message.
The certificates are successfully imported on the server.

Note You must manually restart the Cisco Prime Collaboration Assurance server after you import the certificates.

For Cisco Prime Collaboration Release 12.1 SP3 and later

To restart Cisco Prime Collaboration Assurance server, login as *root* and execute the following commands:

1. Stop the processes:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh stop
```

2. Check the status of the processes - Verify whether the processes have stopped:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh status
```

3. Restart the processes:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh start
```

After the service restart, the login page is displayed. The security warning page (where you make the selection for the login page to appear) is no longer displayed.

Note Before you launch the Cisco Prime Collaboration Assurance server, we recommend that you import the primary and secondary intermediate certificates to the browser. This ensures that you do not get a warning about your connection not being private, when you launch the server for the first time after the CA signed certificate installation.

You can import PKCS12 certificate with any alias name.

You should use the certificates in PKCS#12 (.pfx or .p12) format as PEM/DER (.pem, .cer, .der, .key, and so on) formats are not supported.

For Cisco Prime Collaboration Release 11.6 and later

Note Make sure you import a PKCS12 (.pfx or .p12) format signed certificate.

The certificate must contain **primecollab** alias.

The Key password for **primecollab** alias must be same as the certificate password.

For Cisco Prime Collaboration Release 12.1 and later

If a PKCS7 or PKCS12 certificate is applied to 11.x and the Cisco Prime Collaboration Assurance is migrated to version 12.1, the certificate will not be restored. You need to regenerate the certificate for the Cisco Prime Collaboration Assurance 12.1.

Note From Cisco Prime Collaboration Assurance 11.6 onwards, only PKCS12 certificate is supported.

To import the primary/intermediate/secondary certificates to the browser, see the following table:

Browser	Action
Internet Explorer	Choose Tools > Internet Options > Content > Certificates > Trusted root certification authorities > Import
Mozilla Firefox	Choose Tools > Options > Advanced > Certificates > View certificates > Import

Browser	Action
Chrome	Choose Settings > Advanced settings > HTTP/SSL Manage certificates > Trusted root certification authorities > Import



CHAPTER 5

Manage Licenses

This section explains the following:

- [Manage Licenses, on page 59](#)

Manage Licenses

The Cisco Prime Collaboration Assurance license enables the endpoint quantities for the Cisco Prime Collaboration Assurance application that you choose to install. You can order license based on the quantity of the endpoints. You can view the already installed license details of Cisco Prime Collaboration Assurance by navigating to **System Administration > License Management**.

You can install Cisco Prime Collaboration Assurance in Advanced mode.

The number of endpoints that you can add during the Evaluation mode depends on the OVA size of Assurance. Cisco Prime Collaboration Assurance keeps track of the number of devices that you have added to the inventory. When the number of devices that you can add gets close to the allowed number of devices, a warning message is displayed. You can either upgrade the OVA or delete some of the existing devices in your system inventory.

The Evaluation period for Cisco Prime Collaboration Assurance is 60 days. After the evaluation period, Assurance redirects the License Management page every time you login.



Note “Smart Licensing” is not supported in the Cisco Prime Collaboration Assurance for Release 12.1.

Cisco Prime Collaboration Assurance Licensing

Cisco Prime Collaboration Assurance licensing is based on the endpoint quantity. The number of endpoints determine the number of licenses that you need to purchase to manage your network.

Cisco Prime Collaboration Assurance provides the license usage status of the Total Endpoints in the **License Management** page (**System Administration > License Management**).



Note Soft phones also consume license like hard phones; and every soft phone requires one license each even if they are sharing the same directory number as any hard phone registered in the same Unified CM.

For more information on these endpoints, see the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#).

Cisco Prime Collaboration Analytics Licensing

Cisco Prime Collaboration Analytics license must be applied only after or while deploying the Cisco Prime Collaboration Assurance license.

For Cisco Prime Collaboration Release 11.1 and earlier

You need to deploy Cisco Prime Collaboration Assurance in Enterprise mode to access the Cisco Prime Collaboration Analytics features. Cisco Prime Collaboration Analytics is not supported in Managed Service Provider (MSP) mode.

To access Cisco Prime Collaboration Analytics dashboards after the Evaluation mode (60 days), you must purchase Cisco Prime Collaboration Analytics license. You need to purchase the same scale license as that of Cisco Prime Collaboration Assurance. You can continue to access Cisco Prime Collaboration Analytics in Evaluation mode even after you add a license for Cisco Prime Collaboration Assurance in the Advanced mode.

To add Analytics license file, choose **System Administration > License Management**.

Adding Analytics License

Cisco Prime Collaboration Analytics licensing should be greater than or equal to the sum of the total assurance count.

In Evaluation mode, the Cisco Prime Collaboration Analytics license is same as that of Cisco Prime Collaboration Assurance.

To add Analytics license file, choose **System Administration > License Management**.

NFR license for Cisco Prime Collaboration Analytics can be purchased only after the purchase of Cisco Prime Collaboration Assurance license.

Enable and Disable Analytics

Before you begin

The Cisco Prime Collaboration Analytics must be in the Evaluation mode to enable or disable the Analytics features.

-
- Step 1** Choose **System Administration > License Management**.
 - Step 2** If you have deployed Cisco Prime Collaboration Assurance and Analytics very large OVA, perform the following steps after deploying the remote Cisco Prime Collaboration Analytics database.
 - a) In the Analytics pane, click **Setup Remote Analytics DB** to configure the remote Cisco Prime Collaboration Analytics database.
 - b) Enter the IP address of the remote database and click **OK**.
 - Step 3** In the Analytics pane, click **Enable Analytics** to enable data analysis.
 - Step 4** Log out from the browser and log in to Cisco Prime Collaboration Assurance Serviceability User Interface.
 - Step 5** Click **Dashboard**.

You can view all the processes along with their status and System Update History. You can Start and Stop all the processes.

Step 6 Log in to the Cisco Prime Collaboration Assurance server and verify if the Analytics license is activated. (**System Administration > License Management**).

If you want to disable Analytics, click **Disable Analytics** in the Analytics pane. You must restart the processes on application and database (only for very large OVA) servers after disabling. All analyzed data are purged and the Analyze tab is disabled.

Cisco Prime Collaboration Contact Center Assurance Licensing

Cisco Prime Collaboration Contact Center Assurance is supported only in the Cisco Prime Collaboration Assurance Advanced deployment. The Cisco Prime Collaboration Contact Center Assurance licensing is based on the number of concurrent Unified Contact Center Enterprise (Unified CCE) agents logged in. You must apply the Cisco Prime Collaboration Contact Center Assurance license only after adding the Cisco Prime Collaboration Assurance Advanced license.

Cisco Prime Collaboration Assurance polls the number of agents logged in to the Unified Contact Center Enterprise every 30 minutes; and if the number of logged-in agents exceeds the permitted number that is mentioned in the license file, the system displays a warning.

Cisco Prime Collaboration Assurance raises one violation per day irrespective of the number of warnings received. If there are 10 such violations within the 30 day period, then your license expires within the next 30 days of receiving the tenth violation.

If you add the license file for Cisco Prime Collaboration Assurance Advanced but not Cisco Prime Collaboration Contact Center Assurance, you can access the features for Cisco Prime Collaboration Contact Center Assurance only until the evaluation expiry or purchase of license.

Upon license expiry, the Unified Contact Center infrastructure devices are not displayed in the UC Performance dashboard, Threshold Rules, and Correlation Rules windows. SIP Call Flow Analyzer fails to analyze the call logs received from Contact Center devices (Unified CCE, CVP) and other UC components. The entire Contact Center Topology view is also not accessible.

To continue using these features, you must purchase the required number of Cisco Prime Collaboration Contact Center concurrent agent licenses. You can view the license details for Cisco Prime Collaboration Contact Center Assurance by navigating to the **System Administration > License Management** page.

For details on the features that are enhanced after you add the Cisco Prime Collaboration Contact Center Assurance license, see the [Cisco Prime Collaboration Contact Center Assurance Guide](#).

The number of agents that you can manage after you purchase a license remains the same as the Evaluation mode. See the *Endpoints and Contact Center Agents Count* section in the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#) for more information.

License Count

For Cisco Prime Collaboration Release 12.1 and later

Endpoint Licensing runs every 15 minutes. As per the licensing criteria, the total managed endpoint count should not exceed the purchased license count.

- If the licensing criteria is not met, endpoints are deleted. Deletion starts with Unregistered endpoints.
- If the licensing criteria is still not met, registered endpoints are deleted.

For details on how devices are discovered and managed, see [Discover Devices](#). Endpoints that are not added are listed in the discovery job.

When Cisco Prime Collaboration Assurance is deployed in MSP mode, phones that have the same overlapping IP address are counted as different endpoints.

Endpoint Count in Cisco Prime Collaboration Assurance

The following phones are counted in the Cisco Prime Collaboration Assurance database:

- The soft clients include Cisco Unified Personal Communicator, Cisco IP Communicator, Cisco Jabber and Client Services Framework (CSF).
- Mobile phones are counted separately.
- Analog phones connected to a voice gateway are not monitored and hence not counted.



Note

The system counts each endpoint; and counts Jabber and IP Phones separately.

View License Details

In the **License Management** page (**System Administration > License Management**), you can view the following Cisco Prime Collaboration Assurance License information:

For Cisco Prime Collaboration Release 11.6 and later

System Information

- MAC Address
- DB Server IP Address



Note

DB server IP Address field is specific to Cisco Prime Collaboration Assurance very large OVA deployment model and does not appear in the Assurance Information link for Cisco Prime Collaboration Assurance small, medium, and large OVA deployment models.

For Cisco Prime Collaboration Release 12.1 and later

This implies to all the three types of licensing types (Assurance, Analytics, and Contact Center Assurance).



Note

You can also track the number of licenses allocated to each type of license types (Assurance, Analytics, and Contact Center Assurance).

When you upload a license file, a license count is introduced that allows you to check the count per profile and if it exceeds the maximum count a warning message indicating that the License has exceeded the maximum count allowed appears. The message is specific to the modes of licensing.



Note You will receive a common warning message specific to Assurance and Analytics mode and one specific to Contact Center Assurance mode.

Assurance License Status

- Active Base License Installed - Evaluation or Image.
- Total Endpoint Licenses Used - The total number of licenses allowed and the number of licenses used currently. For more details about the total number of licenses for the Advanced mode, see the “License Count” section.
- License Expiration Date - The date when the license expires. This value is applicable to Evaluation license only.



Note The value of License Expiration Date changes to **Permanent** when you obtain license after evaluation expires.

- Total Endpoint Licenses Installed - The total number of licenses that are installed.

For Analytics and Contact Center Assurance licensing, you can view the following information:

Enterprise Mode	Managed Service Provider (MSP) Mode
Analytics: <ul style="list-style-type: none"> • Licenses Installed • License Expiration Date 	For Cisco Prime Collaboration Release 11.5 and later Analytics: <ul style="list-style-type: none"> • Licenses Installed • License Expiration Date
Contact Center Assurance: <ul style="list-style-type: none"> • Licenses Installed • License Expiration Date 	Contact Center Assurance: <ul style="list-style-type: none"> • Licenses Installed • License Expiration Date



Note Although the License Expiration Date of Contact Center Assurance licensing is same as that of the Assurance License Status in the user interface, the License Expiration Date of Contact Center Assurance may change depending on the number of concurrent Unified CCE agents logged in.

You must review the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#) to learn how to register and obtain the license file for Cisco Prime Collaboration Assurance.

Add and Delete a License File

The image license files for Cisco Prime Collaboration Assurance are mandatory if you wish to activate the Cisco Prime Collaboration Assurance applications in the production network. You can add any number of scale licenses, however, the image license file is added once for Cisco Prime Collaboration Assurance.

To add the license file in Cisco Prime Collaboration Assurance:


-
- Step 1** Choose **System Administration** > **License Management**.
The **License Management** page is displayed.
- Step 2** Under **License Files**, click **Add**.
The **Add License File** pop-up page is displayed.
- Step 3** Click **Browse** to upload the license file and click **OK**.
The newly added license file information appears in the License Status pane of Cisco Prime Collaboration Assurance.
- Note** To delete a license file, choose **System Administration** > **License Management**. On the **License Management** page, select the license file and click **Delete**.
- When you upgrade from Evaluation mode to production, perform a rediscovery of devices. For details on rediscovering devices, see [Rediscover Devices, on page 135](#).
-

Switch Between Advanced Evaluation to Advanced (Purchase License) in Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance allows you to switch from the Advanced Evaluation to Advanced (Purchase License) in Cisco Prime Collaboration Assurance.

The following table captures the different scenarios of switching:

Table 14: Switch from the Advanced Evaluation to Advanced (Purchase License) in Cisco Prime Collaboration Assurance

Installation Mode	Advanced Evaluation to Advanced (Purchase license)
Cisco Prime Collaboration Assurance	Yes. (Click the Get Advanced icon  at the top right corner of the User Interface and click Add Licenses . In the License Management page, click Add and upload the license file for the advanced mode.)



CHAPTER 6

Manage Users

This section explains the following:

- [Manage Users, on page 65](#)

Manage Users

Cisco Prime Collaboration Assurance supports built-in static roles with predefined access control that enables you to perform different tasks.

In Cisco Prime Collaboration Assurance, you can create users and assign roles to the users.

Cisco Prime Collaboration Assurance enables Role-based Access Control (RBAC) through these built-in static roles. Hence, the tasks a user can perform, or the device or device groups a user can view or manage is controlled by the role allocated by the Super Administrator.

You can enforce further access control of selected devices or device groups, and tasks related to those by associating the devices or device groups to domains (if you have deployed Cisco Prime Collaboration Assurance in Enterprise mode). Typically, a user with Operator role, is granted access to certain domains only.

Cisco Prime Collaboration Assurance-Advanced User Roles

User roles are used to define the authorizations of tasks that users can access.

You can be assigned one of the following roles:

- **For Cisco Prime Collaboration Release 11.5 and later**

Report Viewer—Can view and export the reports only. The homepage of Report Viewer is CDR & CMR Reports. The global user interface components like **Search**, **Device Status Summary**, **Alarms**, and **Get Advanced** are not available for the Report Viewer user role. You can view all the reports except the following:

- Launch CUCM Reports
 - Administrative Reports
 - Scheduled Reports
-
- **Helpdesk** — Views and accesses network status information only and cannot perform any action on a device or schedule a job that reaches the network.

- **Operator** — Performs all Helpdesk tasks and tasks related to the network data collection. Cannot perform any Inventory Management operations such as adding, discovering, or importing devices. Also, an operator cannot configure thresholds for Alarms and Events.
- **Network administrator** — Performs all Operator tasks and tasks that result in a network configuration change like credential management, threshold settings, and so on.
- **System administrator** — Performs the Assurance user interface-related administration tasks such as backup and restore, maintaining log files, configuring users, and so on.
- **Super administrator** — Can perform tasks that both system administrator and network administrator can perform.

Helpdesk is a preselected role that is assigned to every user in Cisco Prime Collaboration Assurance.

For Cisco Prime Collaboration Release 11.5 and later

Report Viewer is a preselected role that is assigned to every user in Cisco Prime Collaboration Assurance.

The roles selected for a user, determines the access to data of other users. For example, a user with the Super Admin role can view all other users, however a user with the Network Administrator role cannot view the users with higher roles such as Super Administrator, or System Administrator, but can look at other user's data whose role is of Operator or Helpdesk.

If you have deployed Cisco Prime Collaboration Assurance in MSP Mode, you can look at customers belonging to another user of the same role, only if you are associated with the customer(s).

If you have deployed Cisco Prime Collaboration Assurance in ENT Mode, you can look at domains belonging to another user of the same role, only if you are associated with the domain(s).

Note: The User Management submenu is not available to the following roles:

For Cisco Prime Collaboration Release 11.5 and later

1. Report Viewer
2. Helpdesk
3. Operator

For Cisco Prime Collaboration Release 11.6 and later

The default user role selection is removed from Cisco Prime Collaboration Assurance.



Note

If Report Viewer user role is selected, the system does not allow the user to choose any other roles and vice versa.

For Cisco Prime Collaboration Release 12.1 SP3 and later

The following roles are supported to provide multiple levels of authorization:

1. **Network Administrator** - Performs all Operator tasks and tasks that result in a network configuration change like credential management, and so on
2. **System Administrator** - Performs the user interface-related administration tasks.
3. **Super Administrator** - Performs tasks that both system administrator and network administrator can perform.

Related Topics

[Manage Customers](#), on page 75

[Manage Domains](#), on page 77

Single Sign-On for Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance provides users with admin privileges to enable Single Sign-On (SSO) in Cisco Prime Collaboration Assurance using Security Assertion Markup Language (SAML).

Cisco Prime Collaboration Assurance does not support multiserver SAN certificates and end user SAML SSO.

Ensure that the following prerequisites are met before you enable SSO:

- At least one LDAP Administrative user exists in the system—by manually creating an LDAP administrative user in Cisco Prime Collaboration Assurance.
- An Identity Provider (IdP) server that enables you to use SSO to access many other applications from a single hosted application and a Service Provider. The Service Provider is a website that hosts the applications.

Following are the supported third-party IdP servers:

- Open Access Manager (OpenAM)
- Ping Identity
- Active Directory Federation Services (ADFS)
- Oracle Identity Manager

For the steps to setup an IdP server, see the [SAML SSO Deployment Guide for Cisco Unified Communication Applications, Release 10.0\(1\)](#).

- Download the Identity Provider metadata file from the IdP server and save it in your local system.

To enable Single Sign-On:

Step 1 Choose **System Administration > Single Sign-On**.

Step 2 Click **Enable SSO**.

A warning message is displayed stating, Enabling SSO redirects you to the IdP server for authentication from the next login. To access the application, you will need to be authenticated successfully.

Note **Enable SSO** is disabled if the above mentioned prerequisites are not met.

Step 3 Click **Continue**.

Step 4 Follow the steps provided in the SSO wizard to enable Single Sign-On.

- Locate the IdP metadata file from your local system and click **Import IdP Metadata**.
- Click **Download Trust Metadata file**.
- Launch the IdP server and import the downloaded Trust Metadata file.

Note This is a manual step for Enabling SSO. You need to create a Circle of Trust (CoT) in the IdP server and log out before you proceed with the SSO testing.

- To run SSO Test Setup, select a username from the **Valid Administrative Usernames** drop-down. You can enter any user who is an administrator in Active Directory and is synchronized by Cisco Unified CDM under SSO user.

Note Using any other username to log in to the IdP server might lock the administrator account.

- e) Click **Run SSO Test** to test the connectivity among the IdP server, Cisco Prime Collaboration Assurance Applications, and Single Sign-On.

If you are prompted with an error message, Unable to do Single Sign-On or Federation:

- Manually log in to the IdP server using the end user credentials and check if the authentication is successful.
- Verify if the Trust Metadata file is successfully uploaded in the IdP server.
- Verify if the Cisco Prime Collaboration Assurance server and the IdP server are part of the same Circle of Trust.

- f) Click **Finish**.

Troubleshooting and Logs for SSO

- When you are logged out of the Cisco Prime Collaboration Assurance server while enabling SSO, it is recommended that you close the browser and re-launch the Cisco Prime Collaboration Assurance application. Because, though your conference expires in Cisco Prime Collaboration Assurance server, the IdP server conference might still be active.
- While enabling SSO, ensure that the hostname for Cisco Prime Collaboration Assurance is set and is part of DNS.

When IdP server is down, you can:

- Use the recovery URL- `https://<PCserver IP address or host name that is part of DNS>:8443/ssosp/local/login`.
- Disable Single Sign-On from CMD Utility.

To disable SSO from CMD utility in Cisco Prime Collaboration Assurance applications:

- Log in to Cisco Prime Collaboration Assurance server using SSH with port 26.
- Navigate to the `/opt/emms/emsam/bin` directory for Cisco Prime Collaboration Assurance. Add `<Operation>` and `<Value>` entries for `cpcmconfigsso.sh` file based on the following table:

Operations can be ..	Values can be ..
1-To get the Single Sign-On status	Not applicable
2-To get the recovery URL status	Not applicable
3-To set the Single Sign-On status	False Note You cannot enable SSO through CLI. Use the user interface procedure to enable SSO.
4-To set the recovery URL status	True or False

- To disable SSO, run the following command:

cpcmconfigsso.sh 3 false



Note The recovery URL is enabled. If you want to disable it for security reasons, set it as False by default.

Default User Accounts

Cisco Prime Collaboration Assurance is preconfigured with a default web client administrator user called `globaladmin`; `globaladmin` is a superuser who can access Cisco Prime Collaboration Assurance user interfaces.

Specify a password for `globaladmin` when you configure your virtual appliance. You need to use these credentials when you launch the Cisco Prime Collaboration Assurance web client for the first time.

**Caution**

We recommend that you note down the root password, as if it is forgotten/lost you will have to open a TAC support case to reset the root password.

If you are logging in for the first time to the Cisco Prime Collaboration Assurance web client, log in as `globaladmin`.

**Note**

See the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#) for password validation rules for these users.

**Caution**

You must not create a user with the name: `globaladmin`, `pmadmin` and `admin`.

Choose . Click the Download Log button. Download the tar file and untar it. Check the `/opt/emms/emsm/log/importedprovisioninguser.log` file, to find the users who were not imported into Cisco Prime Collaboration Assurance database due to several reasons such as duplicate user names (user names already used in Cisco Prime Collaboration Assurance), user names with no passwords and so on.

The Cisco Prime Collaboration Assurance applications do not share inventory database. You must manage the devices separately to perform the tasks. See [Manage Device Credentials, on page 85](#) to perform device management tasks using the Cisco Prime Collaboration Assurance application.

Related Topics

[Manage Device Credentials](#)

[Manage Device Groups](#), on page 139

User Roles and Tasks

The [User Roles and Tasks](#) for Cisco Prime Collaboration Assurance 11.x versions and [User Roles and Tasks](#) for Cisco Prime Collaboration Assurance 12.x versions lists the Cisco Prime Collaboration Assurance user roles and tasks they are mapped to.

**Note**

Super administrator has access to all of the user interface menus and can perform all the tasks. Hence, the super administrator is not listed .

Related Topics

[User Roles and Tasks for Cisco Prime Collaboration Assurance](#)

Add a User

You can add a user and assign predefined static roles. The user has access to the Cisco Prime Collaboration Assurance web client only and cannot log in to the Cisco Prime Collaboration Assurance server through the CLI.

To add a user:

Step 1 Choose **System Administration > User Management**.

Step 2 In the **User Management** page, click **Add**.

Step 3 In the **Add User** page, enter the required user details.

Note that because the LDAP server performs authentication, it should have the same user ID as Cisco Prime Collaboration Assurance. For more information, see [Configure an LDAP Server](#).

If you select the LDAP User option, the **Password** and **Confirm Password** fields are not displayed.

Step 4 Select the appropriate Cisco Prime Collaboration Assurance roles.

Step 5 Click **Save**.

To edit user details, select a user at **System Administration > User Management** and make the necessary changes.

For Cisco Prime Collaboration Release 11.6 and later

To exclude Report Viewer user role from the assigned roles, you have to manually deselect the Report Viewer option and click **Save**.

As part of your regular system administration tasks, you sometimes must delete users from the Cisco Prime Collaboration Assurance database. However, you cannot delete the Cisco Prime Collaboration Assurance web client default administrator *globaladmin*.

To delete a user, select the user from **System Administration > User Management** and click **Delete**. Any jobs that are scheduled in the deleted user name continue to run until canceled.

Modify User Roles

When the contact information, role, or account status of a user changes, the administrator must edit the corresponding details in the system.

To edit user details, select a user at **System Administration > User Management** and make the necessary changes.

For Cisco Prime Collaboration Release 11.6 and later

To exclude Report Viewer user role from the assigned roles, you have to manually deselect the Report Viewer option and click **Save**.

As part of your regular system administration tasks, you sometimes must delete users from the Cisco Prime Collaboration Assurance database. However, you cannot delete the Cisco Prime Collaboration Assurance web client default administrator - *globaladmin*.

To delete a user, select the user from **System Administration > User Management** and click **Delete**. Any jobs that are scheduled in the deleted user name continue to run until they are cancelled.

Configure an LDAP Server

You can configure Cisco Prime Collaboration Assurance to connect to a Lightweight Directory Access Protocol (LDAP) server, to access user information stored in the LDAP server.

You must create an LDAP user from the User Management page to enable the user to log in using LDAP credentials. To add a user, see [Add a User](#) and to edit or delete a user, see [Modify User Roles](#).

Cisco Prime Collaboration Assurance supports one primary LDAP server and one backup LDAP server.

To configure LDAP server:

Step 1 Choose **System Administration > LDAP Settings**.

Step 2 In the LDAP Settings page, enter values for all the fields. See [LDAP Configuration Parameters](#) for the field descriptions.

Note a. If Cisco Prime Collaboration Assurance must use SSL encryption, check the Use SSL check box and specify port 636.

For Cisco Prime Collaboration Release 12.1

LDAP configuration with SSL enabled is not supported.

b. In case of invalid login, a message indicating that “Invalid Username or Password. Please try again or check LDAP server configuration if you are a LDAP user” appears. This message is applicable for both local and LDAP users.

Step 3 Click **Test Connection** to check the connectivity to the LDAP server.

Step 4 Upon successful connection, click **Apply Settings** and restart Cisco Prime Collaboration Assurance Server to log in using LDAP.

Note To restart Cisco Prime Collaboration Assurance server, login as *root* and execute the following commands:

1. Stop the processes:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh stop
```

2. Check the status of the processes - Verify whether the processes have stopped:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh status
```

3. Restart the processes:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh start
```

LDAP Configuration Parameters

For example, Consider Microsoft Active Directory.

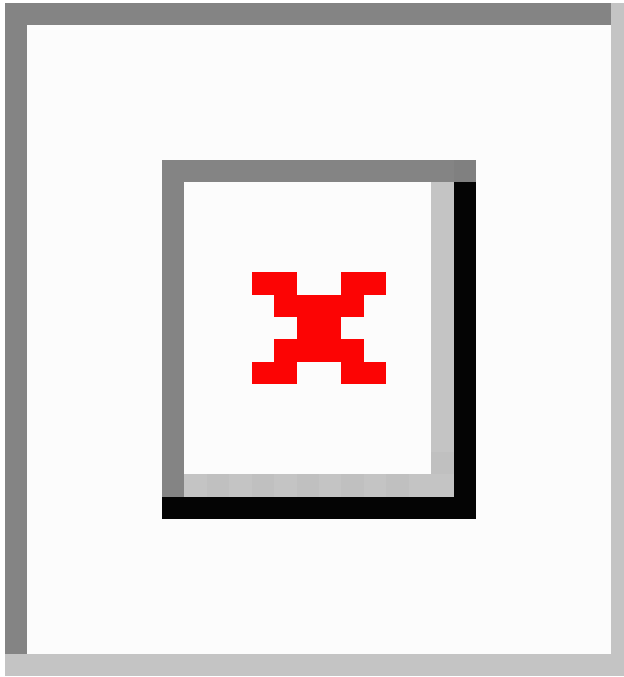


Table 15: LDAP Server Configuration

Field	Description
Server IP address	Enter the LDAP server name or IP address. Optionally enter the Backup LDAP server IP address.
Server Port	<p>Enter the Port number on which the LDAP requests for the server is received.</p> <p>Non-secure port: 389</p> <p>Secure SSL port: 636</p> <p>Optionally enter the Backup LDAP server Port number.</p> <p>Note If the LDAP server is configured to use a non-standard port, that port should be entered here as well.</p>

Field	Description
Admin Distinguished Name	<p>Admin Distinguished Name is the distinguished name to use.</p> <p>For example in the preceding image there is a user whose name is John Doe in the LDAP directory, so the Admin Distinguished Name will be as follows:</p> <ul style="list-style-type: none"> • CN = John Doe • OU = Campus • OU = AdminBLR • OU = ABC • DC = eta • DC = com
Admin Password	<p>Enter the password for the LDAP server authentication and reconfirm the password.</p> <p>Note Do not use the pound sign (#) in the password, because the connectivity to the LDAP server fails if the LDAP user password contains the pound sign (#).</p>
LDAP User Search Base	<p>Enter the user search base. LDAP server searches for users under this base.</p> <p>Search Base is as follows:</p> <ul style="list-style-type: none"> • DC = eta • DC = com <p>Note LDAP authentication fails if you enter special characters in the search base.</p>

**Note**

1. Cisco Prime Collaboration Assurance supports login to PCA with CN or sAMAccountName or uid attributes of an LDAP user as applicable.
2. uid attribute of an LDAP user should be unique.
3. The ampersand (&) character in Distinguished Names (DN) is not allowed in LDAP parameter value.
To connect to LDAP, enter the following LDAP parameter value -
`?CN=hq-prime,OU=Service Access Groups,DC=Megafon,DC=ru?`

For a list of supported LDAP servers, see [Supported Devices for Cisco Prime Collaboration Assurance](#).

Configure Maximum Length for Password

An authentication mechanism is only as strong as its credentials.

A strong authentication mechanism is important to force a strong password. Lack of password complexity, particularly password length, significantly reduces the search space.



Note

- The default maximum length of a password is 127 characters.
- Only the default administrator globaladmin has permissions to modify the security settings page in Cisco Prime Collaboration Assurance user interfaces.

Step 1 Choose **System Administration > Security Settings**.

Note Users must ensure to enter values within the range of 80-127 characters (not bytes). If the entered value is out of range then a message indicating that the value entered is out of the permissible range appears. Click **OK** to continue.

Step 2 Enter the value or click the spinners to configure the password length.

Step 3 Click **Save** to successfully update the configuration details. The application alerts that the user is modifying the maximum length of the password. Ensure compliance with this new value while setting password in other pages appears.

Click **Cancel** to exit.

Note Users cannot enter a password of length more than the configured value in any other page where password is required. An error message appears on the respective pages indicating incompliance.

Unlock Cisco Prime Collaboration Assurance Account

For Cisco Prime Collaboration Release 11.5 and later

The permissible login attempts to access the Cisco Prime Collaboration Assurance user interface is 10. If you make 10 failed attempts to log in to Cisco Prime Collaboration Assurance user interface, your account gets disabled.

A globaladmin user with administrator privileges can unlock the account.

To unlock the account:

Step 1 Log in to Cisco Prime Collaboration Assurance as globaladmin.

Step 2 Choose **System Administration > User Management**.

Step 3 On the **User Management** page, select the user and click **Unlock**.



CHAPTER 7

Manage Customers

This section explains the following:

- [Manage Customers, on page 75](#)
- [Add Customers, on page 75](#)
- [Global Customer Selection, on page 76](#)

Manage Customers

This section applies only if you have deployed Cisco Prime Collaboration Assurance in MSP mode.

The MSP mode provides multiple customer views. This option is used in managed service provider environments. This view enables you to manage networks and to host services of multiple customers that are being managed by Cisco Prime Collaboration Assurance. You can associate devices to customer.

You can choose if you want all existing managed endpoints or subscribers registered to a publisher inherit the customer name from the publisher. For more information, see [Add Devices -Auto Discovery](#).

Add Customers

To add a customer:

-
- | | |
|---------------|--|
| Step 1 | Choose Assurance Administration > Customer Management .
For Cisco Prime Collaboration Release 11.5 and later
Choose Alarm & Report Administration > Customer Management |
| Step 2 | From the Customer Management page, click Add . |
| Step 3 | In the General Info page, enter the required details, and click Next . |
| Step 4 | In the Devices/Device Group page, select the appropriate devices, and click Save . A message appears asking you to confirm the assigning of customers to the selected device(s). If you want to associate the registered endpoints to the customer to which the publisher or seed device such as Unified CM or VCS is associated, select the Assign Registered Endpoints also check box. A message notifies that the devices are associated with the customer. |
-

Related Topics

[Add a User](#), on page 70

[Manage Users](#), on page 65

Global Customer Selection

On the Cisco Prime Collaboration Assurance home page, you can select customers and filter information accordingly. Rest your mouse over the quick view icon next to the Customer field at the top-right corner of the Cisco Prime Collaboration Assurance user interface. You can select one or more customers for which you want to see data for. You can also select multiple customers at the same time by selecting All Customers to see aggregate information for all customers. By default, data is displayed for all the customers.

If you have logged in Cisco Prime Collaboration Assurance as a user associated with particular customers in Cisco Prime Collaboration Assurance, you can select the option All My Customers from the global customer selection list. You can further select specific customer(s) from your All My Customers group.

If you have logged in Cisco Prime Collaboration Assurance as a user or globaladmin associated with all customers available in Cisco Prime Collaboration Assurance, you can select the option All Customers from the global customer selection list. You can further select specific customer(s) from your All Customers group.

The Cisco Prime Collaboration Assurance user interface filters and shows only the information for the selected customer(s) from the global selection field, across all features such as Inventory Management, and Alarms and Events page.

**Note**

The Enterprise dashboards (End-Users Impact, Endpoints Utilization, Infrastructure, Topology, Contact Center Topology, depending on the licenses you have) in Cisco Prime Collaboration Assurance do not filter content by default through the global customer selection field. If you select another customer through global selection the user interface will refresh and the home page showing the Customer Summary dashboard appears. To change the customer you need to click the customer name from the Customer Summary dashboard.

For more information on how user roles will also determine the information available to you, see Cisco Prime Collaboration Assurance-Advanced User Roles.



CHAPTER 8

Manage Domains

This section explains the following:

- [Manage Domains, on page 77](#)

Manage Domains

This section explains about managing domains in Cisco Prime Collaboration Assurance.

Manage Domains

The Domain Management feature is supported if you have installed Cisco Prime Collaboration Assurance in Enterprise mode. You can group your devices and provide restricted view to some set of devices based on your business needs.



Note

Cisco Prime Collaboration Assurance supports the following scenarios according to the Domain Setup behavior:

1. Assign all Endpoints within the same cluster to the same Domain.
2. Cisco Prime Collaboration Assurance does not support assigning different Domains to different Endpoints within same cluster.
3. You can assign different domains for different infrastructure devices.

Related Topics

[Manage Users, on page 65](#)

Add Domains

To add a domain:

-
- Step 1** Choose **System Administration > Domain Setup**.
 - Step 2** From the **Domain Setup** page, click **Add**. You can associate device pools or devices to a domain.
 - Step 3** In the **Create Domain** page, enter the required details, and click **Save**.

All endpoints or subscribers registered to a publisher inherit the domain name from the publisher, if the publisher has been discovered with association to a single domain.

Note You cannot associate multiple domains to a device.

Click **Edit** to unassign an domain.

Note If you want to change the domain of a device pool, you need to unassign the device pool from existing domain before assigning it to a new domain. This limitation is only for device pools.

Click **Delete** to delete a domain. You have the option to delete a domain with the devices or without the devices. You can verify the changes in Inventory Management.

Global Domain Selection

On the Cisco Prime Collaboration Assurance home page, you can select domains and filter accordingly. Hover your mouse over the quick view icon next to the Domain field at the top-right corner of the Cisco Prime Collaboration Assurance user interface. You can select one or more domains based on your domain permission.

If you have logged in to Cisco Prime Collaboration Assurance as a user or globaladmin associated with all domains available in Cisco Prime Collaboration Assurance, you can select Enterprise to see the aggregate details for all domains. You can further select specific domains from My Enterprise group.

The Cisco Prime Collaboration Assurance user interface filters and shows only the information for the selected domains across features such as Inventory Management, and Endpoint Diagnostics. These columns are hidden by default.

For more information on how user roles will also determine the information available to you, see Cisco Prime Collaboration Assurance-Advanced User Roles.



CHAPTER 9

Configure System Parameters

This section explains the following:

- [Configure System Parameters](#), on page 79

Configure System Parameters

The following are the system configuration parameters for Cisco Prime Collaboration Assurance.

- **SMTP Server** — To configure this parameter under **Assurance Administration > E-mail Setup for Alarms & Events**, see [Configure SMTP Server](#).

For Cisco Prime Collaboration Release 11.5 and later

SMTP Server—To configure this parameter under **Alarm & Report Administration > E-mail Setup for Alarms & Events**, see [Configure SMTP Server](#).

- **Call Quality Data Source Management** — Cisco Prime Collaboration Assurance monitors voice-quality measurements in a VoIP network. This real-time, service-quality information is collected from Unified CM or Prime vNAM. To configure this parameter under **Assurance Administration > CDR Source Settings > Manage Call Quality Data Sources**, see [Update Call Detail Records NAM Credentials](#).

For Cisco Prime Collaboration Release 11.5 and later

Call Quality Data Source Management — Cisco Prime Collaboration Assurance monitors voice-quality measurements in a VoIP network. This real-time, service-quality information is collected from Unified CM or Prime vNAM. To configure this parameter under **Alarm & Report Administration > CDR Source Settings > Manage Call Quality Data Sources**, see [Update Call Detail Records NAM Credentials](#).

- **LDAP Settings** — To configure this parameter under **System Administration > LDAP Settings**, see [Configure an LDAP Server](#).
- **Log Management** — To configure this parameter under **System Administration > Log Management**, see [Log Levels](#).
- **SFTP Settings** — To monitor calls from Unified CM, you must configure SFTP. To configure this parameter under **Assurance Administration > CDR Source Settings > CUCM SFTP Credentials**, see [Configure SFTP Settings](#).

For Cisco Prime Collaboration Release 11.5 and later

SFTP Settings — To monitor calls from Unified CM, you must configure SFTP. To configure this parameter under **Alarm & Report Administration > CDR Source Settings > CUCM SFTP Credentials**, see [Configure SFTP Settings](#).

For Cisco Prime Collaboration Release 12.1 SP3 and later

SFTP Settings - To monitor calls from Unified CM, you must configure SFTP. To configure this parameter under **Inventory > Inventory Management**. Click on **CUCM SFTP Credentials** tab, see [Configure SFTP Settings](#).

- Cluster Device Discovery Settings - Allows Cisco Prime Collaboration Assurance to consolidate the inventory and the device registration information it collects from Unified CM. To configure this parameter under **Inventory > Cluster Device Discovery Schedule**, see [Schedule Cluster Device Discovery](#), on page 134.

Global System Parameters

The changes performed on these pages are applicable to all domains (Enterprise mode).

Table 16: System Parameters

Tasks	Navigation
Configure Single Sign-On.	System Administration > Single Sign-On
Add a license file.	System Administration > License Management
Configuring SMTP server.	Alarm & Report Administration > E-mail Setup for Alarms & Events
Configure SSL Certificate Authentication for Device Discovery.	System Administration > Certificate Management
Configure LDAP server to access user details.	System Administration > LDAP Settings
Change the log levels, the default value is “Error”.	System Administration > Log Management
Configure SFTP parameters to monitor calls from Unified CM.	Inventory > Inventory Management > CUCM/sFTP Credentials For Cisco Prime Collaboration Release 12.1 SP3 and later Inventory > Inventory Management. Click on CUCM SFTP Credentials tab.
Configure parameters to consolidate the inventory and the device registration information from Unified CM.	Inventory > Cluster Device Discovery Schedule
Add a dial plan.	Alarm & Report Administration > CDR Analysis Settings > Dial Plan Configuration
Create a call category.	Alarm & Report Administration > CDR Analysis Settings > Call Category Configuration

Tasks	Navigation
Configure parameters to poll devices.	Alarm & Report Administration > Polling Settings
Customize the syslog rules to monitor faults.	Alarm & Report Administration > Event Customization > Syslog Rules
Configure alarm notification (e-mail, syslog, or trap).	Alarm & Report Administration > Notification Setup > Custom Notification
Configure Voice Call Grade Settings (Good, Acceptable, Poor).	Alarm & Report Administration > CDR Analysis Settings > Configure Voice Call Grade
Configure audio phones report export parameters, such as audio phone reports (IP phone audit, move, suspect IP phones), file format, export file location, and notification e-mail.	Reports > UCM/CME Phone Activity Reports > Export Audio Phones
Schedule regular backups.	System Administration > Backup Settings

Configure SMTP Server

You can configure the SMTP server to send and receive e-mail notifications for alarms by specifying the SMTP server name and the sender AAA E-mail address on the **E-mail Setup for Alarms & Events** page (**E-mail Setup for Alarms & Events**). The value in the **Sender AAA E-mail Address** field helps you to identify the server you receive the e-mail from, in case of many servers.

Configure Cisco Prime Collaboration Assurance Server Time Zone

To configure the Cisco Prime Collaboration Assurance server time zone:

-
- Step 1** Log in to the Cisco Prime Collaboration Assurance server with the account that you have created during installation. By default, it is *admin*.
- Step 2** Enter the following command to see the list of supported time zones:
- Example:**
- ```
cm/admin# show timezones
```
- Step 3** Enter the following commands to set the time zone for the Cisco Prime Collaboration Assurance server:
- Example:**
- ```
cm/admin(config)# config t
cm/admin(config)# clock timezone US/Pacific
cm/admin(config)# exit
```
- Step 4** Enter the following command to copy running-configuration to startup-configuration:
- Example:**
- ```
cm/admin# write memory
```
- Step 5** Enter the following command to restart the Cisco Prime Collaboration Assurance server:

**Example:**

```
cm/admin# application stop cpcm
cm/admin# show application status cpcm
cm/admin# application start cpcm
```

**Step 6**

Wait for 10 minutes for the server to finish the restart process and enter the following command to check if the time zone is set to the new value:

**Example:**

```
cm/admin# show timezone
US/Pacific
```

**Note** We recommended you to keep the time zone values configured in postgres database same as that of system time zone to avoid the data mismatch issues. If you change system time zone manually, then change the `log_timezone` and `timezone` parameters in `postgres.conf` file in `/opt/postgres/9.2/data` (Analytics database) and `/opt/postgres/9.2/cpcmdata` (Assurance database, including both `cpcm` and `qovr` database) to match system time zone, and then restart the system. Root access feature is mandatory to change time zone value in postgres database, hence you should raise a TAC case to obtain root access.

---



## PART **III**

# **Manage Devices in Cisco Prime Collaboration Assurance**

- [Manage Device Credentials, on page 85](#)
- [Set Up Clusters, on page 103](#)
- [Discover Devices, on page 105](#)
- [Manage Device Groups, on page 139](#)
- [Manage Inventory, on page 145](#)
- [Poll Devices, on page 189](#)





## CHAPTER 10

# Manage Device Credentials

This section explains the following:

- [Manage Device Credentials, on page 85](#)
- [Add a Device Credentials Profile, on page 86](#)
- [SSL Certificate Authentication for Device Discovery, on page 97](#)
- [Modify Device Credentials, on page 98](#)
- [Verify Device Credentials, on page 98](#)
- [Delete a Device Credential Profile, on page 101](#)

## Manage Device Credentials

You need to configure device credentials for all devices that are managed using Cisco Prime Collaboration Assurance. Device credentials are required for discovering devices and updating inventory. If the credentials vary for different devices, create separate credentials profiles; that is, if you want to manage two Cisco Unified Communications Managers with different credentials in Cisco Prime Collaboration Assurance, you must create two separate credentials profiles. For more information, see the table on [Credential Profiles Field Descriptions](#).

The following are some of the requirements while creating credentials profiles:

- HTTP and SNMP credentials are mandatory for the endpoints to get into Managed state.
- **For Cisco Prime Collaboration Release 11.1 and earlier**  
CLI credentials are required to troubleshoot sessions involving endpoints and network devices.
- **For Cisco Prime Collaboration Release 11.5 and later**  
CLI credentials are required to manage video test call and analyzing call signaling through SIP Call Flow Analyzer.
- JTAPI credentials are mandatory for Unified CM for conference monitoring. This credential is not required for endpoints.
- Create an Enterprise License Manager profile by selecting Enterprise License Manager as the device type for Prime License Manager.
- Define HTTP and SNMP credentials for Unified Contact Center devices such as Cisco Unified Intelligence Center (CUIC), Cisco Voice Portal (CVP), Cisco Finesse, Cisco SocialMiner, Cisco Unified Contact

Center Enterprise (Unified CCE), Cisco Unified Contact Center Express (Unified CCX), Cisco MediaSense.

#### For Cisco Prime Collaboration Release 11.5 and later

Define HTTP and SNMP credentials for Unified Contact Center devices such as Cisco Unified Intelligence Center (CUIC), Cisco Voice Portal (CVP), Cisco Finesse, Cisco SocialMiner, Cisco Unified Contact Center Enterprise (Unified CCE), Cisco Unified Contact Center Express (Unified CCX), Cisco Virtualized Voice Browser.

- Enter HTTP credentials for Contact Center Enterprise in the following format: domain\administrator. For example hcsdc2\administrator.
- Enter HTTP credentials for Cisco Unified Customer Voice Portal (CVP) which have the *ServiceabilityAdministrationUserRole* privileges. The default username *wsmadmin* has this privilege.
- Credentials are not required for the phones, Cisco Cius, Cisco Jabber, and Cisco Jabber Video for TelePresence (Movi) endpoints. These endpoints are discovered with the discovery of the call processor with which they are registered.
- Select VCS/ EXPRESSWAY in the Device type drop-down list to create credentials for Cisco Expressway-Core, Cisco Expressway-Edge or a Cisco VCS with Cisco Collaboration Edge or Core.



#### Note

- You must not enter \* symbol with length of eight characters as SNMP Community String, SNMPv3, HTTP, JTAPI, and MSI password while creating credentials profiles in Credential Profile page or Add Device in Device Discovery.
- You must not enter % symbol with length of eight characters as password for CLI while creating credentials profiles in Credential Profile page or Add Device in Device Discovery.

## Add a Device Credentials Profile

To add or clone a credential profile:

- Step 1** In the **Cisco Prime Collaboration Assurance** page, choose **Device Inventory** > **Inventory Management** from the Toggle Navigation pane.  
**For Cisco Prime Collaboration Release 11.5 and later**  
In the **Cisco Prime Collaboration Assurance** page, choose **Inventory** > **Inventory Management** from the Toggle Navigation pane.  
The **Inventory Management** page is displayed.
- Step 2** In the Credentials Profile page, click **Add** and enter the necessary information described in the Table on [Credential Profiles Field Descriptions, on page 87](#).
- Step 3** Click **Save**.



In your network, you may have configured the same SNMP credentials for all devices. In such cases, first create a new profile and later clone the existing profile. To clone, in the Credentials Profile page, select an existing profile and click **Clone** and after the required updates click **Add/Update**.

## Credential Profiles Field Descriptions

After the devices are discovered, you can check the current Inventory table to verify that the credentials have been updated in the Cisco Prime Collaboration Assurance database.

The following table describes the fields on the Credential Profiles page.

**Table 17: Credential Profiles Field Descriptions**

| Field Name   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile Name | Name of the credential profiles.<br><br>For example: <ul style="list-style-type: none"><li>• CUCM</li><li>• router_switches</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Device Type  | (Optional) The credential fields (such as SNMP, HTTP, CLI) are displayed, based on the device type that you have selected.<br><br>To reduce rediscovery time, we recommend that you select the device type when you create the credential profiles.<br><br>The default device type is “Any”, if you do not select a device type while creating a credential profile.<br><br>See <a href="http://cisco.com">cisco.com</a> for the list of device types.<br><br>For EX series, MX series, SX series, bare Codec devices, and all profiles with Codec, select the device type as TC_CE.<br><br>While managing coresident PLM, you should provide both CLI and HTTP credentials. <ul style="list-style-type: none"><li>• CLI credentials are used to access the license information.</li><li>• HTTP credentials are used to manage Prime License Manager in Cisco Prime Collaboration Assurance.</li></ul> |

| Field Name  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Type | <p><b>For Cisco Prime Collaboration Release 12.1 and later</b></p> <p>While managing co-resident PLM, you should provide both CLI and HTTP credentials.</p> <ul style="list-style-type: none"> <li>• CLI credentials are used to access the license information.</li> <li>• HTTP credentials are used to manage Prime License Manager in Cisco Prime Collaboration Assurance.</li> </ul> <p>Ensure the following conditions are met for the Router to be identified as a Cisco Unified Border Element (CUBE):</p> <ol style="list-style-type: none"> <li>1. CLI credentials (CLI Login Username and CLI Login Password) for the Device Type - Router is mandatory.</li> <li>2. Enabling SSH version 2 or later on Port 22 of the Router is mandatory.</li> <li>3. If Enable Password is set on the Router then provide the password in CLI Enable Password field.</li> </ol> <p><b>For Cisco Prime Collaboration Release 11.6 and later</b></p> <p>For EX series, MX series, SX series, DX series with CE image, bare Codec devices, and all profiles with Codec, select the device type as Codec.</p> <p>For MSE devices, select Cisco MCU as the device type.</p> <p><b>For Cisco Prime Collaboration Release 11.5 and later</b></p> <p>For Cisco Virtualized Voice Browser devices, select Virtualized Voice Browser device type.</p> <p>You can enter any credentials (SNMP, HTTP, CLI, MSI) to create an “Any” credential profile. You must create an “Any” credential profile to run auto-discovery (Ping Sweep and CDP discovery). However, you can run logical discovery also.</p> <p>If your network has multiple subnets, then create an “Any” profile for each subnet.</p> |
| IP Version  | The IP address is version 4 or version 6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Field Name         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address Pattern | <p>IP address of the devices for which the credentials are provided. You must:</p> <ul style="list-style-type: none"> <li>• Separate multiple IP addresses by the delimiter pipe ( ).</li> <li>• Not use 0.0.0.0 or 255.255.255.255.</li> <li>• Not use question mark (?).</li> </ul> <p>We recommend that you:</p> <ul style="list-style-type: none"> <li>• Enter the exact IP address for Cisco Unified CM, and Cisco TMS.</li> <li>• Enter the exact IP address for either CTS or network devices.</li> <li>• Do not use many wildcard expressions in the address patterns.</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>• 100.5.10.* 100.5.11.* 100.5.20.* 100.5.21.*</li> <li>• 200.5.1*.* 200.5.2*.* 200.5.3*.*</li> <li>• 172.23.223.14</li> <li>• 150.5.*.*</li> </ul> <p>Avoid using patterns such as 150.*.*.*, 192.78.22.1?, 150.5.*.*./24.</p> <p>If you are unable to find a common pattern for the devices, enter *.*.*.*.</p> <p>Minimize the use of wildcard character (*), while defining the IP address patterns in the credential profiles.</p> <p><b>For Cisco Prime Collaboration Release 11.5 and later</b></p> <p><b>Inventory &gt; Inventory management &gt; Manage Credentials</b></p> <p>Use of wildcard character may increase the discovery time.</p> <p>See SNMPv2C to understand how the patterns are used.</p> |

| Field Name                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General SNMP Options                               | SNMP Timeout - The default is 10 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                                    | SNMP Retries - The default is 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                    | SNMP Version - Selecting an SNMP version is mandatory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SNMPv2C<br>Used to discover and manage the device. | SNMP Read Community String<br>You can provide either SNMPv1 or SNMPv2C credentials. We recommend that you use different SNMP credentials for Cisco TelePresence systems and network devices.<br><br>Cisco Prime Collaboration Assurance searches the credential profiles, based on the IP address pattern. Cisco Prime Collaboration Assurance then chooses a profile for which the SNMP credentials match. There can be multiple matching profiles, that is, profiles with the same SNMP credentials. In such cases, Cisco Prime Collaboration Assurance chooses the profile that matches first.<br><br><b>For Cisco Prime Collaboration Release 11.1 and earlier</b><br><br><b>Note</b> If multiple profiles have the same SNMP credentials but different CLI credentials, Cisco Prime Collaboration Assurance might chose a profile that contains the correct SNMP credentials but incorrect CLI credentials for the device. If this occurs, the troubleshooting workflow might not work. |
|                                                    | SNMP Write Community String                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SNMPv3<br>Used to discover and manage the device.  | SNMP Security Name - Enter a security name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                    | SNMP Authentication Protocol - You can choose either MD5 or SHA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                    | SNMP Authentication Passphrase - Enter a passphrase.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                    | SNMP Privacy Protocol - You can choose either AES, AES128, or DES.<br><br><b>For Cisco Prime Collaboration Release 11.5 and later</b><br><br>SNMP Privacy Protocol - You can choose either AES128, or DES.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Field Name                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>CLI</p> <p>Used to access the device through CLI to discover media path for troubleshooting.</p>      | <p>CLI Login Username and Password</p> <p>The CLI credentials are used during the troubleshooting workflow. If the credentials are not entered or if the entered credentials are incorrect, the troubleshooting workflow feature may not work.</p> <p><b>For Cisco Prime Collaboration Release 11.5 and later</b></p> <p>The CLI credentials are used to manage video test call and analyze call signaling through SIP Call Flow Analyzer.</p> <p><b>For Cisco Prime Collaboration Release 12.1 and later</b></p> <p>Ensure the following conditions are met for the Router to be identified as a Cisco Unified Border Element (CUBE):</p> <ol style="list-style-type: none"> <li>1. CLI credentials (CLI Login Username and CLI Login Password) for the Device Type - Router is mandatory.</li> <li>2. Enabling SSH version 2 or later on Port 22 of the Router is mandatory.</li> <li>3. If Enable Password is set on the Router then provide the password in CLI Enable Password field.</li> </ol> |
| <p>HTTP</p> <p>Used to access the device through HTTP to poll system status and meeting information.</p> | <p>HTTP Username and Password</p> <p>Cisco Prime Collaboration Assurance first checks the access for HTTP. If the access attempt fails, then Cisco Prime Collaboration Assurance checks the access for HTTPS.</p> <p>If you log in to Cisco TMS using the &lt;domain/username&gt; format, then ensure that you add the same &lt;domain/username&gt; value in the <b>HTTPS Username</b> field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p>JTAPI</p> <p>Used to retrieve the session status information from the Cisco Unified CM.</p>           | <p>(Optional) JTAPI Username and Password.</p> <p><b>Note</b> Password must not contain a semicolon (;) or equals (=).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Field Name | Description |
|------------|-------------|
|            |             |

| Field Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <p><b>For Cisco Prime Collaboration Release 11.5 and later</b></p> <p>Used to retrieve the session status information from the Cisco Unified CM.</p> <p><b>For Cisco Prime Collaboration Release 12.1 SP1</b></p> <p>A new set of JTAPI specific parameters are introduced to secure the JTAPI (TLS v1.2) connection.</p> <p><b>Note</b></p> <ol style="list-style-type: none"> <li>1. For more information on the method to secure the CTI, JTAPI, and TAPI applications and to know more about the certificate authority proxy function, see the Chapter on “<a href="#">Authentication and Encryption Setup for CTI, JTAPI, and TAPI</a>” and “<a href="#">Certificate Authority Proxy Function</a>” respectively in the “Security Guide for Cisco Unified Communications Manager”.</li> <li>2. Ensure that the CUCM is in Mixed mode.</li> </ol> <p>Following are a set of JTAPI specific parameters.</p> <ol style="list-style-type: none"> <li>1. <b>Secure Connection</b> check box <ol style="list-style-type: none"> <li>a. <b>Check the check box</b> - Checking this option enables you to have a secure TLS connection to Cisco Unified Communications Manager.<br/><br/>A warning message appears indicating you to "Ensure that “Standard CTI Secure Connection” role is associated with this JTAPI user, along with other required roles". Click OK to return to Cisco Prime Collaboration Assurance.</li> <li>b. <b>Uncheck the check box</b> - If the check box is not checked, JTAPI cannot make a secure connection.<br/><br/>A warning message appears indicating you to "Ensure that “Standard CTI Secure Connection” role associated with this JTAPI user is removed. To continue to Monitor Conferences, ensure that the required roles are configured". Click OK to return to Cisco Prime Collaboration Assurance.</li> </ol> </li> </ol> <p>For more information, see <a href="#">Setting up Devices for</a></p> |

| Field Name | Description                                                                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <a href="#">Cisco Prime Collaboration Assurance</a> .<br>The check box enables you to enter the parameters in (enable or disable) the new Secure JTAPI fields. |



| Field Name | Description |
|------------|-------------|
|------------|-------------|

| Field Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <p><b>2. TFTP Server IP Address</b> - Specify the IP address of the TFTP Server.</p> <p><b>Note</b> The value must be one of the nodes on the CUCM cluster. Make sure that the TFTP service is running on that node.</p> <p><b>3. TFTP Server Port</b> - The TFTP Server Port defaults to 69.</p> <p><b>Note</b> Do not change the default value unless the System Administrator recommends.</p> <p><b>4. CAPF Server IP Address</b> - Specify the IP address of the CAPF Server.</p> <p><b>Note</b></p> <ol style="list-style-type: none"> <li>1. For more information on the certificate authority proxy function, see the Chapter on “<a href="#">Certificate Authority Proxy Function</a>” in the “Security Guide for Cisco Unified Communications Manager”.</li> <li>2. Ensure to select <b>RSA Only</b> from the <b>Key Order</b> drop-down list while creating the CAPF profile on CUCM.</li> <li>3. You must always provide the CUCM Publisher IP Address.</li> </ol> <p><b>5. CAPF Server Port</b> - The CAPF Server Port number defaults to 3804.</p> <p><b>Note</b> Ensure that the value entered matches with the value that is configured in Cisco Unified Communication Manager.</p> <p><b>7. Instance ID for Publisher</b> - This field specifies the application instance identifier configured in CAPF Settings section of Application or End User CAPF profile configuration page in the Cisco Unified Communication Manager cluster.</p> <p><b>8. Secure Authentication String</b> – Enter the Authentication String configured in CAPF Settings section of Application or End User CAPF profile configuration page in the respective Communication Manager Publisher.</p> <p><b>Note</b> The section on <a href="#">Troubleshooting Secure JTAPI Connection</a> lists the details of troubleshooting the possible errors and recommended actions "with setup of</p> |

| Field Name | Description                                                                               |
|------------|-------------------------------------------------------------------------------------------|
|            | CUCM for Secure JTAPI and Sessions not coming up on Conference Diagnostics" respectively. |

#### For Cisco Prime Collaboration Release 11.5 and later

The following devices are renamed in Credential Profiles Page:

- CISCO INTERACTION MANAGER is renamed as WEB/EMAIL INTERACTION MANAGER
- CUIC is renamed as INTELLIGENCE CENTER
- CTS is renamed as CTS/IX ENDPOINT
- CISCO UNIFIED COMMUNICATIONS MANAGER is renamed as COMMUNICATIONS MANAGER
- C\_SERIES CODEC is renamed as TC/CE ENDPOINT
- E20 is renamed as E20 ENDPOINT
- ISDN is renamed as ISDN GATEWAY
- MCU is renamed as MULTIPOINT CONTROLLER
- MXP is renamed as MXP ENDPOINT
- ROUTER is renamed as ROUTER/VOICEGATEWAY
- TPS is renamed as TELEPRESENCE SERVER
- TELEPRESENCE CONDUCTOR is renamed as TELEPRESENCE CONDUCTOR



#### Note

You do not need to add credentials for Cisco Device, Cisco Unified Communications Manager Express (Cisco Unified CME), and UC500 Series devices in Credential Profiles page.

## SSL Certificate Authentication for Device Discovery

#### For Cisco Prime Collaboration Release 11.1 and earlier

In Cisco Prime Collaboration Assurance, when a device is added, the SSL certificates are exchanged for credential validation by accessing a protected resource using HTTPS. During exchange, the SSL certificate is not stored in Cisco Prime Collaboration Assurance trust-store and communication with the device fails, at a later point of time. It is recommended that you manually import the SSL certificate to Cisco Prime Collaboration Assurance trust-store to access the device.

Cisco Prime Collaboration Assurance enables you to check the authenticity of the SSL certificate during its communication with the devices or applications over HTTPS. However, this is not mandatory as you can still continue to discover the devices without authenticating the certificate.

Cisco Prime Collaboration Assurance does not validate the certificates from the devices or applications it communicates by default.

To enable the SSL certificate authentication:

- 
- Step 1** Choose **System Administration > Certificate Management**.  
The **Certificate Management** page is displayed.
- Step 2** In the **Device Certificate Management** tab, check the **Enable SSL certificate authentication for device discovery** check box.
- Step 3** Click the **Import Certificates** button.
- Step 4** Restart the Cisco Prime Collaboration Assurance server for the changes in trust manager to take effect.
- ```
cm/admin# application stop cpcm
cm/admin# show application status cpcm
cm/admin# application start cpcm
```
-

Modify Device Credentials

If you have modified credentials for the devices that you are currently managing in the Cisco Prime Collaboration Assurance application, you must modify the relevant credential profiles in the Cisco Prime Collaboration Assurance database.

If the credentials are incorrect, a major event — Device is inaccessible is triggered from Cisco Prime Collaboration Assurance (**Monitor > Alarms & Events > Events**).

To edit a credential profile:

-
- Step 1** Choose **Device Inventory > Inventory Management**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Inventory > Inventory Management**
- Step 2** From the Inventory Management page, select a device and click **Modify Credentials**.
- Step 3** Update the credentials as described in the Table on [Credential Profiles Field Descriptions](#), on page 87.
- Step 4** Click **Rediscover**.
- Cisco Prime Collaboration Assurance takes a few minutes to update its database with the modified credentials. After the credentials are updated, an informational event, Device is accessible from Collaboration Manager, is triggered. Cisco Prime Collaboration Assurance uses the updated credentials in the next polling job.
-

Verify Device Credentials

For Cisco Prime Collaboration Release 11.5 and later

If device discovery fails because of incorrect credentials, you can test the credentials for the failed devices and rediscover those devices. Choose **Inventory > Inventory Management > Discovery Jobs** for a list of devices that were not discovered.



Note Do not run this task when a discovery job is in progress.

To verify device credentials:

Step 1 For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**.

The **Inventory Management** page is displayed.

Step 2 From the Credential Profiles page, select the profile name to use for testing the credentials, and click **Verify**.

Step 3 Enter a valid device IP address to test the credentials. You can verify only one device at a time, and you cannot enter expressions such as *.*.*, 192.2.*.*, and so on.

Step 4 Click **Test**. You can see an inprogress moving icon next to the test button till the task completes. The test results are displayed under the Test Credential Result pane.

If the verification fails, see the possible reasons listed in [Credential Verification Error Messages](#).

Note All the nodes in the cluster may not be running all the protocols. For example, JTAPI may not be running on all the nodes. As a result, the credential validation test may fail for some of your nodes. After fixing the credentials issue, test the device credentials again and run the discovery for that device. After the devices are discovered, you can verify if the access information is updated in the Cisco Prime Collaboration Assurance database in the current Inventory table.

Credential Verification Error Messages

The credential verification error messages are tabulated below.

Table 18: Credential Verification Error Messages

Error Message	Conditions	Possible Solutions
SNMPv2		
SNMP Request: Received no response from <i>IP Address</i> .	Failed for one of the following reasons: <ul style="list-style-type: none"> • Device response time is slow. • Device is unreachable. • Incorrect community string entered in the credential profile. 	<ul style="list-style-type: none"> • Verify the device connectivity. • Update the credential profile with the correct community strings.

Error Message	Conditions	Possible Solutions
SNMP timeout.	Either the device response time is slow or the device is unreachable.	<ul style="list-style-type: none"> • Verify the device connectivity. • Increase the SNMP Timeout and Retries values in the credential profile.
Failed to fetch table due to: Request timed out.	Either the device response time is slow or the device is unreachable.	Increase the SNMP Timeout and Retries values in the credential profile.
SNMPv3		
The configured SNMPv3 security level is not supported on the device.	Device does not support the configured SNMPv3 security level.	Change the SNMPv3 security level to the supported security level in the credential profile.
The SNMPv3 response was not received within the stipulated time.	Either the device response time is slow or the device is unreachable.	Verify the device connectivity.
SNMPv3 Engine ID is wrong.	Incorrect engine ID entered in the credential profile.	Enter the correct SNMPv3 engine ID in the credential profile.
SNMPv3 message digest is wrong.	Failed for one of the following reasons: <ul style="list-style-type: none"> • Either the SNMPv3 authentication algorithm or the device password is incorrect. • Network errors. 	<ul style="list-style-type: none"> • Verify that the correct SNMPv3 authentication algorithm and device password are set in the credential profile. • Check for network errors.
SNMPv3 message decryption error.	Cannot decrypt the SNMPv3 message.	Verify that the correct SNMPv3 authentication algorithm is entered in the credential profile.
Unknown SNMPv3 Context.	The configured SNMPv3 context in the credential profile does not exist on the device.	Verify that the configured SNMPv3 context is correct in the credential profile.
Unknown SNMPv3 security name.	Either the SNMPv3 username is incorrect in the credential profile or the SNMPv3 username is not configured on the device.	Verify that the correct SNMPv3 username is set in the credential profile and on the device.
CLI		
Login authentication failed.	Incorrect credentials entered in the credential profile.	Verify and reenter the device CLI credentials in the credential profile.

Error Message	Conditions	Possible Solutions
Connection refused.	Either SSH or Telnet service may not be running on the device.	<ol style="list-style-type: none"> 1. Verify the device connectivity for the supported CLI (port). 2. Verify whether the SSH or Telnet service is running on the device.
HTTP		
Server returned HTTP response code: 401 for URL.	Either the HTTP service is not running or the URL is invalid.	<ul style="list-style-type: none"> • Verify whether the HTTP or HTTPS service is running on the device. • Verify whether the URL is valid on the server.
Connection refused.	The HTTP or HTTPS service is not running.	Verify whether the HTTP or HTTPS service is running on the device.
HTTP check failed.	Incorrect HTTP credentials entered in the credential profile.	Verify and reenter the device HTTP credentials in the credential profile.
For Cisco Prime Collaboration Release 11.1 and earlier		
MSI		
Failed to access MSI.	Incorrect MSI credentials entered in the credential profile.	Verify and reenter the device MSI credentials in the credential profile.

Delete a Device Credential Profile

You can delete only unused credential profiles. We recommend that you do not delete the credential profile of a device that is being managed in the Cisco Prime Collaboration Assurance application.

To delete a credential profile:

Step 1 Choose **Device Inventory > Inventory Management**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**

Step 2 In the Inventory Management page, click **Manage Credentials**. The credentials for a device that appears first on the list are displayed by default.

Step 3 Select the profile name and click **Delete**.



Set Up Clusters

This section provides information on the following:

- [Set Up Clusters, on page 103](#)

Set Up Clusters

Cisco Prime Collaboration Assurance manages the following clusters:

- Cisco TMS
- Cisco VCS
- Cisco Unified CM

If you are using more than one Cisco TelePresence Management Suite (TMS) in your network, you must configure these applications in a cluster for the Cisco Prime Collaboration Assurance application to manage; that is, Cisco Prime Collaboration Assurance cannot manage two standalone TMS.

Cisco Prime Collaboration Assurance monitors only the application servers. It does not monitor the database instances. Health polling is performed for all the Cisco TMS application servers in the clusters.

For TMS clusters, the conference details are imported from the primary Cisco TMS as defined on the Manage Clusters page.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can manage a CTX cluster also. Cisco Prime Collaboration Assurance cannot manage more than one CTX cluster. Health polling is performed for the CTX admin server in the cluster. For CTX clusters, the session details are imported from the primary admin server.

Manage Cisco TelePresence Manager or Cisco TMS Clusters

Before discovering Cisco TelePresence Manager or Cisco TMS clusters, you must enter the cluster details in the **Manage Cluster** page. During the discovery of Cisco TelePresence Manager or Cisco TMS, Cisco Prime Collaboration Assurance uses the cluster details, along with the device credentials (**Device Inventory > Inventory Management > Manage Credentials**) and discovers the management applications.



Note For adding CTX clusters, ensure that you create a new user with API role in the primary CTX admin server. For information on this procedure, see the [Setting up Devices for Prime Collaboration Assurance](#).

For Cisco Prime Collaboration Release 11.5 and later



Note Cisco TelePresence Manager and Cisco TelePresence Exchange (CTX) clusters are not supported.

Before discovering Cisco TMS clusters, you must enter the cluster details in the **Manage Cluster** page. During the discovery of Cisco TMS, Cisco Prime Collaboration Assurance uses the cluster details, along with the device credentials (**Inventory > Inventory Management > Manage Credentials**) and discovers the management applications.

To manage Cisco TMS clusters:

-
- Step 1** Choose **Device Inventory > Inventory Management**.
- For Cisco Prime Collaboration Release 11.5 and later**
- Choose **Inventory > Inventory Management**
- Step 2** From the **Inventory Management** page, click **Manage CTS-MAN/TMS Cluster**.
- If you have deployed Cisco Prime Collaboration Assurance in MSP mode, click **Manage CTS-MAN/TMS Cluster**.
- For Cisco Prime Collaboration Release 11.5 and later**
- From the **Inventory Management** page, click **Manage TMS Cluster**.
- If you have deployed Cisco Prime Collaboration Assurance in MSP mode, click **Manage TMS Clusters**.
- Step 3** In the **Manage Cluster** window, enter the cluster name and choose an item from the **Cluster Type** drop-down list.
- Step 4** For a TMS cluster: Enter the IP address of the primary active server, and the secondary active or passive server.
- For Cisco Prime Collaboration Release 11.5 and later**
- For a TMS cluster: Enter the IP address of the primary active server, and the secondary active or passive server.
- Step 5** Click **Add** to add a new cluster.
- Perform logical discovery to discover these clusters. For information on logical discovery, see [Discovery Methods](#). When you are discovering clusters for the first time in your network, you can enter primary, secondary, hot standby and load-balancer server details for CTS-MAN and TMS clusters. Later, to update inventory or rediscover, you can provide only the primary server details of CTS-MAN and TMS clusters.
-



CHAPTER 12

Discover Devices

This section explains the following:

- [Discover Devices, on page 105](#)

Discover Devices

You must perform discovery to manage devices in Cisco Prime Collaboration Assurance database. After adding the required device credentials, you can discover and manage all the [supported devices](#) in Cisco Prime Collaboration Assurance.

Discovery Life Cycle

Discovery involves three phases:

- Access-level discovery - Cisco Prime Collaboration Assurance does the following:
 1. Checks whether the device can be pinged using ICMP. If ICMP is not enabled on the device, the device is moved to the Unreachable state. See [Rediscover Devices](#) for information on how to disable ICMP verification.
 2. Gets all the defined credential profiles, based on the IP address. See [Manage Device Credentials, on page 85](#) to understand how to define the credential profiles.
 3. Checks whether the SNMP credentials match.
 4. Identifies the device types.
 5. Verifies all other mandatory device credentials, based on the device type. If the mandatory credentials are not defined, discovery fails. See [Manage Device Credentials, on page 85](#) for information on required device credentials.
- Inventory discovery - Cisco Prime Collaboration Assurance polls MIB-II and other device MIBs to collect information on the inventory, neighboring switches, and default gateway. It also verifies whether the polled device is supported in Cisco Prime Collaboration Assurance.
- Path trace discovery - Cisco Prime Collaboration Assurance verifies whether CDP is enabled on the device and discovers the topology, based on CDP. The links between the devices are computed using CDP and they are persisted in the Cisco Prime Collaboration Assurance database.

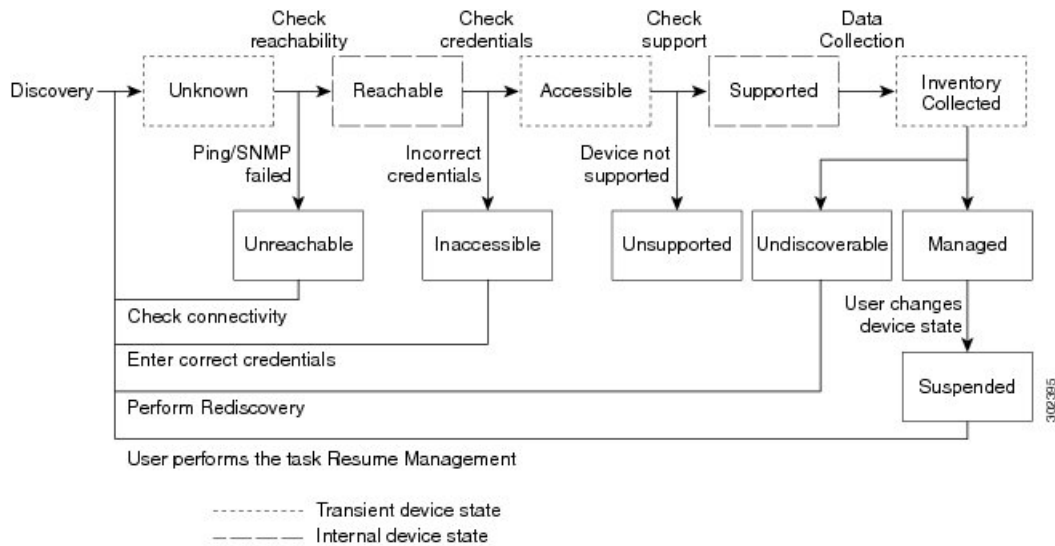
For Cisco Prime Collaboration Release 11.1 and earlier

Cisco Prime Collaboration Assurance discovers both Layer 2 and Layer 3 paths. The Layer 3 path is discovered when a troubleshooting workflow is triggered either manually or automatically. The default hop count is 2 and is not configurable.

A device state indicates that Cisco Prime Collaboration Assurance is able to access the device and collect the inventory. The device state is updated only after performing either a discovery or an update inventory task.

The following diagram shows the device discovery lifecycle.

Figure 2: Device Discovery Lifecycle



Cisco Prime Collaboration Assurance displays the following device states:

Table 19: Discovery States

Discovery States	Description
Unknown	This is the preliminary state, when the device is first added. This is a transient state.
Unreachable	Cisco Prime Collaboration Assurance is unable to ping the device using ICMP. If ICMP is not enabled on the device, the device is moved to the Unreachable state.
Unsupported	Cisco Prime Collaboration Assurance compares the device with the device catalog. If the device does not match with the devices in the device catalog or the SysObjectID is not known, the device is moved to this state.
Accessible	Cisco Prime Collaboration Assurance is able to access the device through all mandated credentials. This is part of the access-level discovery, which is an intermediate (transient) state during the device discovery.
Inaccessible	Cisco Prime Collaboration Assurance is not able to access the device through any of the mandated credentials, see Manage Device Credentials, on page 85 . You must check the credentials and discover the devices.

Discovery States	Description
Inventory Collected	Cisco Prime Collaboration Assurance is able to collect the required data using the mandated data collectors. This is part of the inventory discovery, which is an intermediate (transient) state during device discovery.
Undiscoverable	<p>Cisco Prime Collaboration Assurance is not able to collect the required data using the mandated data collectors. The device state can be undiscoverable when:</p> <ul style="list-style-type: none"> • Connectivity issues can be caused by SNMP or HTTP/HTTPS timeout. Also, if you use HTTP/HTTPS to collect data, only one HTTP/HTTPS user can log in at a time. If Cisco Prime Collaboration Assurance faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery. • There is no mandated data collection for Cisco Unified CM, CTS, CTMS, and other network devices. • Connectivity issues can be caused by SNMP or HTTP/HTTPS timeout. Also, if you use HTTP/HTTPS to collect data, only one HTTP/HTTPS user can log in at a time. If Cisco Prime Collaboration Assurance faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery.
Managed	<p>Cisco Prime Collaboration Assurance has successfully imported the required device data to the inventory database. All conference, endpoints, and inventory data are available for devices in this state.</p> <p>For Cisco Prime Collaboration Release 11.1 and earlier</p> <p>You can troubleshoot a device only if it is in this state.</p> <p>Note Cisco Prime Collaboration Assurance supports third-party devices whose manageability depends on MIB-II support.</p> <p>If the Cisco Prime Collaboration Assurance inventory exceeds your device limit, you will see a warning message. For information on how many devices Cisco Prime Collaboration Assurance can manage, see the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide.</p>
Partially Managed	Devices which are in managed state but have some credentials missing. These credentials are not mandatory for managing inventory, but required for all other features, such as conference monitoring to work. You can click on the corresponding number to cross launch to see a list of all devices in the inventory table which are managed but with insufficient credentials. This count is updated only when you perform rediscovery after adding the credentials.
Suspended	User has suspended monitoring of the device. Conference and endpoint data are not displayed for devices in this state. Periodic polling is also not performed for devices in this state. You cannot update inventory for these devices. To do so, you will need to perform Resume Management.

**Note**

When an unknown endpoint is moved to registered state within a cluster, the Endpoint Diagnostics page displays dual entries of the same endpoint (both unknown and registered status) till midnight. You can view the single entry of the endpoint with registered status only after nightly cluster discovery.

Related Topics

[Manage Device Credentials](#)

[Add a Device Credentials Profile](#), on page 86

[Credential Profiles Field Descriptions](#)

[Suspend and Resume Managed Devices](#), on page 178

Removal of Devices from Cisco Prime Collaboration Assurance on Deletion

None of the devices and its associated Endpoints are retained in the database when the **State** is **Deleted**.

The table below lists the devices along with its associated devices to be deleted:

Devices	Associated Devices to be Deleted
CUCM Deletion: 1. Publisher 2. Subscriber	Following are the associated devices: 1. Delete everything associated with cluster. 2. Delete subscriber along with Endpoints registered to it.
CME Deletion	Delete CME along with endpoints registered to it.
VCS Deletion	Delete all Endpoints registered to it.
TMS Deletion	Only TMS is deleted, other associated devices like MCU, TP_Conductor, etc. are not deleted.
ESX Deletion	Delete all hosted VMs nodes.
VCENTER Deletion	Delete all ESX Devices and associated nodes managed by VCENTER.
TPS, UNITY CONNECTION, MULTIPOINT CONTROLLER, IM&P and other infrastructure devices deletion	Only the devices will be deleted.

Discovery Methods

Choose one of the following discovery methods to manage devices in Cisco Prime Collaboration Assurance:

For Cisco Prime Collaboration Release 11.1 and earlier

Discovery Type	Discovery Method	Description
Auto discovery	Logical Discovery	<ul style="list-style-type: none"> • Discovers management applications, conferencing devices, and call processors such as Cisco TMS, Cisco VCS, and Cisco Unified CM. • All endpoints and infrastructure devices registered with , Cisco TMS, Cisco Unified CM, and Cisco VCS are discovered automatically during logical discovery. <ul style="list-style-type: none"> • For Cisco C and Ex series TelePresence systems, Cisco Prime Collaboration Assurance does not discover the first hop router and switch. • Logical discovery of Cisco TMS discovers VCS, codec, Cisco MCU, TPS, Cisco IP Video Phone E20, and Cisco MXP Series. • Logical discovery of the Cisco Unified CM publisher discovers other Cisco Unified CMs (subscribers) in the network, Cisco Unity, Cisco MGCP Voice Gateways, H.323 Voice Gateways, Gatekeepers, CTI applications. • Cisco Unified CM logical discovery for SIP devices includes the discovery of Conductor. The SIP configured conductor IP is not SNMP enabled, so it is not managed in Cisco Prime Collaboration Assurance. In such configuration, Conductor with admin IP must be managed first, before performing the logical discovery of Cisco Unified CM. • Endpoints and infrastructure devices that are not registered with any of the management applications, conferencing devices, or call processors cannot be discovered using logical discovery. Use ping sweep or direct discovery to discover these devices. • Cisco CTX cluster is discovered using logical discovery. • Unified Contact Center devices are discovered using logical discovery. • Logical Discovery rediscovers the deleted devices, if they are logically associated to seed devices or clusters.
Auto discovery	CDP	<ul style="list-style-type: none"> • Discovers devices independently of media and protocol used. This protocol runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. • This discovery method queries the CDP Neighbor Table to find neighboring devices. When CDP is enabled, discovery queries the CDP cache on each seed device (and its peers) via SNMP. After CDP discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by CDP discovery, then all endpoints and infrastructure devices registered with it are also discovered. • CDP must be enabled on the devices to perform CDP discovery. • There is no limit on the number of seed devices that can be used for CDP discovery. However, for a large network, it is advised to perform this on limited chunks of seed devices rather than all at once.

Discovery Type	Discovery Method	Description
Auto discovery	Ping Sweep	<ul style="list-style-type: none"> • Discovers devices within a range of IP addresses from a specified combination of IP address and subnet mask. • This method pings each IP address in the range to check the reachability of devices. If a device is reachable, you must specify a list of subnets and network masks to be pinged. After ping sweep discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by ping sweep discovery, then all endpoints and infrastructure devices registered with it are also discovered. • If no call processors are deployed, or if no devices are registered to call processors, use ping sweep discovery. This method discovers all new infrastructure devices, new network devices, and new locations of devices in the target network. You must provide a list of subnet and network masks of the target network. During a scheduled ping sweep discovery, all devices in the network are identified and matched with their credential profiles. If a new device is discovered, it is added to the inventory. • Ping Sweep discovery does not require seed devices. Instead, you must specify a list of subnets and network masks to be pinged. • Ping Sweep discovery may take longer than usual to discover devices if the IP ranges are large. • You must create an “Any” credential profile for ping sweep and CDP discovery. • Ping Sweep does not work for devices with IPv6 addresses.
-	Add Devices	<ul style="list-style-type: none"> • Discovers the device directly using the IP address. • Discovers individual devices in your network. • If the discovery of a device fails because of incorrect credentials during a scheduled discovery, then you can discover the failed device alone using the direct discovery method. • SIP devices and Presence server cannot be discovered using logical discovery. You must add these devices manually, or perform direct discovery. • To discover the seed or publisher devices without discovering the network devices or video endpoints registered to them. • To discover infrastructure devices, which have not been discovered after a fresh installation. • For MSP mode - To discover a single device without auto discovery of network devices.

Discovery Type	Discovery Method	Description
-	Import	Use this option to add: <ul style="list-style-type: none">• Devices in bulk.• A subset of devices, within a subnet, from a larger group.

**Note**

- If you plan to discover endpoints individually using any one of these methods - CDP, Ping Sweep, Add, or Import, you must ensure that the appropriate Unified CM or Cisco VCS with which the endpoint is registered is rediscovered. The endpoints must be associated with the call controller.
- For MSP mode - To discover a single device without auto discovery of network devices use either Add devices or Import option.

For Cisco Prime Collaboration Release 11.5 and later

Discovery Type	Discover	Description
Auto discovery	Communications Manager (UCM) Cluster and connected devices	<ul style="list-style-type: none"> Performs logical discovery of Cisco Unified CM by using the Inventory > Inventory Management > Auto Discovery path. All endpoints and infrastructure devices registered with Cisco Unified CM are discovered automatically during the discovery. Endpoints and infrastructure devices that are not registered with any call processors cannot be discovered using logical discovery. Use ping sweep or direct discovery to discover these devices. Communications Manager and its connected devices discovery rediscovers the deleted devices, if they are associated to seed devices or clusters. Logical discovery of the Cisco Unified CM publisher discovers other Cisco Unified CMs (subscribers) in the network, Cisco MGCP Voice Gateways, H.323 Voice Gateways, Gatekeepers, CTI applications. Cisco Unified CM logical discovery for SIP devices includes the discovery of Conductor. The SIP configured conductor IP is not SNMP enabled, so it is not managed in Cisco Prime Collaboration Assurance. In such configuration, Conductor with administrator IP must be managed first, before performing the logical discovery of Cisco Unified CM. During CUCM logical discovery (Communications Manager Publisher) no SIP trunks are discovered. In the MSP mode, if you are changing the customer name for publisher then update all other Infrastructure devices under that cluster with the new customer name. When you autodiscover Unified Communications Manager (Inventory > Inventory Management > Auto Discovery), you can choose to add Cisco Prime Collaboration Assurance server as a CDR billing application server and syslog receiver in Unified Communications Manager servers by using the Auto-Configuration option.
	Video Communications Server (VCS) / Expressway Cluster and connected devices	Performs logical discovery of Video Communications Server (VCS) or Expressway Cluster and connected devices.
	Telepresence Management Suite (TMS) and connected devices	<p>Performs logical discovery of Telepresence Management Suite (TMS) and connected devices.</p> <p>Logical discovery of Cisco TMS discovers , Cisco MCU, TPS, and TP conductor.</p>

Discovery Type	Discover	Description
	Contact Center Customer Voice Portal (CVP) and connected devices	Performs logical discovery of Contact Center Customer Voice Portal (CVP) and connected devices.
	VCenter and connected ESXi devices	Performs logical discovery of VCenter and connected ESXi devices. For Cisco C and EX Series TelePresence systems, Cisco Prime Collaboration Assurance does not discover the first hop router and switch.
	UCS Manager	Performs logical discovery of UCS Manager.
Auto discovery	Network devices using CDP	<ul style="list-style-type: none"> • Discovers devices independently of media and protocol used. This protocol runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. • This discovery method queries the CDP Neighbor Table to find neighboring devices. When CDP is enabled, discovery queries the CDP cache on each seed device (and its peers) by using SNMP. After CDP discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by CDP discovery, then all endpoints and infrastructure devices registered with it are also discovered. • CDP must be enabled on the devices to perform CDP discovery. • There is no limit on the number of seed devices that can be used for CDP discovery. However, for a large network, it is advised to perform this on limited chunks of seed devices rather than all at once.

Discovery Type	Discover	Description
Auto discovery	Network devices using Ping	<ul style="list-style-type: none"> • Discovers devices within a range of IP addresses from a specified combination of IP address and subnet mask. • This method pings each IP address in the range to check the availability of devices. If a device is reachable, you must specify a list of subnets and network masks to be pinged. After ping sweep discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by ping sweep discovery, then all endpoints and infrastructure devices registered with it are also discovered. • If no call processors are deployed, or if no devices are registered to call processors, use ping sweep discovery. This method discovers all new infrastructure devices, new network devices, and new locations of devices in the target network. You must provide a list of subnet and network masks of the target network. During a scheduled ping sweep discovery, all devices in the network are identified and matched with their credential profiles. If a new device is discovered, it is added to the inventory. • Ping Sweep discovery does not require seed devices. Instead, you must specify a list of subnets and network masks to be pinged. • Ping Sweep discovery may take longer than usual to discover devices if the IP ranges are large. • You must create an “Any” credential profile for ping sweep and CDP discovery. • Ping Sweep does not work for devices with IPv6 addresses.
Auto discovery	Any Device	Discovers any other seed devices such as conductors.

Discovery Type	Discover	Description
-	Add Devices	<ul style="list-style-type: none"> • Discovers the device directly using the IP address. • Discovers individual devices in your network. • If the discovery of a device fails because of incorrect credentials during a scheduled discovery, then you can discover the failed device alone using the direct discovery method. • SIP devices and Presence server cannot be discovered using logical discovery. You must add these devices manually, or perform direct discovery. • To discover the seed or publisher devices without discovering the network devices or video endpoints registered to them. • To discover infrastructure devices, which have not been discovered after a fresh installation. • For MSP mode - To discover a single device without auto discovery of network devices.
-	Import	<p>Use this option to add:</p> <ul style="list-style-type: none"> • Devices in bulk. • A subset of devices, within a subnet, from a larger group.



Note Endpoints and infrastructure devices that are not registered with any of the management applications, conferencing devices, or call processors cannot be discovered using logical discovery. Use ping sweep or direct discovery to discover these devices.

Prerequisites and Recommendations

Before performing the discovery, you must review the following and configure the devices as required:

All devices

- If DNS is configured on a device, ensure that Cisco Prime Collaboration Assurance can resolve the DNS name for that device. Check the DNS Server configuration to make sure it is correct. This is critical for Cisco Unified CM, Unified Presence Server, Unity Connection devices. Cisco Prime Collaboration Assurance needs to resolve the hostnames for MGCP gateways. This is because, the MGCP gateway hostnames are not added to the DNS server generally as the gateways and Cisco Unified CM are capable of operating together without DNS resolution. However, the Cisco Unified CM does not resolve the hostnames for MGCP gateways, considering it as an FQDN.
- Publisher name and the Hostname must be same (case-sensitive).
- CDP must be enabled on all CTMS, and network devices (routers and switches). For more information, see [Configuring Cisco Discovery Protocol on Cisco Routers and Switches Running Cisco IOS](#).

- You can discover the devices, such as endpoints, TelePresence server, and so on individually, except for IP Phones/Software Clients. These endpoints are discovered only with the discovery of the call processor with which they are registered.
- You must ensure that the device credentials that you have entered are correct. During the discovery process, based on the device that you want to discover, Cisco Prime Collaboration Assurance connects to the device using CLI, HTTP/HTTPS, or SNMP.
- When you add devices, the HTTP (and HTTPS) port numbers are optional. These settings are automatically detected.
- If you have both voice and video endpoints deployed in your network, do not discover all clusters in your network at the same time, as discovery could take a long time.
- Firewall devices are not supported.
- If HTTP is used to retrieve device details, disable the HTTP firewall.
- HSRP-enabled devices are not supported.
- When you add devices that have multiple interfaces and HTTP administrative access, you must manage the devices in Cisco Prime Collaboration Assurance using the same interface on which you have enabled HTTP administrative access.
- After discovering devices, if the IP address changes for network devices and infrastructure devices (such as CTMS, Cisco Unified CM, Cisco MCU, Cisco VCS, Cisco TS, and so on), you must rediscover these devices by providing the new IP address or hostname. See [Rediscover Devices, on page 135](#) for information on rediscovering devices.
- If a managed device is removed from the network, it will continue to be in the Managed state until the next inventory collection occurs, even though the device is unreachable. If a device is unreachable, an Unreachable event for this device appears.
- Configuration changes on a device are discovered by Cisco Prime Collaboration Assurance only during the inventory collection process. Therefore, any changes to a device's configuration will not be shown by Cisco Prime Collaboration Assurance until the next inventory collection after the configuration change.
- To periodically update inventory, and synchronize the inventory with the Cisco Prime Collaboration Assurance database, you must perform inventory update. For more information, see [Update and Collect Inventory Details](#).

Cisco Unified CM

- Cisco Prime Collaboration Assurance supports Unified Communications Manager cluster discovery. The Cluster IDs must be unique.
- The Access Control List (ACL) in Unified Communications Manager must contain all endpoints to be managed. If the Unified Communications Manager SNMP user configuration includes the ACL, all Unified Communications Manager nodes in the cluster must contain the Cisco Prime Collaboration Assurance server IP address.
- Cisco Prime Collaboration Assurance must discover and manage only the Unified Communications Manager publisher to manage a cluster. Subscribers are not discovered directly; they are discovered through the publisher. Cisco Prime Collaboration Assurance must manage the publisher to monitor a cluster. The Computer Telephony Integration (CTI) service must be running on all subscribers. You must ensure that the access control list in Unified Communications Manager contains all endpoints that need

to be managed. If the Unified Communications Manager SNMP user configuration includes the use of the Access Control List, you must enter the Unified Communications Manager server IP address on all Unified Communications Manager nodes in the cluster.

- You must provide the credential profile of ELM or PLM device type with the right IP address pattern in Cisco Prime Collaboration Assurance, so that the configured ELM or PLM gets discovered and managed when a Unified Communications Manager publisher is added to Cisco Prime Collaboration Assurance using auto discovery User Interface.

When you autodiscover Unified Communications Manager publisher in Cisco Prime Collaboration Assurance (**Inventory > Inventory Management > Auto Discovery**), you can choose to autoconfigure syslog receiver and CDR billing application server in Unified Communications Manager by using the Auto-Configuration option. You can uncheck the check boxes under Auto-Configuration option, if you want to configure syslog receiver and CDR billing application server manually. We recommend you to check whether a slot is available in Unified Communications Manager to manually add syslog receiver or CDR billing application server entry.



Note You can automatically configure syslog receiver and CDR billing application server only when Unified Communications Manager is in managed state in Cisco Prime Collaboration Assurance.

You can view PLM as a separate group under Cisco Unified Communications (UC) applications.

- The JTAPI credential is optional for Cisco Unified CM clusters. However, the SNMP and HTTP credentials are mandatory for Cisco Unified CM publishers and subscribers.
- After discovering Cisco Unified CM, if you have registered any new endpoints, you must rediscovers Unified CM Publisher node to add them to Cisco Prime Collaboration Assurance. See [Rediscover Devices, on page 135](#) for information on rediscovering devices.



Note We recommend that you should not add a subscribe node manually.

For Cisco Prime Collaboration Release 11.5 and earlier

In MSP mode, if you have registered any new endpoints before discovering Cisco Unified CM, you must delete the endpoints and add them again after discovering Cisco Unified CM.

Cisco Unified CM Express and Cisco Unity Express

- For discovery of Cisco Cius and Cisco Unified IP Phone 8900 and 9900 Series, you must enable the HTTP interface so these devices appear in the inventory table. See the “Enabling and Disabling Web Page Access” section in the [Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1 \(3\) \(SIP\)](#) for more information.
- To enable Cisco Prime Collaboration Assurance to provide the correct phone count for the Cisco Unified CM Express and Cisco Unity Express (CUE), you must use the following configuration:

```
ephone 8
mac-address 001A.E2BC.3EFB
type 7945
```

where type is equal to the phone model type. If you are unsure of your model type, see Cisco.com for details on all phone model types, or enter type?. For information on how phone counts are displayed, see the Device Management Summary window in the Inventory Management page.

- If a UC500 Series router is running Cisco Unified CM Express, you must configure "type" under ephone config for each phone so that the cmeEphoneModel MIB variable of CISCO-CME_MIB will return the correct phone model. This enables Cisco Prime Collaboration Assurance to discover the phones registered with Cisco Unified CM Express.
- For a Cisco Unity Express that is attached to a Cisco Unified CM Express to display in the Service Level View, you must use the following configuration:

```
dial-peer voice 2999 voip <where voip tag 2999 must be different from voicemail>
destination-pattern 2105 <prefix must be the full E.164 of configured voicemail
2105>
conference protocol sipv2
conference target ipv4:10.10.1.121
dtmf-relay sip-notify
codec g711ulaw
no vad
!
!
telephony-service
voicemail 2105
```

where the dial-peer VoIP tag, 2999, is not equal to the voice mail number, and the destination-pattern tag, 2105, is equal to the voice mail number. This will allow Unity Express to display properly in the Service Level View.

Cisco VCS and Cisco VCS Expressway

- You can discover Cisco VCS clusters. Cluster names must be unique, and all endpoints that Cisco Prime Collaboration Assurance should manage must be registered in the Cisco VCS. During VCS discovery, the endpoints registered to it are also discovered. All the VCSs in a cluster need to be in managed state so that all related features work, for example conference monitoring may not work and affect CDR creation.



Note Even if one VCS in a cluster is not in a managed state, there will be inconsistencies in data reporting.

- After discovering Cisco VCS, the newly registered endpoints are automatically discovered. Also, if there any changes in the endpoint IP address, Cisco Prime Collaboration Assurance detects the IP address change automatically.
- If the Cisco VCS Expressway is configured within the DMZ, Cisco Prime Collaboration Assurance must be able to access the Cisco VCS Expressway through SNMP. If it cannot, then this device is moved to the Inaccessible state. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
 - [Configure Devices for Cisco Prime Collaboration Assurance](#)

For Cisco Prime Collaboration Release 11.1 and earlier

CTS-Manager

- If you have installed a licensed version of Cisco Prime Collaboration Assurance, it is mandatory to configure the CTS-Manager Reporting API. If this feature is not configured on the CTS-Manager 1.7, 1.8, or 1.9, Cisco Prime Collaboration Assurance will not manage the CTS-Manager. See [Cisco TelePresence Manager Reporting API Developer's Guide](#) for more information.
- Cisco Prime Collaboration Assurance cannot manage two standalone CTS-Manager. If you are using more than one CTS-Manager, you must configure in a cluster for the Cisco Prime Collaboration Assurance application to manage. Before performing the discovery, enter the Primary Server IP address and hot standby or secondary server details in **Device Inventory > Inventory Management > Manage CTS-MAN/TMS/CTX Clusters**.

For Cisco Prime Collaboration Release 11.1 and earlier

CTX Cluster

- Cisco Prime Collaboration Assurance supports Cisco TelePresence Exchange (CTX) clusters only in Managed Service Provider (MSP) mode. Cluster names must be unique. Each CTX cluster must nominate one server as a primary admin server and another as a secondary server. Cisco Prime Collaboration Assurance must discover and manage the primary and secondary admin server to manage a cluster. The database servers and call engine servers are automatically discovered.
- API user and SNMP credentials are mandatory for admin nodes. For call engine and database nodes, only SNMP credentials are required. For more information, see [Setting Up Devices for Cisco Prime Collaboration Assurance](#).
- Before performing the discovery, enter the IP address of the primary and secondary admin server details in .

Cisco TelePresence Conductor

Cisco Prime Collaboration Assurance supports Cisco TelePresence Conductor XC, version 1.2 to version 3.0.1, in the standalone model. The cluster model is not supported.

Auto Discovery of Cisco TelePresence Management Suite (TMS) also discovers the Cisco TelePresence Conductor.

Cisco TelePresence Conductor support is available only in Enterprise mode of Cisco Prime Collaboration Assurance server.

Media Server

If Cisco Discovery Protocol (CDP) is not enabled on a media server (it is either disabled or not responding), Cisco Prime Collaboration Assurance does not discover the device correctly and the device is moved to the Unsupported state.

Mobile and Remote Access (MRA) Clients

The Mobile Remote Access (MRA) clients (such as Cisco Jabber, Cisco TelePresence MX Series, Cisco TelePresence System EX Series, and Cisco TelePresence System SX Series) are discovered as part of the Cisco Unified Communications Manager discovery only.

For MRA to be discovered correctly, the Cisco VCS with Cisco Expressway Core capability must be in Managed state in Cisco Prime Collaboration Assurance. If the Cisco VCS with Cisco Expressway Core capability is not in Managed state, and Cisco Unified Communications Manager is discovered directly, then the MRA clients appear with duplicate IP address (same as that of the Cisco VCS with Cisco Expressway Core capability) in Inventory Management.

TP MRA Endpoints will not be discovered (shown in Inventory) if VCS Core is not managed in Cisco Prime Collaboration Assurance.

Cisco Unified Contact Center Enterprise (Unified CCE) and Packaged Contact Center Enterprise (PCCE)

- Cisco Prime Collaboration Assurance supports Unified CCE and PCCE device discovery by using Simple Network Management Protocol (SNMP) feature. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
 - [Configure Devices for Cisco Prime Collaboration Assurance](#)
- You must install Microsoft Windows SNMP components on Unified ICM/CCE servers for any SNMP agent to function. The Microsoft Windows SNMP service is disabled as part of web setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests.
- You can configure Cisco SNMP Agent Management settings using a Windows Management Console Snap-in.
- Cisco Prime Collaboration Assurance displays authentication errors and incorrect device information if you enter special characters in the **System Description** field under SNMP Agent Management Snap-in window. The description cannot include hyphen (-), double quotes ("), asterisk (*), octothorpe (#), dollar (\$), underscore (_), percentage sign (%), double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([]).

Cisco Unified Contact Center Express (Unified CCX)

You must configure SNMP. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:

- [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
- [Configure Devices for Cisco Prime Collaboration Assurance](#)

Cisco SocialMiner

You must configure SNMP. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:

- [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
- [Configure Devices for Cisco Prime Collaboration Assurance](#)

Cisco Integrated Management Controller (CIMC)

- Cisco Prime Collaboration Assurance generates traps for alarms and events of CIMC device and sends notifications to the trap receiver. The traps are converted into SNMPv1c notifications and are formatted according to the CISCO-UNIFIED-COMPUTING-MIB.
- The system cannot auto-discover a CIMC device. You must manually add the device by using the **Add Device** button under **Device Inventory > Inventory Management**.
- **For Cisco Prime Collaboration Release 11.5 and later**
The system cannot auto-discover a CIMC device. You must manually add the device by using the **Add Device** button under **Inventory > Inventory Management**.

- You must configure the SNMP. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
 - [Configure Devices for Cisco Prime Collaboration Assurance](#)
- The CIMC device will be in managed state only when you enter the correct IP address and SNMP credentials.

For Cisco Prime Collaboration Release 11.5 and later

Cisco Unified Attendant Console

The system supports Cisco Unified Attendant Console as a third-party Windows device. You must configure SNMP to support Cisco Unified Attendant Console in Cisco Prime Collaboration Assurance. For more information, see [Configure Devices for Cisco Prime Collaboration Assurance](#).

For Cisco Prime Collaboration Release 11.6 and later

ciscoDX70 and ciscoDX80 with CE image

The system supports ciscoDX70 and ciscoDX80 devices with CE image. ciscoDX70 and ciscoDX80 devices act similar to Cisco TelePresence devices. You must register DX Series devices to Cisco Unified Call Manager (UCM) to discover ciscoDX70 and ciscoDX80 devices in Cisco Prime Collaboration Assurance. You must configure SNMP, HTTP, and CLI to support ciscoDX70 and ciscoDX80 devices in Cisco Prime Collaboration Assurance. For more information, see [Configure Devices for Cisco Prime Collaboration Assurance](#).

**Note**

Cisco Prime Collaboration Assurance does not support CMR reports and Endpoint diagnostic feature for ciscoDX70 and ciscoDX80 devices with CE image.

Automatic Discovery of Devices

You can discover seed or publisher devices with endpoints and subscriber devices registered to them.

**Note**

- A discovery job, once started, cannot be stopped or cancelled.
- You cannot run both Ping Sweep and CDP discovery simultaneously in your network.

To discover clusters using logical discovery, you must discover the publisher of the cluster, which will automatically discover its subscribers and all the endpoints and infrastructure devices registered with both publisher and subscribers.

If the IP address of a DHCP-enabled endpoint registered with Cisco Unified CM, Cisco Prime Collaboration Assurance may not be able to automatically discover this endpoint. This is applicable to all Cisco TelePresence systems registered with Cisco Unified CM.

For Cisco Prime Collaboration Release 12.1 SP2 and later

The TelePresence endpoint discovery (TC/CE) uses slot2 as a dedicated slot to receive HTTPS feedbacks. As part of any rediscovery, Cisco Prime Collaboration Assurance has to unsubscribe and subscribe it again. Subscribe for the TC/CE HTTPS feedback only when the endpoint is in Managed State and Registered.

When a Unified Communications Manager publisher is added to Cisco Prime Collaboration Assurance using auto discovery User Interface, the configured ELM or PLM also gets discovered and managed. This is possible only if Cisco Prime Collaboration Assurance has the credential profile with ELM or PLM device type and right IP address pattern.

For Cisco Prime Collaboration Release 11.5 and later

Auto Discovery only works in a non-NAT environment. In a NAT environment, to have the seed device and endpoint or subscriber association, perform a rediscovery of the seed device and select the **Enable Logical Discovery** button.

Auto Discovery *only* works in a non-MSP deployment. In MSP deployment, to associate devices (such as endpoint, subscriber, gateway) to a cluster, all the associated devices must be managed in Cisco Prime Collaboration Assurance and then rediscover the publisher CUCM for a cluster.

To discover Unified Contact Center devices, you must enter the CVP - OAMP server as the seed device for the task.

To auto discover devices:

Before you begin

You must review the following sections before performing auto discovery:

- Managing Device Credentials: The required credentials must be entered before performing discovery.
- Discovery Methods: Based on your deployment, select the appropriate discovery methods.
- Prerequisites and Recommendation: Configure the required settings on the devices and review the recommendations.
- Setting up Clusters: If you are managing multiple Cisco TMS or CTX clusters, you need to enter specific application details.

Step 1 Choose **Inventory > Inventory Management**.

For Cisco Prime Collaboration Release 11.1 and earlier

Choose **Device Inventory > Inventory Management**.

Step 2 In the Inventory Management page, click **Auto Discovery**.

Step 3 Enter the job name, and check the **Check Device Accessibility** check box.

Step 4 Select a discovery method. For information on the best discovery option to use, see [Prerequisites and Recommendations](#).

Note **For Cisco Prime Collaboration Release 11.5 and later**

If you select “Communications Manager (UCM) Cluster and connected devices” from the **Discover** drop-down list, you get an additional Auto-Configuration option described in steps 7 and 8.

Step 5 Enter the IP address or hostname of the device. For various discovery protocols, enter the following:

Example:

- For Logical Discovery, Cisco Discovery Protocol and Direct Discovery, you can enter multiple IP addresses or hostnames using one of the supported delimiters: comma, colon, pipe, or blank space.
- **For Cisco Prime Collaboration Release 11.5 and later**
For Communications Manager (UCM) Cluster and connected devices, Video Communications Server (VCS) / Expressway Cluster and connected devices, Telepresence Management Suite (TMS) and connected devices, Contact Center Customer Voice Portal (CVP) and connected devices, VCenter and connected ESXi devices, and UCS Manager Discovery, Network devices using CDP Discovery, and Direct Discovery, you can enter multiple IP addresses or hostnames using one of the supported delimiters: comma, colon, pipe, or blank space.
- For Network devices using Ping/Sweep Discovery, specify a comma-separated list of IP address ranges using the /netmask specification. For example, use 172.20.57.1/24 to specify a ping sweep range starting from 172.20.57.1 and ending at 172.20.57.255.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can select the customer for which you want to discover the device. In a non-Nat environment, the Public IP (managed IP) is populated with the discovered IP Address, and the Private IP is populated as Public IP (managed IP) by default. If you have deployed Cisco Prime Collaboration Assurance in Enterprise mode, you can select the **Assurance Domain** for which you want to discover the device. All the endpoints discovered through auto discovery are associated with the same **Assurance Domain** selected for the seed device.

For Cisco Prime Collaboration Release 11.5 and later

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can select the customer for which you want to discover the device. In a non-Nat environment, the Public IP (managed IP) is populated with the discovered IP Address, and the Private IP is populated as Public IP (managed IP) by default. If you have deployed Cisco Prime Collaboration Assurance in Enterprise mode, you can select the **Associate to Domain** option for which you want to discover the device. All the endpoints discovered through auto discovery are associated with the same **Associate to Domain** selected for the seed device.

Step 6 (Optional) Enter the Filter and Advanced Filter details (available only for logical, CDP and ping sweep discovery methods). You can use a wildcard to enter the IP address and DNS information that you may want to include or exclude. See [Discovery Filters and Scheduling Options](#) for field descriptions.

Step 7 (Optional) If you have selected “Communications Manager (UCM) Cluster and connected devices” from the **Discover** drop-down list in [Step 4](#), you must uncheck the **Add the Prime Collaboration Server as a CDR Destination in the Unified CM Servers** check box from the Auto-Configuration pane if you do not want to enable automatic configuration of CDR billing server on Unified Communications Manager servers.

Note As part of the automatic configuration of CDR billing server, Cisco Prime Collaboration Assurance enables the CDR and CMR flags on both publishers and subscribers of Unified Communications Manager. However Cisco Prime Collaboration Assurance performs automatic configuration of CDR billing server only on managed Unified Communications Manager publishers.

Step 8 **(For Cisco Prime Collaboration Release 11.5 and later)** (Optional) If you have selected “Communications Manager (UCM) Cluster and connected devices” from the **Discover** drop-down list in [Step 4](#), you must uncheck the **Add the Prime Collaboration Server as a Syslog Destination in the Unified CM Servers** check box from the Auto-Configuration pane if you do not want to enable automatic configuration of syslog receiver on Unified Communications Manager servers.

Note Cisco Prime Collaboration Assurance performs automatic configuration of syslog receiver on managed Unified Communications Manager publishers as well as subscribers. Unified Communications Manager updates the alarm and event level to “Informational” for all configured syslog receivers.

Step 9 Schedule a periodic discovery job (see [Discovery Filters and Scheduling Options](#) for field descriptions) or run the discovery job immediately by following [Step 10](#).

Step 10 Click **Run Now** to immediately run the discovery job, or click **Schedule** to schedule a periodic discovery job to run at a later time. If you have scheduled a discovery, a notification appears after the job is created. You can click Job Progress to view the job status on the job management page. Or, if you have run the discovery immediately, you can click Device Status Summary hyperlink to know the current state of the device being discovered.

- Note**
- If you remove a particular Unified Communications Manager node, Cisco Prime Collaboration Assurance also removes the syslog or CDR configuration of its own IP address of the node. The other syslog or CDR configuration changes are not affected on the device.
 - If automatic configuration or manual configuration of CDR billing server or syslog receiver is not available in Unified Communications Manager publisher or any of its subscribers, the system displays the **Status Reason** of the device as “Partially Managed” along with the reason (for example, "Syslog Configuration is missing on the device"). However, the device remains in the “Managed” state in Cisco Prime Collaboration Assurance.

Troubleshooting

a. Issue: Cisco Prime Collaboration Assurance is not added as a CDR application billing server in the device.

Recommended Action:

- Ensure that Unified Communications Manager publisher is added in Cisco Prime Collaboration Assurance by using the “Auto Discovery” option.
- Ensure that the device is in managed state after you discover the inventory. Also, the device should appear as a Call Quality Data Source under **Alarm & Report Administration > CDR Source Settings**.
- In the Unified Communications Manager Administration page, select the Serviceability page and navigate to CDR Management page. Ensure that at least one slot of CDR Billing Server is available so that automatic configuration can occur.

b. Issue: Cisco Prime Collaboration Assurance is not added as a Remote Syslog receiver in the device.

Recommended Action:

- Ensure that Unified Communications Manager publisher is added in Cisco Prime Collaboration Assurance by using the “Auto Discovery” option.
- Ensure that the device is in managed state after you discover the inventory.
- In the Unified Communications Manager Administration page, select the Serviceability page and navigate to **Alarm > Configuration**. Ensure that at least one slot of Syslog Receiver is available so that automatic configuration can occur.

c. Issue: TMS discovery does not discover all connected devices.

Recommended Action:

From Cisco Prime Collaboration Provisioning Assurance 12.1 onwards, TMS discovery does not automatically discover the CUCM, VCS, and endpoints managed in the TMS.

Discovery Filters and Scheduling Options

Discovery Filters

The following table describes the filters that are available when you run discovery.

Table 20: Discovery Filters

Filter	Description
IP Address	<p>Comma-separated IP addresses or IP address ranges for included or excluded devices. For the octet range 1-255, use an asterisk (*) wildcard, or constrain using [xxx-yyy] notation; for example:</p> <ul style="list-style-type: none"> To include all devices in the 172.20.57/24 subnet, enter an include filter of 172.20.57.*. To exclude devices in the IP address range of 172.20.57.224 to 172.20.57.255, enter an exclude filter of 172.20.57.[224-255]. <p>You can use both wildcard types in the same range; for example, 172.20.[55-57].*.</p> <p>If both include and exclude filters are specified, the exclude filter is applied before the include filter. After a filter is applied to an auto-discovered device, no other filter criterion is applied to the device. If a device has multiple IP addresses, the device is processed for auto-discovery as long as it has one IP address that satisfies the include filter.</p>
Advanced Filters	
DNS Domain	<p>Comma-separated DNS domain names for included or excluded devices.</p> <p>An asterisk (*) wildcard matches, up to an arbitrary length, any combination of alphanumeric characters, hyphen (-), and underscore (_).</p> <p>A question mark (?) wildcard matches a single alphanumeric character, hyphen (-), or underscore (_).</p> <p>For example, *.cisco.com matches any DNS name ending with .cisco.com. and *.?abc.com matches any DNS name ending with .aabc.com, .babc.com, and so on.</p>

Filter	Description
Sys Location	<p>Available only for CDP and ping sweep discovery methods) Comma-separated strings that match the string value stored in the sysLocation OID in MIB-II, for included or excluded devices.</p> <p>An asterisk (*) wildcard matches, up to an arbitrary length, any combination of alphanumeric characters, hyphen (-), underscore (_), and white space (spaces and tabs). For example, a SysLocation filter of San * matches all SysLocation strings starting with San Francisco, San Jose, and so on.</p> <p>A question mark (?) wildcard matches a single alphanumeric character, hyphen (-), underscore (_), or white space (space or tab).</p>

Schedule Options

The following table describes the scheduling options that are available

Table 21: Schedule Options

Field	Descriptions
Start Time	<p>Click Start Time to enter the start date and time in the yyyy/MM/dd and hh:mm AM/PM formats, respectively.</p> <p>Click the date picker if you want to select the start date and time from the calendar. The time displayed is the client browser time. The scheduled periodic job runs at this specified time.</p>
Recurrence	Click None, Hourly, Daily, Weekly, or Monthly to specify the job period.
Settings	Specify the details of the job period.
End Time	If you do not want to specify an end date/time, click No End Date/Time. Click Every number of Times to set the number of times you want the job to end in the specified period. Enter the end date and time in the yyyy/MM/dd and hh:mm AM/PM formats, respectively.

Manual Discovery of Devices

You can add single or multiple devices to Cisco Prime Collaboration Assurance manually by using the Add Device option in the Inventory Management page.

To add a new device and perform discovery:

Before you begin

You must review the following sections before adding devices:

- Managing Device Credentials: The required credentials must be entered before performing discovery.
- Discovery Methods: Based on your deployment, select the appropriate discovery methods.
- Prerequisites and Recommendation: Configure the required settings on the devices and review the recommendations.

Step 1 Choose **Device Inventory > Inventory Management**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**.

Step 2 In the Inventory Management page, click **Add Device**.

Step 3 In the Add Device window, enter the necessary information. For information regarding different credentials, see the [Credential Profiles Field Descriptions](#).

Based on your deployment, you can select either the Customer or Associate to Domain for which you want to add the devices in the Device Information pane:

- NAT - If the devices you want to discover are in a NAT environment, select this check box.
- Customer - You can select the customer for which you want to discover the devices.
- IP Address - Enter the Public IP address or the Managed IP. You can enter an IPv4 or IPv6 address.
- Private IP Address - Enter the Private IP address. You can enter an IPv4 or IPv6 address.
- Private Host Name - Enter the private host name.

Note If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you must provide FQDN in the Private Host Name field, while configuring endpoints registered with Unified CM or ELM.

Note You need to add devices for each customer in separate instances. You can add up to five devices for a customer in a single instance. To add more devices, click the **Add Device** button. Ensure that you delete blank rows.

Step 4 Click **Discover**. You can see the status of the discovery job in the Job Management page. The device appears in the inventory table after discovery. For more information, see [Verify Discovery Status](#).

You can also look at the Assurance Inventory Summary to know the number of discovered devices and the number of devices for which discovery is in progress.

Step 5 Click **Discover**. You can view a popup.

For Cisco Prime Collaboration Release 11.5 and later

The device discovery has started. To know the current state of the device being discovered, click **Device Status Summary** hyperlink.

Import Devices

You can import devices into Cisco Prime Collaboration Assurance, by importing a file with the device list and credentials.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, only the devices of the customers you have selected in the global customer selection field are imported.

You need to add the following for each device to import it:

- Hostname
- IP address
- Protocol credentials



Note You can add plain text credentials or encrypted credentials, but not both in the same file.

- If the devices are in a NAT environment, ensure that you add the Customer name, Private IP and Public IP address, and Private hostname of the devices.
- If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you must provide hostname as FQDN, while configuring endpoints registered with Unified CM or ELM.
- All endpoints or subscribers registered to a publisher inherit the customer name from the publisher.



Note Ensure that you modify only the device details. Modification of any other line corrupts this file and causes the import task to fail.

To import a device from a file:

Before you begin

You must review the following sections before importing devices:

- Manage Device Credentials: The required credentials to manage devices.
- Discovery Methods: Based on your deployment, select the appropriate discovery methods.
- Prerequisites and Recommendation: Configure the required settings on the devices and review the recommendations.
- Export Device Lists and Credentials: The import file format is same as export.

Step 1 Choose **Device Inventory > Inventory Management**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**.

Step 2 Click **Import**.

Warning For Cisco Prime Collaboration Release 11.5 and later

For security purposes, you can import the exported device credentials file on the same server only.

Step 3 In the Import dialog box, browse to the file with the list of devices and credentials that you want to import. (Only the CSV or XML file format is supported.) If you are importing a file with encrypted credentials, select the File contains Encrypted Credentials check box.

Step 4 Click **Import**.

Note When you perform an import-based discovery for a seed or publisher device, registration and association details of the registered endpoints such as cluster names are not populated completely. In such a case, perform the rediscovery of the seed device to get the complete registration and association details.

The status reason of imported devices is updated, when you perform the rediscovery of the device or wait for the auto discovery to discover the devices which updates the status reason.

Credential Profiles are not created for the imported list of devices and credentials. After import, device discovery is triggered automatically using the credentials available in the import file. You can check the status of the import-based discovery job on the Job Management page. See [Verify Discovery Status](#) for more information. If any of the imported device credentials are incorrect, then the device may not be in Managed state.

After discovery, the imported devices appear in the inventory. Other device details, physical information, access information are displayed in the respective panes below the inventory table. You can also look at the Device Status Summary to know the number of discovered devices and the number of devices for which discovery is in progress.

Export Device Lists and Credentials

You can export device lists, and device credentials to a file. You could use this file to modify the device list and credentials and import it later. This feature is only available to users with network administrator, super administrator, and system administrator roles.

To export device list and credentials:

Step 1 Choose **Device Inventory > Inventory Management > Export**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management > Export**

Step 2 Select **Device list and Credentials**, and enter a name for the output file. (Only CSV and XML file format is supported.)

Step 3 Click **Export**. This file contains encrypted credentials only.

For Cisco Prime Collaboration Release 11.5 and later

Warning For security purposes, you can import the exported device credentials file on the same server only.

Step 4 In the dialog box that appears, do one of the following:

- Click **Open** to review the information.
- Click **Save** to save the CSV or XML file on your local system.

Note If the devices are in a NAT environment, then the customer name, Private IP and Public IP addresses, and Private host name is also updated.

Troubleshooting

- Issue:** Devices are not getting discovered while trying to import the device credential from one server to other.
Recommendation: You can import the exported device credentials file on the same server only.
- Issue:** Devices are not getting discovered while trying to use the exported credential from the previous release to import in current release.
Recommendation: You can import the exported device credentials file on the same server only.

Discovery of Cisco Unified Computing System (UCS)

Perform the following procedure to discover Cisco UCS in a NAT deployment and ensure that the vCenter, ESX, and UCS Manager devices are added to Cisco Prime Collaboration Assurance.

Before you begin

- VMware vCenter Server (vCenter), VMware ESX Server (ESX), and Cisco UCS Manager (UCS Manager) devices must be supported in a non-NAT deployment.
- The Virtual Machines (VMs) must be powered on during discovery.



Note The newly added Virtual Machines (VMs) that are not getting discovered either through polling or rediscovery of ESXi host can be discovered through Logical Discovery.

- VMware Tools must be installed on the VMs before performing the discovery. This ensures the tools are discovered during the VMware ESX server discovery.
- In a NAT deployment, the VM name in the managed ESX server must be same as the private host name of the VM in Cisco Prime Collaboration Assurance.
- Check the Event and Alarm correlation rules with UCS blades by configuring vCenter. See [Configure vCenter, on page 132](#) for more information.
- Enable and configure SNMP on Cisco UCS Manager to create the relationship between the SNMP manager and the SNMP agent:
 - In Cisco UCS Manager, navigate to the **Admin** tab and expand it to select the **Communication Services** tab.
 - Configure the fields in the SNMP window and save the changes.

-
- Step 1** Login to Cisco Prime Collaboration Assurance server and navigate to **Device Inventory > Inventory Management**.
For Cisco Prime Collaboration Release 11.5 and later
Login to Cisco Prime Collaboration Assurance server and navigate to **Inventory > Inventory Management**.
- Step 2** Click the **Manage Credentials** button to create credential profiles for VMware ESX Server (ESX), Cisco UCS Manager (UCS Manager), and VMware vCenter Server (vCenter).
- Note**
- You must configure SNMP credentials on the VMware ESX Server. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
 - [Configure Devices for Cisco Prime Collaboration Assurance](#)
 - The HTTP credentials for the VMware ESX Server credential profile must be same as the VMware ESX Server device login credentials.
 - In a clustered scenario, the HTTP credentials for the Cisco UCS Manager credential profile must be the same as the primary Fabric Interconnect device login credentials.
 - In a standalone scenario, the HTTP credentials for the Cisco UCS Manager credential profile must be the same as the Fabric Interconnect device login credentials.
 - The HTTP credentials for the vCenter credential profile must be same as the vCenter device admin login credentials.
 - The virtual machines are supported both in a NAT and non-NAT deployment.
- Step 3** Perform logical discovery of the following:
- **ESX Logical Discovery** - Use the ESX Server IP address as the seed device to discover all the VMs running on it.
 - **UCS Manager Logical Discovery** - In a clustered scenario, use the virtual IP address of the Cisco UCS Manager as the seed IP address for logical discovery. This discovers the UCS Chassis managed by the UCS Manager, and also associates the managed ESX Server to the right UCS Chassis. In a standalone scenario, use the IP address of Fabric Interconnect device as the seed IP address for Logical Discovery.
 - **vCenter Logical Discovery** - Use the vCenter IP address as the seed device to discover the vCenter and the ESX servers managed in the vCenter server.
- Note**
- The VM name in the managed ESX server must be same as the private host name of the VM in Cisco Prime Collaboration Assurance to ensure proper grouping of the VMs.
 - Logical Discovery is not supported in MSP deployment.

To discover the Cisco UCS and one or more associated virtual machines in a non-NAT deployment, perform the following procedure:

a. For Cisco Prime Collaboration Release 11.1 and earlier

Choose **Inventory Management > Auto Discovery**, and then select **Logical Discovery** in the **Discovery Methods** drop-down list.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management > Auto Discovery**, and then select **UCS Manager** in the **Discover** drop-down list.

Perform Logical Discovery with the vCenter IP address as the seed device. This discovers the vCenter and the ESX servers managed in vCenter, and the associated Virtual Machines or Cisco Unified Communications (UC) applications of the ESX servers. The model of the ESX server shows whether the device is C Series or B Series.

b. For Cisco Prime Collaboration Release 11.1 and earlier

(Optional) Discover the ESX host separately which is not configured in vCenter. You can use the Add Device (**Inventory Management > Add Device**) or Import (**Inventory Management > Import**) feature, however you need to perform Logical Discovery to get the association between ESX and VM /UC applications.

For Cisco Prime Collaboration Release 11.5 and later

(Optional) Discover the ESX host separately which is not configured in vCenter. You can use the Add Device (**Inventory Management > Add Device**) or Import (**Inventory Management > Import**) feature, however you need to perform Logical Discovery to get the association between ESX and VM /UC applications.

c. (Optional) If you have a UCS Manager in your deployment, perform logical discovery as follows:

- In a clustered scenario, use the virtual IP address of the Cisco UCS Manager as the seed IP address.
- In a standalone scenario, use the IP address of Fabric Interconnect device as the seed IP address.

This discovers the UCS chassis. It also associates the managed ESX Server to UCS Chassis. You must discover the blades separately as the Logical discovery of the UCS Manager does not discover the blades. Perform logical discovery of UCS manager to build the Chassis and Blade association, after discovering the ESX host.

Note A combination of the UCS Manager name and UCS Chassis name is displayed instead of the IP address in Inventory Management for the UCS Chassis. This is because the UCS chassis does not have an IP address.

After successful discovery you can see groups related to Cisco UCS populated with the devices or applications in the Device Group Selector pane under the Infrastructure group.

For UCS-B Series Blade Server group you can see a list of all the managed Cisco UCS Chassis and the managed blades under each chassis. When you click on a chassis listing, you can view all the details of the managed blades of that particular chassis in the right pane and the IP address of the managed blades in the device selector under the chassis. When you click on a managed blade IP address, you can view the list of managed Virtual Machines Cisco Unified Communications (UC) applications associated with the blade on the right pane.

For the UCS-C Series Rack Server group you can see a list of all the managed ESX Servers as a node. When you click the IP address of the ESX Server, you can view all managed Virtual Machines or Cisco Unified Communications (UC) applications running on the ESX server in the right pane.

Configure vCenter

Perform the following procedure to configure SNMP, and triggers and alarms in vCenter.

Step 1 Configure SNMP in vCenter

- a) Log in to vCenter by using vSphere and navigate to **Administration > vCenter Server Settings**
- b) Select **SNMP** menu on the left of the page to configure the SNMP settings.

Step 2 Configure the triggers and alarms in vCenter

- a) Select a virtual machine and navigate to **Alarms > Definition**.
 - b) Click the vCenter name and select the alarm to configure the settings.
 - c) Navigate to **Triggers** tab and select the trigger as described in the section “Triggers for Alarms of VMware vCenter Server” in the following link:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
 - [Configure Devices for Cisco Prime Collaboration Assurance](#)
 - d) Select the state as “Alert” and click **OK**.
 - e) Click **Actions** and then select **Repeat** for all the following cases: “Normal->Warning”, “Warning->Error”, “Error->Warning”, and “Warning->Normal”.
 - f) Click **OK**.
-

Unified CM Cluster Data Discovery

After the Unified CM publisher is managed in Cisco Prime Collaboration Assurance, you must collect the additional inventory data by performing the Cluster Data Discovery. This discovery helps you to collect:

- Cluster configuration data including Redundancy group, Devicepool, Location, Region, RouteList, RouteGroup, RoutePattern, Partition, and so on. This also includes the entities provisioned in the cluster such as phones, voice mail endpoints, media resources, gateways, and trunks.
- Registration information about all the entities which register with the Unified CM cluster. This includes Device IP, Registration status, the Unified CM server to which the entity is registered currently, the latest registration or unregistration time stamp, and the status reason.

Registration information can be configured using a configuration file. This information is collected from all the subscriber nodes in the clusters to which the entities such as phones or gateways register.

Cisco Prime Collaboration Assurance collects cluster configuration from the Cisco Unified CM once a day as well as at startup. This periodic discovery data collection is done by default at midnight daily; the default schedule can be changed.



Note

- Only endpoints registered to Unified CM are discovered. The endpoints registered to Cisco VCS are discovered separately.
 - SIP devices are not discovered.
 - Cisco Prime Collaboration Assurance supports Cisco Unified CM cluster in Mixed mode. For more information on the CUCM Mixed mode, see [Cisco Unified Communications Manager Maintain and Operate Guides](#).
 - Do not associate the Standard CTI Secure Connection Access Control Group or Role with the JTAPI application user on CUCM Mixed mode configured for Cisco Prime Collaboration Assurance.
-

Schedule Cluster Device Discovery

Before you begin

The following conditions must be met before you perform Unified CM cluster discovery:

- Data is collected from Publisher or First node through AXL. Therefore, the publisher should be in fully in monitored state with proper HTTP credentials entered and the AXL Web Service should be running in the publisher.
- Cisco RIS Data Collector running in 7.x versions of Unified CM.
- Cisco SOAP - CDRonDemand Service running in other versions of Unified CM.
- If the Unified CM publisher is configured using name in the Unified CM section or System Server section of Unified CM Administration, then this name must be resolvable through DNS from the Cisco Prime Collaboration Assurance server. Otherwise, an entry must be configured for this name in the host files for the data collection to proceed further.
- For Cisco Prime Collaboration Assurance to be able to receive syslogs and process configurations required in the Unified CM, you must perform the steps in the Syslog Receivers section. Any changes in the registration information are updated through processing the relevant syslogs from Cisco Unified CM.

Syslog processing can detect the following changes of the entities registered to the Cisco Unified CM cluster:

- Any registration changes on entities such as phone, voice mail endpoint, gateways, and so on.
- Any new phones provisioned in the cluster are detected and updated to the inventory.

Other devices may also require configuring syslogs from within the device. For details on the device configurations required, see [Configure Syslog Receiver](#) section in the following link:

- [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
- [Configure Devices for Cisco Prime Collaboration Assurance](#)

Step 1 Choose **Device Inventory > Inventory Schedule > Cluster Data Discovery Schedule**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Schedule > Cluster Data Discovery Schedule**.

For Cisco Prime Collaboration Release 12.1 and later

Choose **Inventory > Cluster Device Discovery Schedule**.

Step 2 Click **Apply** to set the discovery schedule for a future discovery, or **Run Now** to run the cluster discovery immediately.

If any of the following changes occur on the cluster configuration before the scheduled periodic data collection and you want these changes to appear in Cisco Prime Collaboration Assurance immediately, you must use the **Run Now** option to collect the following types of data:

- New device pools, location, region, redundancy group, Route List, Route Group, Route pattern or Partition added, deleted or modified in the cluster.
- Changes in membership of any endpoint to the device pool or association of any endpoint to the redundancy group.

- New subscriber added to or deleted from the Unified CM cluster.
- Changes in membership of any subscriber to the redundancy group.
- Changes in membership of any gateway to route group or route group to route List.

If changes are limited to a specific cluster, you can rediscover the publisher of the cluster by using **Device Inventory > Inventory Management > Rediscover**.

For Cisco Prime Collaboration Release 11.5 and later

If changes are limited to a specific cluster, you can rediscover the publisher of the cluster by using **Inventory > Inventory Management > Rediscover**.

For a new Unified CM cluster, discovery or rediscovery is followed by phone discovery for that cluster. In case there is any other phone synch up operation (such as cluster phone discovery, or XML discovery) in progress then the cluster-based phone discovery will wait for it to complete. Thus a phone status change reflection in Cisco Prime Collaboration Assurance takes more time than expected in case there is any other phone sync up operation in progress.

Related Topics

[Setting Up Devices for Cisco Prime Collaboration Assurance](#)

Rediscover Devices

You can rediscover devices that have already been discovered. The credentials previously entered are already available in the Cisco Prime Collaboration Assurance database, and the system is updated with the changes. Devices in any state can be rediscovered.

For Cisco Prime Collaboration Release 12.1 SP2 and later



Note

As part of any rediscovery, Cisco Prime Collaboration Assurance has to Unsubscribe and Subscribe again.

Perform rediscovery when:

- Device must be added first and then rediscovered.
- There are changes in the first hop router configuration, and for software image updates.
- There are changes to the credentials; location; time zone; and device configurations such as IP address or hostname, SIP URI, H.323 gatekeeper address, and so on.
- After performing a backup and restoring Cisco Prime Collaboration Assurance.

Use the Rediscover button in the Current Inventory pane to rediscover devices listed in the Current Inventory table. You can perform rediscovery on a single device as well as on multiple devices.

When you perform rediscovery of a device (router, switch, or voice gateway) that has become unreachable with its earlier managed IP address in Inventory Management, the device is rediscovered with the IP Address of any of its interfaces. You can change this behavior, by setting the value of *com.cisco.nm.emms.discovery.ip.swap* property to **false** in the *emsam.properties* file. In this case, the device (router, switch, or voice gateway) does not get rediscovered with the IP Address of the interfaces. Now, rediscover (**Operate > Device Work Center**) the device with the earlier managed IP Address.

For Cisco Prime Collaboration Release 11.1 and earlier

Choose **Inventory Management** to rediscover the device with the earlier managed IP Address.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory Management** to rediscover the device with the earlier managed IP Address.



Note Accessibility information is not checked during rediscovery.

The workflow for rediscovery is the same as for discovery. See [Discovery Life Cycle](#) for details.

Verify Discovery Status

The status of all discovery jobs is displayed in the **Job Management** page. After running discovery, a dialog box appears with the Job Progress Details link to enable you to verify the discovery status. The time taken to complete a discovery job depends on your network. After the discovery is complete, the details appear in the Current Inventory table.

To verify discovery status:

Step 1 Choose **Device Inventory > Inventory Management > Discovery Jobs**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management > Discovery Jobs**.

Step 2 From the **Job Management** page, select the discovery job for which you want to view the details.

The status of discovery, and all the devices discovered during discovery appear in the pane below the Job Management table.

Step 3 Check the Job Management table for discovery status. or the Job details pane for details about discovered devices.

Step 4 Depending on your results, perform any one or more of the following:

- For any devices that were not discovered because of incorrect credentials, verify the credentials for those devices, and run the discovery again.
 - To discover the same devices more than once, use the Rediscover option. For more information, see [Rediscover Devices](#).
-

Troubleshooting

1. **Issue:** Cisco TelePresence Video Communication Server (Cisco VCS) Edge - External interface IP address is not reachable and causes alarms.

Recommended Action: You must discover the Cisco VCS Core and Cisco VCS Edge before discovering the Cisco Unified Communications Manager. This ensures that all the IP addresses of Cisco VCS - Edge external and internal interfaces are known in the Cisco Prime Collaboration Assurance inventory. When

the Cisco Unified Communications Manager publisher is discovered, the interface IP address is matched with the collected inventory and does not cause unreachable alarms.

2. **Issue:** Cisco TelePresence Management Suite (TMS) - The associated devices are not discovered.
Recommended Action: Ensure that you have performed Logical Discovery of the Cisco TelePresence Management Suite (TMS) to discover the associated devices. The Add Device option only discovers the TMS and does not discover the associated devices.

Rediscover the TMS with selection of the Enable Logical discovery option. Ensure that the credentials are added for all the associated devices.
3. **Issue:** Cisco TelePresence Touch Panels are not capable of sending syslog event without being directly connected to a Codec Endpoint.
Recommended Action: Ensure that the Cisco TelePresence Touch Panels are connected to the Codec and the Codec is rediscovered in Cisco Prime Collaboration Assurance.
4. **Issue:** DX80/Phones are not discovered successfully.
Recommended Action: DX80 and other phones are only discovered as part of Phone Sync, CDT, or Cisco Unified Communications Manager publisher cluster discovery. Other than Registration/Un-Registration status, any configuration change in phones is updated in the Cisco Prime Collaboration Assurance inventory only after the Cluster Data Discovery.

You should not discover the DX80 device separately by adding DX IP address.
5. **For Cisco Prime Collaboration Release 11.6 and later**
Issue: CiscoDX80/DX70 devices with CE image are not discovered successfully.
Recommended Action: Ensure that the CiscoDX80/DX70 devices are present in Cisco Unified Communications Manager.

For more information, see [Configure Devices for Cisco Prime Collaboration Assurance](#).
6. **For Cisco Prime Collaboration Release 11.6 and later**
Issue: CiscoDX80/DX70 devices with CE image are discovered successfully and it is in Inaccessible state.
Recommended Action: Add credential profile for CiscoDX80/DX70 devices and also verify that Cisco Prime Collaboration Assurance can ping the device from the Device360 view ping option.

For more information, see [Configure Devices for Cisco Prime Collaboration Assurance](#).
7. **For Cisco Prime Collaboration Release 11.6 and later**
Issue: CiscoDX80/DX70 devices with CE image are in the Unsupported state.
Recommended Action: Ensure Cisco Prime Collaboration Assurance is above the 11.6 version, if it is below 11.6 version then CiscoDX80/DX70 devices with CE image is not supported.

For more information, see [Configure Devices for Cisco Prime Collaboration Assurance](#).
8. **For Cisco Prime Collaboration Release 11.6 and later**
Issue: CiscoDX80/DX70 devices with CE image are not displaying in Conference Diagnostics page.
Recommended Action: Ensure that proper JTAPI credentials are added for the managed Unified CM where these phones are registered.

For more information, see [Configure Devices for Cisco Prime Collaboration Assurance](#).

9. **Issue:** Unable to find the serial number of phones.

Recommended Action: Device 360° View of the phone shows the serial number. Go to the **Inventory > Inventory Management**, and click the icon on the IP address of the phone to launch its Device 360° View.

10. **Issue:** Cisco Unified Communications Manager shows as a non-Cisco Device.

Recommended Action: Enable the Cisco Unified Communications Manager SNMP service on the Cisco Unified Communications Manager. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:

- [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
- [Configure Devices for Cisco Prime Collaboration Assurance](#)

11. **Issue:** Endpoint name is not updated immediately in the Cisco Prime Collaboration Assurance inventory.

Recommended Action: Check the following:

- The endpoint name of an endpoint belonging to a cluster is updated only after performing the Cluster Data Discovery.
- Reset the endpoint in Cisco Unified Communications Manager, after modifying the endpoint description. The endpoint name is immediately updated in Cisco Prime Collaboration Assurance through syslog notification. Ensure that the syslog is configured in Cisco Prime Collaboration Assurance.

12. **Issue:** Counters are not getting loaded for Cisco SocialMiner devices and custom dashboard displays **No Data Available**.

Recommended Action: Check that the following conditions are met:

- Ensure that the Cisco SocialMiner device is up and running and is in Managed state on the **Inventory Management** page.
- Verify that the service is running by typing the following URL on a browser:

```
http://<ServerIP>:8080/sm-dp/rest/DiagnosticPortal/GetPerformanceInformation
```

13. **Issue:** Counters are not getting loaded for Cisco Finesse devices and custom dashboard displays **No Data Available**.

Recommended Action: Check that the following conditions are met:

- Ensure that the Cisco Finesse device is up and running and is in Managed state on the **Inventory Management** page.
- Verify that the service is running by typing the following URL in a browser:

```
https://<server>/finesse-dp/rest/DiagnosticPortal/GetPerformanceInformation
```



CHAPTER 13

Manage Device Groups

This section explains the following:

- [Manage Device Groups, on page 139](#)

Manage Device Groups

This chapter provides information about managing device groups.

About Device Groups

Device groups are created automatically. After device discovery, you can find device groups based on the device type, irrespective of their states. Only licensed devices which you have deployed in your network appear in the groups. No empty groups or groups with no devices appear in the Device Group pane.

Grouping devices helps you to display data for a single device, or for a group. You can create customized groups to monitor information that you are interested in. You can view the grouping structure as a list or tree view in the Device Group pane. The Device Group pane is available in the Inventory, Conference Diagnostics (as a filter), Endpoint Diagnostics, and Alarms and Events pages. You can select devices or endpoints from the groups you are interested in, to check inventory details. You can also select devices for polling from the Device Group Selector in the Polling Parameters page. See [Device Group Selector](#) for information.

Cisco Prime Collaboration Assurance supports groups in a hierarchical fashion. Each child group is a subgroup of a parent group, and its group membership will be a subset of its immediate parent group. For an object to belong to a group, it must satisfy the immediate group rules and the parent group rules.

You can also create groups manually on any page where the group selector (tree view) is available.

Grouping is used to filter:

- Devices on the Inventory Management page
- Reports
- Conferences on the Conference Diagnostics page
- Endpoints on the Endpoint Diagnostics page
- Alarms and events on alarm and event browser pages
- Dashlets on the landing page

Devices in Cisco Prime Collaboration Assurance are grouped into:

- System-defined groups—defined by the system based on the device type. System-defined groups are always dynamic, and cannot be deleted or edited.

Predefined groups—defined by system based on endpoint groups. Predefined groups are always dynamic, and cannot be deleted or edited. The following predefined groups are available:

- Audio IP Phones
- Desktop Video
- Immersive Telepresence
- IP Phones
- Mobile Endpoints
- Multipurpose Telepresence
- Personal Communicators
- Personal Telepresence
- Soft Clients
- Telepresence Endpoints
- Unknown

To know the devices that belong to each group, rest your mouse over the quick view icon of that group, and then click on Rules.

- User-defined groups—Can be either of the following:
 - Static—Devices are added to these groups without a defined set of rules. After the group is created, you can manually add devices to it. Devices for which you cannot easily set a rule fall into this group. Only static user-defined groups are synchronized from Device Group to the Device Selector pane in the Polling Parameters page. Static groups created within dynamic groups are also not synchronized.
 - Dynamic—Devices are added to dynamic groups during group access, based on a set of rules or attributes (for example, device type, device model, hostname, and so on) that you define. You can use group properties to define the rules, and the group is updated when the group rule is met.



Note The amount of time it takes to create a user-defined dynamic group depends on the number of members within the group.

For user-defined dynamic and static groups, you can add subgroups, edit groups, delete groups, and duplicate groups, using the quick view. For dynamic groups, when you create or add a dynamic subgroup, it automatically inherits the parent group rule.

To launch the quick view, rest your mouse over the device group and click on the quick view icon. The Quick View details for user-defined groups are as follows.

Table 22: Quick View Details for User-Defined Groups

Field	Description
Name	Name of the device.
Description	Description of the device.
Type	Type of the device.
Group Type	Displays the group type: Dynamic or static.
Number of Members	Displays the total number of members in the group.
Number of SubGroups	Displays the number of subgroups (children) in the group. You can add any number of subgroups to a group.
Number of Rules	<p>Displays the number of rules set for the group.</p> <p>Note To know the details of the rules, hover the mouse over Number of Rules and click on the quick view icon.</p>
Add SubGroup	<ol style="list-style-type: none"> 1. Click Add SubGroup. 2. In the Create SubGroup window, enter details for the sub group. 3. Click Save. <p>You can create a static group within a dynamic group and vice versa. When you create a static subgroup, it does not inherit any rules from the parent dynamic group. Static subgroups are independent groups created at any hierarchy.</p> <p>For dynamic groups, when you create a dynamic subgroup, it automatically inherits the parent group rule.</p>
Edit Group	<ol style="list-style-type: none"> 1. Click Edit Group. 2. In the Edit Group window, edit the required fields. 3. Click Save. <p>You can edit the group name and description, and select a parent group.</p>
Delete Group	<ol style="list-style-type: none"> 1. Click Delete Group. 2. In the confirmation message box, click OK.

Field	Description
Duplicate Group	<ol style="list-style-type: none"> 1. Click Duplicate Group. 2. In the Duplicate Group window, enter details for the group. 3. Click Save. <p>When you perform a Duplicate Group for a dynamic group, the rule properties are copied to the new group.</p>

Create Groups

To create a group:

-
- Step 1** Click the icon at the right of the Device Group pane.
 - Step 2** Click **Create Group**.
 - Step 3** In the Create Group window, enter the group name and description.
 - Step 4** Select the group type **Static** or **Dynamic**.
 - Step 5** For Dynamic Group, set the rule by selecting **Match as All** or **Match as Any** and selecting a suitable combination of criteria from the drop-down list.
You can set more than one rule by clicking +. New rows are added.
 - Step 6** Click **Save**.
-

Add Devices to a Group

To add a device to a group:

-
- Step 1** Choose **Device Inventory > Inventory Management**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Inventory > Inventory Management**
 - Step 2** Select the managed devices from the Current Inventory table.
 - Step 3** Click the right arrow on the Current Inventory pane.
 - Step 4** Select **Add To Group**.
 - Step 5** In the Add To Group window, select the group you are interested in from the Select Group drop-down list, and click **Save**.
- Note** You can add or delete devices to a user-defined static group only. You cannot add devices to a user-defined dynamic group.
-

Remove Devices from a Group

To remove a device:

-
- Step 1** Choose **Device Inventory** > **Inventory Management**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Inventory** > **Inventory Management**
- Step 2** From the **Inventory Management** page, select the managed devices from the Current Inventory table.
- Step 3** Click the right arrow on the Current Inventory pane.
- Step 4** Select **Remove From Group**.
- Step 5** From the confirmation message box, click **OK**.
-

Device Group Selector

The device group selector provides a way to filter devices. It is available on the Polling Parameters page; choose (**Assurance Administration** > **Polling Settings**) to select groups for polling.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **Polling Settings** to select groups for polling.

Related Topics

[Poll Settings](#), on page 189



CHAPTER 14

Manage Inventory

This section explains the following:

- [Manage Inventory, on page 145](#)
- [View Inventory Details, on page 145](#)
- [Device-Specific Inventory Details, on page 161](#)
- [Update and Collect Inventory Details, on page 175](#)
- [Suspend and Resume Managed Devices, on page 178](#)
- [Delete Devices, on page 179](#)
- [Performance Graphs, on page 180](#)
- [Unified CM Device Search, on page 185](#)
- [SNMP Query, on page 186](#)

Manage Inventory

This chapter provides information about managing inventory.

View Inventory Details

Cisco Prime Collaboration Assurance performs continuous, real-time discovery of inventory. You need to periodically update the inventory so that you have up-to-date information about your network. You can schedule how often you want to update inventory.

When you update inventory, the inventory synchronizes with the Cisco Prime Collaboration Assurance database. The Cisco Prime Collaboration Assurance inventory reflects every addition, deletion, and modification that occurs in the network after update.

In Cisco Prime Collaboration Assurance, devices are grouped based on the device type. The Device Group pane is available in the Inventory Management, Conference Diagnostics (as a filter), Endpoint Diagnostics, and Alarms and Events pages. You can select devices or endpoints from the groups you are interested in, to check inventory details.

**Note**

Cisco Telepresence Endpoints discovered as TC/CE device type in Cisco Prime Collaboration Assurance should not be included in the JTAPI user controlled devices list. We recommend you to keep the IP Phones into the JTAPI user controlled list.

You can hover over the device host name column in the inventory table, and click the Device 360 ° view to see device details, such as alarms, interfaces, ports, environments, modules and other device-specific capabilities of that device. For more information, see [Device 360° View](#). The inventory table also displays the software version of the devices that are managed and registered to Unified Communications Manager. The devices include soft phones, hard phones, and Jabber.

In addition to the inventory table, the Inventory Management page contains System Information, Access Information, Interface Information, and Event Settings panes that appear below the inventory table. All of these panes are populated based on the last polled data. A device must be in the Managed state at least once for these details to be displayed.

Inventory Pane

The current inventory table is available in the Inventory page.

Each device that is managed by Cisco Prime Collaboration Assurance is modeled to display the physical inventory of a device (interface and peripherals). To view the inventory details for a device, click on a row in the Current Inventory pane.

To select multiple devices (first 500 entries), use the check box available on the top left corner of the Current Inventory pane.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can assign a customer to a device or devices by selecting the device(s), and then clicking on the **Edit > Assign**. The Edit Device dialog box appears, from where you can select the customer name from the drop-down list. You can assign a customer to a cluster too, by selecting the cluster from the Device Group pane, select the Host Name check box (this selects all the devices of the cluster), and then click **Edit > Assign**. Similarly to unassign a customer, select the device(s), and then click **Edit > Unassign**.

You can modify the credentials and rediscover devices using the Modify Credentials option. Click on Job Progress in the confirmation message window and cross launch to the Jobs Management page to see the details of the discovery job.

For Cisco Prime Collaboration Release 11.1 and earlier

You can enable, disable or set different options for automatic troubleshooting using the Threshold Settings option.

You can suspend and resume the management of the device using the Suspend and Resume options. Inventory is not updated for devices in the Suspended state.

You can use the show drop-down list on the inventory table to filter devices based on the device type and state. For example, if you want to rediscover all deleted devices in your network, select Deleted from the show drop-down list. The inventory table will list all deleted devices. Perform rediscovery to discover these devices.

For example, if you want to rediscover all deleted devices in your network, select Deleted from the show drop-down list. The inventory table will list all deleted devices. Perform rediscovery to discover these devices.

There are options such as Quick Filters, Advanced Filters to filter devices based on the device criteria.

The Total field in the upper right corner of the inventory table displays the device count. To view the number of devices in a group, select the group.

For example, to view the number of phone endpoints, select the Endpoints group in Device Group. The number of endpoints will be updated in the Total field. For more information on the device count, see the Field Descriptions for the Current Inventory table.

You can view the list of unknown endpoints by selecting Device Group Selector > Predefined > Unknown Endpoints.

For Cisco Prime Collaboration Release 12.1 and later

You can enable, disable or set different options for automatic troubleshooting using the Threshold Settings option.

You can suspend and resume the management of the device using the Suspend and Resume options. Inventory is not updated for devices in the Suspended state.

You can use the show drop-down list on the inventory table to filter devices based on the device type and state.

There are options such as Quick Filters, Advanced Filters to filter devices based on the device criteria.

The Total field in the upper right corner of the inventory table displays the device count. To view the number of devices in a group, select the group.

For example, to view the number of phone endpoints, select the Endpoints group in Device Group. The number of endpoints will be updated in the Total field. For more information on the device count, see the table on "Field Descriptions for the Current Inventory Table".

You can view the list of unknown endpoints by selecting **Device Group Selector > Predefined > Unknown Endpoints**.

This table describes the fields on the Inventory table. Not all columns of the inventory table appear by default. To see all the columns, click the Settings option on the top right corner. You can export the inventory table as a CSV or a PDF file by clicking the Export icon at the upper right corner of the inventory table.

Table 23: Field Descriptions for the Current Inventory Table

Field	Description
Endpoint Name	Name assigned to the endpoint for ease of identification.
Extension	Directory Number of endpoints. This number helps to identify a device uniquely.
Phone Description	A unique description of the endpoints that you have added during configuring the devices on Cisco Unified Communications Manager (CUCM) or Cisco TelePresence Video Communication Server (VCS).
Host Name	Name assigned to the device for ease of identification.
Model	Device model, such as Catalyst3506G48PS.

Field	Description
IP Address	<p>IP address used for managing the device.</p> <p>Click on the IP address to log into the device.</p> <p>This feature is not available in MSP mode.</p> <p>Click on the quick view icon to launch the Device 360 Degree View for that device.</p> <p>If that device is an endpoint the Endpoint 360 Degree View appears.</p> <p>If these devices are discovered by logical discovery then the IP Address and Private IP address will be same.</p> <p>For routers and switches, you must associate a terminal client application, such as Putty, to log into the device.</p>
Mac Address	MAC Address of the devices.
Software Type	Software running on the device, such as IOS, CentOS.
Software Version	<p>Software version running on the device.</p> <p>Note The Software Version field displays NA when the device is not registered to Unified Communications Manager.</p>
Device Pool	Only for CUCM registered devices.
Partition	Only for CUCM registered endpoints.
Serial Number	Applicable only for endpoints.
State	Status of the device.
Status Reason	Reason for the device status.
Type	The most applicable role or service of the device.
Capabilities	All other roles or services of the device.
Last Discovered	<p>Date and time when the device was last discovered.</p> <p>The time will be according to the time zone set in the Cisco Prime Collaboration Assurance server.</p>
For Cisco Prime Collaboration Release 11.1 and earlier Customized Events	<ul style="list-style-type: none"> • Green check mark displayed—Event settings are customized for the device using Customize Events tab. • Green check mark not displayed—Event settings are not customized for the device. The device uses global settings.

Field	Description
For Cisco Prime Collaboration Release 11.1 and earlier Mediatrace Role	<ul style="list-style-type: none"> • Unsupported—Device does not support Cisco Mediatrace. • Transparent—Device supports Cisco Mediatrace but profile is not configured. • Responder—Cisco Mediatrace responder profile is enabled on the device. Enable this profile if you want to monitor and collect information on Cisco Mediatrace. • Initiator—Cisco Mediatrace initiator profile is enabled on the device. Enable this profile if you want to initiate Cisco Mediatrace session or polls. • Initiator/Responder—Cisco Mediatrace initiator and responder profiles are enabled on the device.
For Cisco Prime Collaboration Release 11.1 and earlier IP SLA Role	<ul style="list-style-type: none"> • Unsupported—Device does not support Video IP SLA. • Not Configured—Device supports the Video IP SLA but the device is not configured. • Responder—IP SLA Responder profile is configured on the device. The device that is configured with this profile processes measurement packets and provides detailed time stamp information. The responder can send information about the destination device's processing delay back to the source Cisco router.
For Cisco Prime Collaboration Release 11.1 and earlier Performance Monitor	<ul style="list-style-type: none"> • Unsupported—Device does not support Cisco Performance Monitor. • Not Configured—Device supports Cisco Performance Monitor but the device is not configured. • Configured—Cisco Performance Monitor is enabled to allow you to monitor the flow of packets in your network and become aware of any issues that might impact the flow.

**Note**

- To update the unknown phones in inventory, trigger Cluster Data Discovery. This is triggered automatically at midnight.
- If you change the IP address or swap IP addresses, the device type is not identified. In such a case:
 - Navigate to the `/opt/emms/emsam/conf/` folder and edit the `emsam.properties` file.
 - Find the line `com.cisco.nm.emms.devicetype.rediscovery = false` and change the value from 'False' to 'True'.
 - To restart Cisco Prime Collaboration Assurance server, login as `root` and execute the following commands:
 - 1. Stop the processes:**

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh stop
```
 - 2. Check the status of the processes** - Verify whether the processes have stopped:


```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh status
```
 - 3. Restart the processes:**

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh start
```
 - Rediscover the device.

The Mobile Remote Access (MRA) clients (such as Cisco Jabber, Cisco TelePresence MX Series, Cisco TelePresence System EX Series, and Cisco TelePresence SX Series) have the same IP address as that of the Cisco Expressway-Core device in Cisco Unified Communications Manager, however in Cisco Prime Collaboration Assurance the IP Address is shown as NA.

**Note**

Device 360° View is available for MRA clients.

Related Topics

[Conference Diagnostics Dashboard](#), on page 258

[Manage Device Groups](#), on page 139

[Unified CM Cluster Data Discovery](#), on page 133

Device 360° View

You can get a concise summary information regarding any device through its 360° view. Rest your mouse over a device IP address, then click the quick view icon to launch the Device 360° View window. You can also do a global search for a device to see the device details in the Device 360° View.

In addition to viewing device information such as status, location, you can also view modules, alarms, and interfaces on the device, invoke tools like ping, and traceroute for that device.

If the device belongs to a cluster, you can cross launch to the cluster view of the cluster the device belongs to, by clicking on the Cluster ID value.



Note If you are using Internet Explorer 10 and 11, ensure that you have the recommended browser settings to view the Device 360° View window. Press F12 in your browser and set the following:

- For Internet Explorer 10:
 - **IE10 Browser Mode:** IE10 or IE10 Compatibility View
 - **Document Mode:** Standards (Default) or Quirks
- For Internet Explorer 11:
 - **Browser Profile:** Desktop
 - **Document Mode:** Edge (Default)

Launch the browser again to view the Device 360° view window.

The 360° Device View window contains the following device details:

Table 24: Field/Buttons and their Description

Field	Descriptions
State	You can hover on the State icon to know the state of the device. Different colors of the icon represent different states.
Status Reason	You can hover over the icon to know the status reason of the device and any additional activities you need to perform to make all features work. Different colors of the icon correspond to the state the device is in.
Host Name	—
Host IP /Global IP Address	You can click the IP address to launch the device management page. To log into routers and switches, ensure that you click on the IP address and associate a terminal client application, such as TELNET or SSH. This feature is not available in MSP mode.
MAC Address	MAC address of the device.
Type	The device type or primary role or capability of the device is mentioned on the right corner below the hostname row. For example, Finesse, Unified CM or Unity Connection.
Host Name	If you have deployed Cisco Prime Collaboration Assurance in MSP mode in a NAT environment, you will see the host name of the device.

Field	Descriptions
Customer	If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to.
Version	Software version of the device.
Last discovered	Time stamp of last successful discovery.
Cluster ID	Cluster ID of the cluster the device belongs to. You can click on the cluster ID to launch the Cluster Details page.
—	<p>Click the support community icon to open the Cisco Support Community Dialog box which has the related posts and discussions filtered for the device. You can post a question for that device.</p> <p>You can go to the support pages of other devices, and also visit the support community page of Cisco Prime Collaboration Assurance. To visit the Cisco Prime Collaboration Assurance page, click Visit the Cisco Support Community, click on Navigate to a Community Topic and Post pane, then click Collaboration, Voice and Video. In the Collaboration, Voice and Video Communities table, click Prime Collaboration Management.</p> <p>You can post questions in the Cisco Prime Collaboration Community forum, and look for related questions or information in existing discussions, videos, and additional documents for your issues.</p> <p>For business impacting technical issues, we recommend that you open a service request with Cisco TAC for timely support.</p>
—	Click the ping icon to ping the device and get ping statistics, such as the number of packets transmitted and received, packet loss (in percentage), and the time taken to reach the device by ping in milliseconds (ms).
—	Click the traceroute icon to know the route to reach the device, the number of hops to reach the device, and the time elapsed at each hop in milliseconds (ms).
—	<p>Click the tasks icon, and select from the drop-down list to perform multiple tasks such as launching performance graphs and managing thresholds.</p> <p>Note The options available depend on the device you have selected.</p>

Other device-specific information is as follows:

Table 25: Device 360° View - Tabs Description

Tabs	Description
Alarms	<p>It includes the following:</p> <ul style="list-style-type: none"> • Severity — Severity of the alarm • Status — Status of the alarm • Name — Name of the device • Component — Name of the component that has alarms • Last Updated — Time stamp of the last alarm generation.
Interfaces	<p>It includes details on interfaces, voice interface and port (whichever applicable for the device). It specifies the card is playing on a particular port, and the capability of the card. The following information is available for the interface, voice interface and port:</p> <ul style="list-style-type: none"> • Operation Status (Oper Status) — Operational state of the device • Admin Status — Administrative status of the interface • Name — Description of the device • Address — Physical address of the device • Type — Device type
Card/Services	<p>It includes the following:</p> <ul style="list-style-type: none"> • Name — Description of the voice/service • Version — Version of the card/service • Status — Status of the card/service
Port	—
Environment	<p>It includes:</p> <ul style="list-style-type: none"> • Power supply • Fan • Temperature sensor • Voltage sensor

Tabs	Description
Device-specific details	—

You can view the Differentiated Services Code Point (DSCP) values (both in decimal format and its meaning) for Cisco TelePresence TX Series under the Connectivity Details tab of the Endpoint 360° View of the devices.

Choose **Inventory Management**, and click on the IP Address column to launch the Endpoint 360° View.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**, and click on the IP Address column to launch the Endpoint 360° View.

For more information on Differentiated Services Code Point (DSCP) values, see [RFC 2474](#).



Note

The fields displayed depend on the device you have selected.

Click the **View More** button on top to:

- View the Device 360° View pop up in window size.
- Create performance dashboards for Cisco Unified Communication applications/devices by selecting specific counters. For more information, see “Create Custom Performance Dashboards”.

Metric Charts

You can view metric charts for voice devices (excluding phones) and CTS. These charts appear only for devices in managed state and for which at least one polling cycle is over.



Note

It will take time for the chart to appear after the device is in managed state. This is because polling has to be completed to fetch data for these charts.

These charts display values for CPU, Memory and Hard Disk utilization etc. You can view maximum, minimum and current value (in percentage or bytes in MB) of the last hour. Each bar on the metric chart denotes a period of four minutes, thus there are 15 bars, each denoting the value for four minutes. The figures in brown represent the minimum value, and the figures in blue represent the maximum value for the last hour.

You can click **See More** to launch performance graphs for some devices.

For an Multipoint Controller (MCU) you can see the absolute values and percentage of Audio and Video Port utilization in the performance graphs. You can select these options near the top right of the chart.

Performance graph is available for TP Server. You can see the absolute values and percentage.



Note

The metric charts and performance graphs availability depend on the device you have selected.

Global Search Options for Cisco Prime Collaboration Assurance

For Cisco Prime Collaboration Release 11.6 and 12.1

The following table describes the Global Search options for Cisco Prime Collaboration Assurance.

Table 26: Global Search Options for Cisco Prime Collaboration Assurance

Search	Variable	Sample String Format	Exceptions and Allowed Search Strings
Endpoint	DN	10002 1000* 100* 1* *0002	Alphanumeric characters, dash, period, and underscore.
	IP	10.64.101.162 10.64.101.* * 10.78.22.77 . 10.78.22.* 10.78.*.* 10.*.*.* *.	Alphanumeric characters, dash, period, and underscore. The special character % does not retrieve results. Ampersand (&) and blank space are not allowed.
	MAC	00260bd75cf8 00260bd75cf* 00260bd* 0* 00*	Dash, period, underscore, are not allowed. Alphanumeric and blank space are allowed. Note When you search for phones using the MAC address in the global search option, do not use colon or hyphen or dots in between.
	Endpoint Name	San Jose	-
Device	IP	10.78.22.129 10.78.22.* 10.*	Alphanumeric characters, dash, period, underscore, and space.
	DNS	cussmtest-15.cisco.com	If the domain name is not resolvable, the IP address is displayed in the search results.

Search	Variable	Sample String Format	Exceptions and Allowed Search Strings
User	First Name or Last Name or User Name	HS John	Alphanumeric characters, dash, underscore, and blank space are not allowed.

For Cisco Prime Collaboration Release 11.6 and 12.1

Search Results

Search Parameter	Search Result
Endpoint	Endpoint Name, Directory Number, IP Address, IPv6 Address, MAC Address, Model, Cluster Name, Software Version, Registration Status, and Status Reason. When you perform an endpoint search, all phones and Cisco TelePresence endpoints are also included in the search. You can click on the icon next to the IP address to launch the Endpoint 360° View for that endpoint.
Device	Name, IP Address, Status, and Device Type. When you perform a device search, all phones and Cisco TelePresence endpoints are also included in the search. You can click on the icon next to the device name to launch the Endpoint or Device 360° View for that device. Note The information displayed depends on the device you have searched for.
User	First Name, Last Name, and User Name. You can click on the icon next to the user name to launch the User 360° View for that user.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can also see the customer to which the searched device belongs to. If the device belongs to multiple customers, then all the customers to which it belongs are mentioned. If the device is not associated with any customer or is associated with all customers, it is part of the default customer domain - All Customers, but shows a blank for customer details in the search result. You can click on the customer name to launch the home page filtered for that customer.

Search Use Cases

You can perform a search based on the following use cases.

Table 27: Search Use Cases

To search for...	Perform/Use
All devices belonging to a particular customer.	Select the customer from the global customer selection drop-down list at the top right of your screen, select Device search, and then enter the search string *.

Cisco Jabber	Endpoint Search
E20	Endpoint Search
Infrastructure devices	Device Search
IP address of a device with a partial IP address.	Device Search - For example search with a string such as 10.*
List of all users associated with a particular customer.	Select the customer from the global customer selection drop-down list at the top right of your screen, select User search, and then enter the search string *.

Inventory Summary

The Inventory Summary lists the count of devices based on the device state. The Total column displays the total number of devices in a particular state. The device count is available as a cross-launch to the Inventory table in Inventory Management. When you click on any count, you will be directed to the Inventory table, where you can see all the devices in that particular state.

The Inventory Summary is available as a slider at the bottom of your user interface browser. You can view the details when you scroll down. The Inventory Summary data is refreshed every 30 seconds.

Table 28: Inventory Summary - Field Descriptions

Field	Descriptions
Unknown Endpoints	Total number of unknown endpoints. You can click on this number to launch the filtered list of unknown endpoints in the Endpoint Diagnostics page.
Partially Managed	Devices which are in managed state but have some credentials missing. These credentials are not mandatory for managing inventory, but required for all other features, such as troubleshooting to work. You can click on the corresponding number to cross launch to see a list of all devices in the inventory table which are managed but with insufficient credentials. This count is updated only when you perform rediscovery after adding the credentials.



Note

Although the Total Count column contains the sum of the Infrastructure Devices, Endpoints columns combined for each device state, you may see some inconsistency in the number of devices in the Total Count column. This difference can happen when the computation includes device types in Unknown state from the inventory.

Device Status Summary

For Cisco Prime Collaboration Release 11.5 and later

The Device Status Summary lists the count of devices based on the device state. The counts does not include Phones & Unknown devices. The device count is available as a cross-launch to the Inventory table in Inventory Management. When you click on any count, you will be directed to the Inventory table, where you can see all the devices in that particular state. You can filter count based on Customer/Assurance Domain.

The **Device Status Summary** is available under **Inventory > Device Status Summary**. The **Devices** column displays the total number of devices in a particular state. The **Status** column displays the status of the devices. When you click on **Discovery Jobs**, you will be directed to **Job Management** page and where you can see the status of the discovery job.

You can view the following device status. For more information on status, see “Discovery Life Cycle” section in *Cisco Prime Collaboration Assurance Guide- Advanced*.

- Managed
- Partially Managed
- Inaccessible
- Unreachable
- Suspended
- Unsupported
- Undiscoverable

When you hover your mouse over Partially Managed, Inaccessible, or Undiscoverable states, you can view a tool tip with an explanation.

You can view Unmanaged device count in the global summary bar, adjacent to **Inventory Summary**. When you click on the count, you will be directed to **Device Status Summary** page.

Table 29: Device Status Summary - Field Descriptions

Field	Descriptions
Device Discovery Status	Displays the device discovery status.
Devices Discovery In-Progress <count>	Displays the number of devices for which discovery is in progress. Devices Discovery In-Progress <count> is not displayed, if there are no discovery in progress.

For Cisco Prime Collaboration Release 12.1 and later

The Device Status Summary lists the count of devices based on the device state. Devices, as referred to in this table, include Infrastructure components and Video/TelePresence endpoints. Phones are not counted (which includes DX series). When you click on any count, you will be directed to the Inventory table on the **Inventory Management** page, where you can see all the devices in that particular state. You can filter count based on Customer/Assurance Domain.

The Device Status Summary is available under **Inventory > Device Status Summary**. The **Devices** column displays the total number of devices in a particular state. The **Status** column displays the status of the devices.

When you click on **Discovery Jobs**, you will be directed to **Job Management** page from where you can see the status of the discovery job.

You can view the following device status. For more information on status, see "Discovery Life Cycle" section in Cisco Prime Collaboration Assurance Guide- Advanced.

Device Status Summary data is divided into 2 categories: Managed and Unmanaged.

- Managed category includes the following:
 - Discovered successfully
 - Partially Managed
- Unmanaged category includes the following:
 - Inaccessible
 - Unreachable
 - Suspended
 - Unsupported
 - Undiscoverable
 - Unknown

When you hover your mouse over Partially Managed, Inaccessible, Unreachable, or Undiscoverable state, you can view a tool tip with an explanation.

The count for both categories (Managed and Unmanaged) should match the sum of count of devices in the respective categories.

You can view Unmanaged device count in the global summary bar, adjacent to **Inventory Summary**. This count must match the Unmanaged device count in the **Device Status** table. When you click on the count, you will be directed to **Device Status Summary** page.

Table 30: Device Status Summary - Field Descriptions

Field	Descriptions
Device Discovery Status	Displays the device discovery status.
Devices Discovery In-Progress <count>	Displays the number of devices for which discovery is in progress. Devices Discovery In-Progress <count> is not displayed, if there are no discovery in progress.

Troubleshooting

Issue: CUCM rediscovery causes Pub to disappear from Cisco Prime Collaboration Assurance Inventory. This is due to the co-resident ELM/PLM configuration on CUCM. Since Cisco Prime Collaboration Assurance is case sensitive the ELM/PLM configuration should match the hostname of CUCM.

For example, if the co-resident ELM/PLM configuration on CUCM has a hostname lax-ccm-px.apl.com whereas the hostname of CUCM is LAX-CCM-PX.apl.com then, when you perform a re-discovery of the CUCM Pub, the CUCM Pub disappears from the inventory or gets deleted.

Recommended Action: Modify the file `/etc/hosts` of Cisco Prime Collaboration Assurance to re-discover the CUCM pub. Add an entry to the host file like the one mentioned below.

10.8.2.20

LAX-CCM-PX.apl.com

Inventory Status Error Messages

The credential verification error messages are tabulated below.

Table 31: Credential Verification Error Messages

Error Message	Condition	Possible Solutions
SNMP_ERROR	Failed for one of the following reasons: <ul style="list-style-type: none"> • SNMP service is enabled in the device • SNMP credentials do not match. • Firewall settings blocking the port. 	<ul style="list-style-type: none"> • Verify if SNMP service is enabled in the device • Verify and reenter the device SNMP credentials in the credential profile. • Verify if firewall settings blocks the port, and unblock the port using the correct port. For more information on required port, see Required Ports for Prime Collaboration.
UNKNOWN_ERROR	Error in discovering the device.	Perform a re-discovery. If issue persists, contact TAC for assistance.
INSUFFICIENT_INV_COLLECTION	The device is taking a longer time to respond than expected, may be due to the network latency.	Verify the the SNMP/HTTP(S) response time and perform a rediscovery. If the issue persists, contact TAC for assistance.
HTTP_ERROR	HTTP access has failed. Failed for one of the following reasons: <ul style="list-style-type: none"> • HTTP(S) credentials do not match • Firewall settings blocking the port. 	<ul style="list-style-type: none"> • Verify and reenter the device HTTP credentials in the credential profile. • Verify if firewall settings blocks the port, and unblock the port using the correct port. For more information on required port, see Required Ports for Prime Collaboration.

Error Message	Condition	Possible Solutions
JTAPI_ERROR	JTAPI access has failed. Firewall settings blocking the port.	<ul style="list-style-type: none"> Verify and reenter the device JTAPI credentials in the credential profile. <p>Note Password must not contain a semicolon (;) or equals symbol (=).</p> <ul style="list-style-type: none"> Verify if firewall settings blocks the port, and unblock the port using the correct port. For more information on required port, see Required Ports for Prime Collaboration. Verify if JTAPI user is configured in Cisco Unified CM. For more information to enable JTAPI, see Configure Devices for Prime Collaboration Assurance
UNSUPPORTED_DEVICE	Device is unsupported	Verify the supported devices from Supported Devices for Cisco Prime Collaboration Assurance .
UNDISCOVERABLE	Error while persisting	Perform a re-discovery. If issue persists, contact TAC for assistance.
DISCOVERY_FAIL_TOO_MANY_DB_CONNECTIONS	Error while persisting	Perform a re-discovery. If issue persists, contact TAC for assistance.

Device-Specific Inventory Details

The following tables provide field descriptions for additional inventory details for:

- [Table 32: Cisco Codec, MX, E20, and MXP](#)
- [Table 33: Cisco TelePresence Movi](#)
- [Table 34: Cisco Unified IP Phone 8900 and 9900 Series](#)
- [Table 35: CTMS](#)
- [Table 36: Cisco TMS](#)
- [Table 37: Cisco Unified CM](#)
- [Table 38: Cisco MCU and MSE](#)

- [Table 39: Cisco VCS](#)
- [Table 40: Cisco TelePresence Conductor](#)

Table 32: Cisco Codec, MX, E20, and MXP

Field		Description
TelePresence Endpoint (Data displayed based on selected endpoint type CTS, Cisco Codec, MX, E20, MXP, .)	Endpoint Name	Name assigned to the endpoint for ease of identification.
	Directory Number	IP phone details as defined in the endpoint.
	Call Controller	
	CUCM Address	Hostname or IP address of the Cisco Unified CM server where the endpoint is registered.
	CUCM Cluster ID	Identification of the Cisco Unified CM cluster where the Cisco Unified CM server is registered.
	VCS Address	Hostname or IP address of the VCS server where the endpoint is registered.
	VCS Cluster ID	Identification of the VCS cluster where the VCS server is registered.
	Registration Status	Registration status of the endpoint with call processor (Cisco Unified CM or VCS). If Cisco Unified CM or VCS is not managed, the information displayed is N/A.
	H323 ID	H.323 ID configured on the Cisco Codec device.
	E164 No	E164 number configured on the Cisco Codec device.
	H323 Gatekeeper Address	Network address of the gatekeeper to which the Cisco Codec device is registered.
	SIP URI	Registered SIP URI on the Cisco Codec device.
	SIP Proxy Address	SIP proxy address that is configured manually on the Cisco Codec device.

Field		Description
	Application Manager	
	TMS	Hostname or IP address of the application manager where the Cisco Codec device is integrated.
	Switch Details	
	Connected To Switch	Details of the switch to which the endpoint is connected.
	Port Connected	Details of the switch port to which the endpoint is connected.
	Peripherals	Name
Position		Position of the peripheral, such as <i>front_center</i> for a microphone.
MAC Address		MAC address of the peripheral.
Software Version		Software version running on the peripheral.
Model		Model of the peripheral.
Serial		Serial number of the peripheral.
Make		Manufacturer's details for the peripheral.
Firmware Version		Firmware version of the peripheral.
Hardware Version		Hardware version of the peripheral.
Midlet Version		

Peripheral type, such as uplink, phone, camera, display, touch screen monitor, microphone.

Field		Description
		Midlet version running on the peripheral.

**Note**

Cisco Prime Collaboration Assurance does not support peripheral details for Cisco TelePresence 150 MXP.

Table 33: Cisco TelePresence Movi

Field		Description
Movi	Endpoint Name	Name assigned to the endpoint for ease of identification.
	SIP URI	Registered SIP URI on the Cisco TelePresence Movi endpoint.
	VCS Address	Hostname or IP address of the VCS where the endpoint is registered.
	VCS Cluster ID	Identification of the VCS cluster where the VCS is registered.

Table 34: Cisco Unified IP Phone 8900 and 9900 Series

Field		Description
CUCM Endpoint	Endpoint Name	Name assigned to the endpoint for ease of identification.
	Model	Model of the endpoint, such as CP-8945 or CP-9971.
	Directory Number	IP phone details as defined in the endpoint.
	Serial Number	Serial number of the endpoint.
	Description	Description of the endpoint as defined in the call processor.
	Call Controller	
	CUCM Address	Hostname or IP address of the Cisco Unified CM server where the endpoint is registered.
	CUCM Cluster ID	Identification of the Cisco Unified CM cluster where the Cisco Unified CM server is registered.
	Registration Status	Registration status of the endpoint with call processor (Cisco Unified CM). If Cisco Unified CM is not managed, the information displayed is N/A.
	Switch Details	
	Connected To Switch	Details of the switch to which the endpoint is connected.
	Port Connected	Details of the switch port to which the endpoint is connected.
Status	Displays the status of the wi-fi connection, such as connected or not connected.	
IP Address	IP address used to manage the endpoint when connected using a wi-fi network.	
Default Router	IP address of the default router to which the endpoint is connected.	

Field		Description
Access Point Name	Name of the access point to which the endpoint is connected.	
Ethernet Details		
Status	Displays the status of the Ethernet connection, such as connected or not connected.	
IP Address	IP address used to manage the endpoint when connected using Ethernet.	

**Note**

For discovery of Cisco Unified IP Phone 8900 and 9900 series, you must enable the HTTP interface. If the HTTP interface is not enabled, these devices will not appear in the inventory table.

Table 35: CTMS

Field		Description
Multipoint Switch	Timezone	Time zone configured on the multipoint switch.
	SKU	—
	Hardware Model	Model number of the media convergence server on which the multipoint switch is running.
	Software Version	Version of multipoint switch administration software currently installed.
	OS Version	Operating System version.
	Hostname	Hostname configured for the multipoint switch.
	IP Address	IP address used to manage the multipoint switch.
	Subnet Mask	Subnet mask used on the IP address.
	MAC Address	MAC address of the media convergence server on which the multipoint switch software is running. This MAC address belongs to Ethernet interface 0 (the eth0 network interface card [NIC]). With failover, this MAC address persists, although another Ethernet interface becomes active.
	Switch Details	
	Connected To Switch	Details of the switch to which the multipoint switch is connected.
	Port Connected	Details of the switch port to which the multipoint switch is connected.
	Ad hoc Segments	Maximum number of segments that are available for impromptu meetings. The maximum number is 48.
	Maximum Segments	

Field		Description
		Total number of segments (individual video displays) that this multipoint switch can handle. The maximum number is 48.
	Schedulable	Number of segments available at any one time for scheduled meetings. The multipoint switch automatically derives this value by subtracting the defined number of ad hoc Segments from the defined number of maximum segments.

Table 36: Cisco TMS

Field		Description
Application Manager	SKU	—
	Hardware Model	Model number of the server on which the application manager is running.
	Software Version	Version of administration software currently installed.
	OS Version	Operating System version.
	Hostname	Hostname configured for the application manager.
	IP Address	IP address used to manage the application manager.
	Subnet Mask	Subnet mask used on the IP address.
	MAC Address	MAC address number supplied for the application manager.

Field		Description
System Connectivity (see note following this table)	Status	Whether the exchange server is running or down.
	IP Address	IP address assigned to the exchange server.
	Software Version	Version of software currently installed on the exchange server.
	Status	Whether the LDAP server is running or down.
	IP Address	IP address assigned to the LDAP server.
	Software Version	Version of software currently installed on the LDAP server.

Table 37: Cisco Unified CM

Field		Description
Call Processor	Cluster ID	Parameter that provides a unique identifier for the cluster. This parameter is used in Call Detail Records (CDRs), so collections of CDR records from multiple clusters can be traced to their sources. The default is StandAloneCluster.
	Publisher Hostname	Hostname configured for the cluster publisher.
	Registered CTS Endpoints	Number of registered endpoints on the call processor.
	Total CTS Endpoints	Total number of endpoints.

Table 38: Cisco MCU and MSE

Field		Description
MCU or MSE Details (Data displayed based on selected conferencing device: MCU or MSE.)	Hardware Model	Model number of the media convergence server on which the multipoint switch is running.
	Serial Number	Serial Number of the Multipoint Control Unit (MCU).
	Software Version	Version of multipoint switch administration software currently installed.
	MCU Type/Device Type	Type of the MCU or device.
	Build Version	Build version of the installed software.
	Manufacturer	Manufacturer's name.
	Hostname	Hostname configured in the device (MCU or Media Service Engine).
	IP Address	Local IP address of the MCU or Media Service Engine (MSE) network interface used to access the MCU or MSE web user interface.
	Subnet Mask	Subnet mask used on the IP address.
	MAC Address	Fixed hardware MAC address of the Ethernet port.
	Connected To Router	IP address of the router to which the MCU or MSE is connected.
	Cluster Type	Whether the cluster is a master or slave. If the cluster is configured, <i>Not Configured</i> is displayed.
	Total Video Ports	Number of video ports configured in MCU. (Data displayed only for MCU devices.)
	Total Audio Ports	Number of audio ports configured in MCU. (Data displayed only for MCU devices.)
SIP (Data displayed only for MCU devices.)		
Status		

Field		Description
		Whether the SIP registration is enabled or disabled.
	Proxy	Network address of the SIP proxy.
	Domain	Network address of the SIP registrar to which the MCU has registered.
	H.323 (Data displayed only for MCU devices.)	
	Status	Whether the H.323 gatekeeper registration is enabled or disabled.
	Gatekeeper ID	Identifier used by the MCU to register with the H.323 gatekeeper.
	Gatekeeper Address	Network address of the gatekeeper to which the MCU has registered.
MSE Blades (Data displayed only for MSE.)	Type	Type of the blade.
	Slot	Slot number. Slot 1 is MSE Supervisor; slots 2-10 are blades.
	Software Version	Version of the software used.
	Status	Status of the blade: OK or absent.
	Port A IP Address	IP address of Port A.
	Port B IP Address	IP address of Port B.

Table 39: Cisco VCS

Field		Description
Call Processor	Cluster ID	Cluster Name that is used to identify one cluster of VCSs from another.
	Master	Name of the VCS peer that is configured as the cluster master.
	Registered Endpoints	Number of endpoints registered to the VCS.
	Peers	Number of VCS peers configured within the cluster.

Field		Description
VCS Configuration	Timezone	Time zone that is configured on the VCS.
	Maximum Traversal Calls	Number of traversal call licenses available on the VCS.
	Maximum Non-Traversal Calls	Number of non-traversal call licenses available on the VCS.
	Maximum Registrations	Number of endpoints that can be registered with the VCS.
	Expressway	Whether the VCS Expressway is configured.
	Interworking	Whether the VCS is configured to allow H.323 systems to connect to SIP systems.
	Encryption	Whether AES encryption is available in the software build.
	Find Me	Whether FindMe is enabled or disabled.
	Device Provisioning	Whether the provisioning server is enabled on the VCS.
	Dual Network Interface	Whether the LAN 2 interface on the VCS Expressway is enabled.
	Starter Pack	Whether the Starter Pack option key is installed.



Note Cisco Prime Collaboration Assurance manages both the Cisco VCS application and appliance.

Table 40: Cisco TelePresence Conductor

Field		Description
TelePresence Conductor	Name	Hostname configured for the conductor.
	IP Address	IP address of the conductor.
	Software Version	Version of software currently installed.
	Cluster Master	Name of the conductor peer that is configured as the cluster master.
	Cluster Peers	Number of conductor peers configured within the cluster.
	Total Registered MCUs	Number of MCUs registered to the conductor.
	Software ID	Identification of the software on the conductor.
	Hardware Serial Number	Serial number of the conductor hardware.
Registered MCUs	Name	Name of the MCU registered to the conductor.
	IP Address	IP address of the MCU registered to the conductor.
	Type	Type of the MCU registered to the conductor.
	Pool	MCU pool to which the MCU belongs.
	Blacklisted	Listed MCUs are not used by the conductor.
	Blacklisted Reason	Reason why the MCUs are not used by the conductor.
	Media Load: Allocated/In Use/Max Available	Media load allocated and in use, and the maximum available load.
	Signalled Load: Allocated/In Use/Max Available	Signalled load allocated and in use, and the maximum available load.



Note Only Cisco TelePresence Conductor-controlled MCU cascading is supported.

For Cisco Prime Collaboration Release 11.5 and later**Note** The following devices are not supported:

- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence-Manager (CTS-MAN)

Update and Collect Inventory Details

Updating and collecting inventory details depend on the type of network deployed: voice, video or both. It also depends on the data you want to collect at a given point. The following table recommends when to update inventory based on your network.

Table 41: Recommendations to Update Inventory

Description	Task
If you have both voice and video endpoints deployed in your network, and want to collect data on both.	Perform Update Inventory (choose Device Inventory > Inventory Management > Update Inventory). For more information, see Update Inventory . For Cisco Prime Collaboration Release 11.5 and later Choose Inventory > Inventory Management > Update Inventory
If you have both voice and video endpoints deployed in your network, and you want to collect data on video endpoints only.	Perform Update Inventory (choose Device Inventory > Inventory Management > Update Inventory). For more information, see Update Inventory . For Cisco Prime Collaboration Release 11.5 and later Choose Inventory > Inventory Management > Update Inventory
If you have both voice and video endpoints deployed in your network, and you want to collect data on voice endpoints only.	Perform Cluster Data Discovery (choose Assurance Administration). For more information, see Inventory Details Collection . For Cisco Prime Collaboration Release 11.5 and later Choose Alarm & Report Administration .

Description	Task
If you have only a voice network	Perform Cluster Data Discovery (choose Assurance Administration). For more information, see Inventory Details Collection . For Cisco Prime Collaboration Release 11.5 and later Choose Alarm & Report Administration .
If you have only a video network	Perform Update Inventory (choose Device Inventory > Inventory Management > Update Inventory). For more information, see Update Inventory . For Cisco Prime Collaboration Release 11.5 and later Choose Inventory > Inventory Management > Update Inventory

Update Inventory

The Update Inventory task helps you to synchronize the Cisco Prime Collaboration Assurance Inventory database with the network. During this task, accessibility verification is not performed (see the Update Inventory Lifecycle chart).

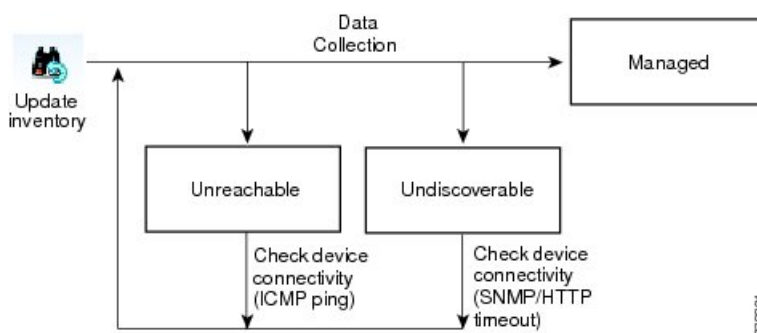
Perform the Update Inventory task when:

- You want to synchronize the database for all devices managed in your network. However, you can update the configuration details for specific devices based on the device status criteria.
- You want to define a periodic Update Inventory job to keep the Cisco Prime Collaboration Assurance database up-to-date.
- There are any changes in the network devices' interfaces.



Note The new devices that are added to the network will not be identified.

Figure 3: Update Inventory Lifecycle



We recommend that you define a periodic Update Inventory job to keep the Cisco Prime Collaboration Assurance database up-to-date.

To update inventory:

Step 1 Choose **Device Inventory > Inventory Management**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**

Step 2 In the **Inventory Management** page, click **Update Inventory**.

Step 3 If you want to update the inventory based on device status, check the Update devices based on device criteria check box in the Update Inventory window and select the desired device criteria from the drop-down list.

If you choose to update the inventory based on device status, an accessibility information check is performed. If you do not, the inventory is updated with all devices in the Managed state. Device accessibility is not checked.

To schedule a periodic update inventory job, go to add **step 4**. To run the job immediately, go to **step 5**.

Step 4 Enter the job name and the scheduling details. See [Job Schedule - Field Descriptions](#) for field descriptions.

Step 5 Click **Run Now** to immediately run the update inventory job, or click **Schedule** to schedule the periodic update inventory job at a later time.

Step 6 To check the status of your job, perform any one of the following :

- If you click **Run Now**, click the progress details in the progress window that appears.
- Click the **Discovery Jobs** button on the Inventory Management page.

Job Schedule - Field Descriptions

Table 42: Job Schedule - Field Descriptions

Field	Description
Start Time	Select Start Time to enter the start date and time in the yyyy/MM/dd and hh:mm AM/PM format, respectively. Alternatively, click the date picker to select the start date and time from the calendar. The displayed time is the client browser time. The scheduled periodic job runs at this specified time.
Recurrence	Select None, Hourly, Daily, Weekly, or Monthly to specify the job period.
Settings	Details of the job period.
End Time	If you do not want to specify an end date/time, click No End Date/Time . Click End at to enter the end date and time in the yyyy/MM/dd and hh:mm AM/PM format respectively.

Inventory Details Collection

Cisco Prime Collaboration Assurance supports on-demand inventory update for managed devices by collecting and updating data about the devices and the phones registered to them.

All additions, deletions, and modifications of phones, XML phones, and clusters are reflected in the inventory. There are separate inventory collection schedules for phones and clusters. For details on cluster discovery, see [Unified CM Cluster Data Discovery](#).

You cannot create additional schedules; you can only edit an existing schedule. For phones, you can create multiple inventory collection schedules.



Note

You can schedule periodic discovery of Cisco Unified CM clusters only. Phones registered with other clusters are not discovered. For more information, see [Unified CM Cluster Data Discovery](#).

As Cisco Prime Collaboration Assurance performs inventory collection of phones and Cisco Unified CM clusters, these phones and clusters pass through various device states until they are fully recognized by Cisco Prime Collaboration Assurance (see [Discovery Life Cycle](#) for details).

You can specify how often to collect information about the phones and clusters that are managed in Inventory Collection. To schedule Inventory Collection, choose **Assurance Administration**.

For Cisco Prime Collaboration Release 11.5 and later

To schedule Inventory Collection, choose **Alarm & Report Administration**.

For an overview of inventory collection tasks, see the following table.

Table 43: Overview of Inventory Collection Tasks

Task	Description
Schedule inventory collection of cluster devices	For Cisco Prime Collaboration Release 12.1 and later Inventory > Cluster Device Discovery Schedule to add, edit, or delete the cluster device discovery schedules (For more information, see Schedule Cluster Device Discovery, on page 134)

Suspend and Resume Managed Devices

You can suspend a device that is in the Managed state. After the device is moved to the Suspended state, Cisco Prime Collaboration Assurance does not monitor this device. That is, conference, endpoint, and inventory details are not updated and alarms are not triggered for this device.

The following are behaviors for a device in the Suspended state:

- If a device is in the Suspended state, Cisco Prime Collaboration Assurance does not poll the devices.
- If a suspended endpoint joins a new conference, the endpoint is shown as Unknown in the Conference Topology pane.
- If a suspended endpoint is already in an in-progress conference, the endpoint icon (in the Conference Topology pane) changes to Unknown immediately after the endpoint state is changed to Suspended.

- If Cisco Unified CM publisher is suspended, Cisco Prime Collaboration Assurance does not poll the registered endpoints that belong to that corresponding Cisco Unified CM cluster.
- If there are any active alarms, they are not cleared immediately. You can either manually clear the alarms; otherwise, they are cleared automatically after they expire (by default, in 24 hours). No new alarms are triggered for a suspended device.
- You are not allowed to Suspend CUCM devices if any background job (like endpoint sync, phone XML, and so on) is running for the current cluster.
- **For Cisco Prime Collaboration Release 11.1 and earlier**
If a suspended endpoint is already in a troubleshooting job, you cannot troubleshoot from the suspended endpoint. However, you can troubleshoot up to the suspended endpoint.
- If a device is suspended, the Endpoint Utilization report does not contain any data for this device.
- **For Cisco Prime Collaboration Release 12.1 SP2 and later**
When the TC/CE endpoint management status changes from Managed to Suspend, it should Unsubscribe.

To suspend or resume managed devices:

Step 1 Choose **Device Inventory > Inventory Management**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**

Step 2 From the Current Inventory table, select managed or suspended devices.

Step 3 Click **Suspend** or **Resume**.

Step 4 In the confirmation message box, click **OK**.

Note You cannot delete phones directly from the inventory using the delete option. Phones are deleted automatically when the clusters with which they are registered are deleted. The inventory is updated only after a rediscovery is performed.

Delete Devices

You can delete devices that are in the Unknown, Unreachable, Inaccessible, Undiscoverable, Suspended, and Unsupported states. You cannot delete devices in the Managed state.

After a device is deleted, it is not listed in the Current Inventory table, but the details are available in the Cisco Prime Collaboration Assurance server. To rediscover a deleted device, see [Rediscover Devices](#). You can access the deleted device's details as part of the past conference data.

For Cisco Prime Collaboration Release 12.1 and later

You can delete devices that are in the Unknown, Unreachable, Inaccessible, Undiscoverable, Suspended, and Unsupported states. You cannot delete devices in the Managed state.

After a device is deleted, it is not listed in the Current Inventory table.

Endpoint with old IP entry must be deleted as part of DEVICE_REMOVED feedback and new IP entry (considered as a new endpoint on VCS) must be added separately.

For Cisco Prime Collaboration Release 12.1 SP2 and later

If the TC/CE endpoint is deleted from Inventory, the HTTPS feedback subscription will be removed from the endpoint.

The following are behaviors for a device in the Deleted state:

1. You are not allowed to Delete CUCM devices if any background job (like endpoint sync, phone XML, and so on) is running for the current cluster.
2. Cisco Prime Collaboration Assurance allows only 1 delete request at a time for all concurrent sessions. If you try deleting device(s)/endpoint(s) from other sessions, a message indicating that "Concurrent delete operation is running in background, please try after sometime" appears.
3. Cisco Prime Collaboration Assurance will not keep any device information once they are removed or deleted. There is no more DELETED state for device management status.

To delete a device:

Step 1 Choose **Device Inventory > Inventory Management**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > Inventory Management**

Step 2 From the Current Inventory table, select devices to delete.

You can use the quick filter to get a list of devices in the desired state.

Step 3 Click **Delete**.

Step 4 In the confirmation message box, click **OK**.

Note You cannot delete phones directly from the inventory using the delete option. Phones are deleted automatically when the clusters with which they are registered are deleted. The inventory is updated only after a rediscovery is performed.

Troubleshooting

Issue: Unable to delete a device that is in Managed state.

Recommended Action: Ensure that you suspend the device first, and then delete the device.

Performance Graphs

Cisco Prime Collaboration Assurance enables you to select and examine changes in network performance metrics. You can select, display, and chart network performance data using real time, as well as collected data.

You can access the performance graphs through the Alarm & Events page, Device 360° view, and Diagnostic Summary pages. You can create performance graphs from the current or real-time data when:

- Voice utilization polling is enabled for devices.
- Device is in managed state.

**Note**

You can view performance graphs for voice devices (excluding phones) only. These graphs appear only for devices in managed state and for which at least one polling cycle is over.

Performance Graphing Notes

This section contains information you should be aware of when working with performance graphs.

Summary	Explanation
Cisco recommends following these guidelines for optimal performance graph viewing.	The following guidelines are recommended: <ul style="list-style-type: none"> • No more than five metrics be selected for one graph. • No more than ten graphs on the user interface. • No more than ten items selected for merge.
An MGCP gateway on a Catalyst 6000 switch. When you have all three capabilities (voice gateway, switch, and MGCP) performance graphing cannot graph all the data. Only the common metrics are available for graphing.	When graphing performance metrics for a device that has these three capabilities (voice gateway, switch, and MGCP) you will only be able to graph the common metrics. In the Event Details page you cannot graph HighUtilization events.
A voice gateway, MGCP, and H323 on a router. When you have all these capabilities on one device, each metric displays two graphs.	When graphing performance metrics for a device that has these capabilities (voice gateway, MGCP, H323, and router), each metric displays two graphs. Also, when graphing multiple devices or devices that have multiple polling intervals, the least common multiple is used to plot the x axis. Real-time graphs will refresh at this common polling interval.
Cisco Unity Express servers (CUES) graph real-time data and update in real-time. You can switch from line to bar charts and zoom in on specific data to troubleshoot and find peak utilization periods.	Ensure Cisco Prime Collaboration Assurance is collecting data and is configured properly to receive this data.

Launch a Performance Graph

The performance graphs are available through the following:

- Device 360 degree View - Click on the Launch Tools icon, and then click on Performance Graph.
- Event Details page

- Diagnostics views - UCM Cluster Call Usage Summary in Server and Cluster views, UCM Resource Utilization Summary and UCM Cluster Location Summary in Cluster view, and trunk utilization can be accessed through the UCM Resource Utilization Summary portlet. in the Cluster view.

Before you Begin

- Verify that Cisco Prime Collaboration Assurance is monitoring the devices for which you want to collect utilization statistics. This includes the Cisco Unified Communications Manager that the ports are registered to.
- Verify that voice utilization polling settings are enabled. Cisco Prime Collaboration Assurance uses the statistics gathered during voice utilization polling for charting network performance.
- Review the Performance Graphing Notes.

Performance Graph Window

Performance graphs provide real-time information and historical information.

When you launch a performance graph, one line graph is displayed for each metric that you select. Each line graph contains 16 data points displayed in real time. The following table provides details on the data options.

Graph Data Option	Description
Real Time	When you launch a performance graph, it shows real time data by default.
Hourly Average	When you select Hourly Average, the performance graph shows average data for the hour.
Hourly Max	When you select Hourly Max, the performance graph shows peak data for the hour.
Hourly Min	When you select Hourly Min, the performance graph shows minimum data for the hour.
History	When you select History, the performance graph shows hourly average data for seven days.
All	Displays all data. Graphs display up to a maximum of 130 points. If data ranges in the Zoom/Pan view contain more than 130 points, then Cisco Prime Collaboration Assurance selects points at regular intervals and plots them in the graph.

Troubleshooting Performance Graphs

This section contains information that will help you if you encounter problems generating performance graphs. If you encounter an error, it will likely appear either when you select Performance Graphing from the menu, or when Cisco Prime Collaboration Assurance is checking for the data file to graph. In the first case (when selecting Performance Graphing), you will see an error message that describes the problem and an action to take. The following table describes the errors and their possible causes, for both of these types of cases.

Error	Possible Causes
Cannot collect data	<ul style="list-style-type: none"> Account and credentials are not the same on all Cisco Unified Communications Managers in the cluster. HTTP server problems: <ul style="list-style-type: none"> HTTP server on the device is down. HTTP server is operational, but the Cisco Unified Communications Manager is down. Device unreachable because of a network problem. For Cisco Prime Collaboration Release 11.1 and earlier Performance Monitor process on the media server is down. The Cisco Unified Communications Manager that the MGCP gateway is registered to, is not in Cisco Prime Collaboration Assurance Inventory. Device capability is not supported. Performance graphing supports the following: Cisco Unity, Cisco Unity Express, Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, H.323 devices, and Voice Mail Gateways. Device is suspended or deleted. Device platform is not support. <p>For a list of supported devices, see Supported Devices for Cisco Prime Collaboration Assurance.</p>
Cannot collect data because of the following: <ul style="list-style-type: none"> The username or password for the device is empty. The system has the wrong credentials for the device. The device does not have credential information. 	<ul style="list-style-type: none"> No credentials in Cisco Prime Collaboration Assurance. Incorrect credentials in Cisco Prime Collaboration Assurance. <p>To add credentials, see Adding a Device Credential Profile.</p>

Error	Possible Causes
<p>Cannot collect data from the device because of the following:</p> <ul style="list-style-type: none"> • A processing error occurred. • Parsing or processing errors occurred. • Internal initialization errors occurred. • Initialization problems occurred in the device data collector. 	<p>Incorrect Cisco Unified Communications Manager version. Check the following:</p> <ul style="list-style-type: none"> • The version of the Cisco Unified Communications Manager that is running on the device. • The Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance. • If the Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance is incorrect, add the device again. <p>For a list of supported devices, see Supported Devices for Cisco Prime Collaboration Assurance.</p>
<p>Cannot collect data from the device. The certificate hostname/IP Address cannot be mapped to the URL hostname/IP Address.</p>	<p>The device is not in DNS.</p>
<p>Incomplete data collected because an error occurred in communicating with the device.</p>	<p>Incorrect Cisco Unified Communications Manager version. Check the following:</p> <ul style="list-style-type: none"> • The version of the Cisco Unified Communications Manager that is running on the device. • The Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance. • If the Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance is incorrect, add the device again. <p>For a list of supported devices, see Supported Devices for Cisco Prime Collaboration Assurance.</p>
<p>Cannot collect data because of the following:</p> <ul style="list-style-type: none"> • The device returned no data from a required MIB. • The device received no MIB data. 	<ul style="list-style-type: none"> • No data from a required MIB. • A required MIB is not populated on the device. • No MIBs returned data. • Device is unreachable due to a network problem. • Device credentials do not contain a valid SNMP community read string. • SNMP response slow; data collection timed out.

Error	Possible Causes
<ul style="list-style-type: none"> The rate of queries on the Cisco Unified Communications Manager exceeds the limit. An error has occurred in the data processing stage. 	<p>Too many queries on a Cisco Unified CM 6.0 or later.</p> <p>Check the polling settings; they should not be less than three minutes.</p>
<ul style="list-style-type: none"> The Cisco Unified Communications Manager did not have enough time to handle the query requests. An error has occurred in the data processing stage. 	<p>Query exceeded time limit on Cisco Unified CM 6.0 or later.</p>
Cisco Unity or Unity Express trunk utilization graphs are not working.	Cisco Prime Collaboration Assurance must be configured properly using the maximum capacity.

When working with performance graphs, remember the following:

- If you are not able to collect performance data and you do not see an error message (either a popup message or a message in the log file) indicating the problem, you should verify the status of the device. To do so, use the View/Rediscover/Delete Devices page. If the device is in the Unreachable state, verify that the device's credentials are correct and rediscover the device.
- If a gray line or a gray area appears in a graph, hover your mouse over it to obtain a tool tip with an explanation.

Unified CM Device Search

You can search for devices within a cluster, based on the search criteria you specify.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, search results depend on the global customer selection.

For Cisco Prime Collaboration Release 11.5 and later

To perform a device search, go to **Inventory > UC Device Search**. You can view the devices based on the saved search criteria you select from the Saved Search drop-down list.



Note The table displays only 200 entries. Therefore, we recommend that you use the filter criteria to the best use to ensure that you get the desired result.

To create a new search criteria:

Step 1 For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > UC Device Search**.

Step 2 Select the Cluster from **Cluster** drop-down list.

You can also search for a device in the Cluster drop-down list.

Step 3 Click **New Search**.

Step 4 Enter the Criteria Name, Device Type, and Polling Interval

If you choose the devices only configured in the DB option, you cannot specify the polling interval or the other parameters, except the device type. This option displays the devices in the Unknown state.

The same user cannot use the same search criteria name for the same cluster. The same user can have the criteria name for a different cluster.

Step 5 For Custom Search, specify the status within call Manager, Device Model, and the Search with Name parameters.

The search criteria available vary based on the device type you chose.

Step 6 Click **Search**.

The search results are displayed in the page. The results get refreshed based on the polling interval you specify. You can launch the Unified CM from the IP address link available in the IP Address column.

The search results also provides the following information:

- App Info— The information about the application.
- Configuration— This applies to H.323 Gateways.
- Port/Channel Status— Shows all the configured port or channels and their status. You can set the polling interval to refresh this view.

This search does not get saved in the database and cannot be retrieved after you log out, unless you save the search. To save the search, click the **Save** icon.

You can also edit a search that you had saved. You can delete a search that you had created, even if it is unsaved. Use the edit or delete icon to edit/delete the search. Fields that you cannot edit are disabled.

You can also view the destination status for SIP trunks. Select **SIP Trunk** from the Device Type drop-down list, enter the Criteria Name, Polling Interval and click **Search**. Hover your mouse over the **Name** column and click the quick view icon to launch the Destination Details pop-up window.

Note If you want to save the search criteria in Internet Explorer 10 or 11, you must enable Always Refresh from Server option in the browser. To enable this option, press the F12. In the Internet Explorer tool bar menu, choose **Cache > Always refresh from server**.

SNMP Query

The SNMP query feature helps you to troubleshoot devices in your network.

You should perform SNMP query when:

- Devices in your network do not get into a managed state in Cisco Prime Collaboration Assurance.
- Devices in your network are not listed in Inventory Management.
- SNMP Polling is not happening successfully.

Prerequisite - Devices should be supported by Cisco Prime Collaboration Assurance.

For a list of supported devices, see [Supported Devices for Cisco Prime Collaboration Assurance](#).

To perform SNMP query:

1. Choose **Device Inventory > SNMP MIB Query Tool**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory > SNMP MIB Query Tool**.

2. Enter the IP Address, select and OID type from the OID drop-down list, and then do one of the following:

- Click the GET button - To know the return value of a particular OID. For example to know the Interface Name or Interface Status.

Credentials are required to perform this task. If the device information is available in the Cisco Prime Collaboration database, the details are auto-populated on the screen. Otherwise, check the Enter the Credentials check box, select an SNMP version from the version drop-down list, and enter the details on the fields that appear.

- Click the Walk button - To get detailed information on the MIB of that device.

Credentials are required to perform this task. If the device information is available in the Cisco Prime Collaboration database, the details are auto-populated on the screen. Otherwise, check the Enter the Credentials check box, select an SNMP version from the version drop-down list, and enter the details on the fields that appear.

The information about the IOD appears as a table on the page.

Troubleshooting - SNMP credentials are not auto populated when:

- Discovery is not completed so credentials may not have been added in the Cisco Prime Collaboration database yet.
- If device is in Unknown or Inaccessible state in Inventory Management.
- SNMP Credentials have not been configured on the device.



CHAPTER 15

Poll Devices

This section explains the following:

- [Poll Settings, on page 189](#)
- [Overview, on page 189](#)
- [Polling Parameters— Settings, on page 191](#)
- [View Polling Parameters, on page 191](#)
- [Edit Polling Parameters, on page 191](#)

Poll Settings

This section explains the settings used to poll devices.

Overview

Polling devices at regular intervals help you detect devices and check their health. Managed network devices are polled periodically to synchronize the device data with the Cisco Prime Collaboration Assurance database.

Cisco Prime Collaboration Assurance polls devices to:

- Check whether the devices are reachable
- Check whether the devices are up and running
- Display up-to-date device data

You can define polling values for groups. Devices can belong to system-defined or user-defined groups. Devices can belong to multiple groups, and can have specific polling settings.



Note

You cannot create a group in the Polling Parameters page. Groups are synchronized from default Device Groups. See [Device Group Selector](#) for more information.

Cisco Prime Collaboration Assurance is configured with default settings for polling parameters. You can use the defaults, edit them, or restore them at any time. Depending on how important a device group is, you can increase or decrease the polling interval to do either of the following:

- Minimize the impact on the polled devices
- Enhance the resolution of the collected data

When Cisco Prime Collaboration Assurance polls devices, it receives data on the following parameters:

Environment Settings

Enables you to poll data for device power supply, fan, voltage, and temperature sensor.

Interface Settings

Enables you to poll data for device interfaces and ports; for example, device communication over HTTP.

Data polling from interfaces and ports are controlled at the device level; that is switches have a specific polling setting, and this setting determines when the switch ports are polled.

System Settings

Enables you to poll data for device availability, processor, CPU, and memory utilization.

Utilization

Enables you collect performance and capacity planning data that is used to view Performance Graphs.

You can access the performance graphs through the Alarms & Events page, Device 360 degree view, and Diagnostics Summary pages.

Application Settings

Enables you to poll data for device connectivity, system status, and call quality.

Service Settings

Service settings provide data for service issues, such as cluster connectivity and telephony configurations.

The polling parameters vary based on the device type that you select.

If you do not want to poll any specific data, you can disable the polling settings using the Disable option.

Recommendations:

• For Cisco Prime Collaboration Release 11.1 and earlier

You can customize the polling interval for the parameters based on your business needs. However we recommend that you select the **Use Best Practice** labeled polling interval. For each of the polling setting, you can also view the associated events when there is a threshold violation (**Assurance Administration > Event Customization > System**). For description and device type, see the [Supported Alarms and Events for Prime Collaboration Assurance](#) page.

For Cisco Prime Collaboration Release 11.5 and later

You can customize the polling interval for the parameters based on your business needs. However we recommend that you select the **Use Best Practice** labeled polling interval. For each of the polling setting, you can also view the associated events when there is a threshold violation (**Alarm & Report Administration > Event Customization > System**). For event description and device type, see the [Supported Alarms and Events for Prime Collaboration Assurance](#) page.

- The default polling interval is set to 4 minutes, however you can set it to 1 minute also. We recommend that you set the polling interval to 1 minute for a few critical devices only. Setting the polling interval to 1 minute for all devices has an impact on the performance adversely.
- If you do not want to poll any specific data, you can disable the polling settings using the Disable option.

Polling Parameters— Settings

When you change the polling parameter settings, the changes are applied for the entire group and not just the device. Polling Parameters are displayed in page, when you select a Device Group.

From the Polling Parameters page, you can perform any of the following tasks:

- [View Polling Parameters](#)
- [Edit Polling Parameters](#)

View Polling Parameters

When you view polling settings for a device group, you can see the devices that are members of the device group, and you can see the default and current values for the polling parameters.

To view polling parameters:

-
- | | |
|---------------|--|
| Step 1 | Choose Assurance Administration > Polling Settings .
For Cisco Prime Collaboration Release 11.5 and later
Choose Alarm & Report Administration > Polling Settings |
| Step 2 | Select a Device Group for which you can set polling parameters. (Generally, this is a device group that does not contain subgroups.) |
| Step 3 | When you are done viewing the polling parameters, close the window. |
-

Edit Polling Parameters

When you edit Cisco Prime Collaboration Assurance polling parameters, you edit settings that are associated with device groups, not with individual devices. When you have finished all changes to polling parameters (and thresholds and priorities), apply all changes.

To edit polling parameters:

-
- | | |
|---------------|--|
| Step 1 | Choose Polling Settings .
For Cisco Prime Collaboration Release 11.5 and later
Choose Alarm & Report Administration > Polling Settings . |
| Step 2 | Select a device group for which you can set polling parameters. (Generally, this is a device group that does not contain subgroups.) |
| Step 3 | Select the polling parameter that you want to edit, choose the appropriate value from the Polling Interval drop-down, and click Enable . |
| Step 4 | Repeat the following for each parameter that you want to edit: |

- a) Select a parameter type.
- b) Change the parameters appropriately for each setting.

Step 5 Click Save. Your changes will not go into effect until you apply them.

Step 6 When a confirmation dialog box appears, click **OK**.



PART **IV**

Monitor Faults

- [Configure Notifications, on page 195](#)
- [Set Threshold Rules, on page 213](#)
- [Monitor Alarms and Events, on page 229](#)



CHAPTER 16

Configure Notifications

This section explains the following:

- [Configure Notifications, on page 195](#)
- [Notification Groups, on page 196](#)
- [Notification Criteria, on page 197](#)
- [Types of Notifications, on page 197](#)
- [SNMP Trap Notifications, on page 199](#)
- [Configure SMTP Server, on page 205](#)
- [Syslog Notifications, on page 206](#)
- [Notifications Limited to Specific Alarms, on page 207](#)

Configure Notifications

Cisco Prime Collaboration Assurance displays event and alarm information in response to events that occur in the IP Telephony and TelePresence environment and the IP fabric.

You can view events and alarms on Cisco Prime Collaboration Assurance dashboards, such as the alarms and events browser. In addition, you can configure notifications to forward information about events to SNMP trap collectors on other hosts, syslog collectors, and users.

Notifications monitor events on device roles, not on device components. For a list of supported events and alarms, see [Supported Alarms and Events for Prime Collaboration](#).

For each alarm, Cisco Prime Collaboration Assurance compares the alarms, devices, severity, and state against the configured notification groups and sends a notification when there is a match. Matches can be determined by user-configured alarm sets and notification criteria. The procedure for configuring notification criteria is described in [Add a Device Notification Group](#).

The following table lists values for severity and explains how the state of an alarm changes over time.



Note You can change the event severity sent in notifications from the Cisco Prime Collaboration Assurance default value to a user-defined value.

This table describes the alarm and event severity and status.

Table 44: Alarm and Event Severity and Status

Events	Alarms
Severity	
<ul style="list-style-type: none"> • Critical. • Major • Minor • Warning. • Informational - If any event is cleared, its severity changes to informational. Some events, by default, have severity as Informational. 	<ul style="list-style-type: none"> • Critical • Major • Minor • Warning • Cleared
Status	
<ul style="list-style-type: none"> • Active - The event is live. • Cleared - The event is no longer active. 	<ul style="list-style-type: none"> • Acknowledged - A user has manually acknowledged the alarm. A user can acknowledge only active events. • Cleared - The alarm is no longer active. • Active - The alarm is live. • User Cleared

Notification Groups

A notification group is a user-defined set of rules for generating and sending notifications.

The following table describes the contents of a notification group.

Table 45: Notification Groups

Item	Description
Notification criterion	A named set of reasons to generate a notification.
Notification type	The type of notification to send: SNMP trap, e-mail, or syslog.

Item	Description
Notification recipients	Hostnames and ports for systems that listen for SNMP traps, syslog messages, or e-mail addresses.
Daily subscription activity period	The hours during which Cisco Prime Collaboration Assurance should use this subscription while monitoring the events for which to send notifications.

Notification Criteria

Notification criteria define what you want to monitor for the purpose of sending notifications. A notification criterion is a user-defined, named set of devices or phones, and events of a particular severity and status. You must specify notification criteria to configure a notification group.

Cisco Prime Collaboration Assurance supports device-based notification criterion. The following table describes the device-based notification criterion.

Table 46: Notification Criterion

Item	Description
Devices	The devices, device groups, or clusters that you want to monitor.
Alarm sets	(Optional). One or more groups of alarms that you want to monitor. See Notifications Limited to Specific Alarms .
Alarm severity and status	One or more alarm severity levels and status.

You can also customize the names and severity of the [Notifications Limited to Specific Alarms](#) device-based events displayed by Notifications.

Types of Notifications

Cisco Prime Collaboration Assurance provides three types of notification: SNMP trap, e-mail, and syslog. When you configure a notification group, you specify one or more types of notification to send and you must also specify recipients for each type of notification.

The following table describes the types of notification.

Table 47: Notification Types

Type	Description
SNMP Trap Notifications	<p>Cisco Prime Collaboration Assurance generate traps for alarms and events and sends notifications to the trap receiver. These traps are based on events and alarms that are generated by the Cisco Prime Collaboration Assurance server.</p> <p>CISCO-EPM-NOTIFICATION-MIB defines the trap message format.</p> <p>Using SNMP trap notification is different from forwarding raw traps to another server before they have been processed by Cisco Prime Collaboration Assurance.</p> <p>Note Cisco Prime Collaboration Assurance supports SNMP version 1 (SNMPv1) and SNMPv2 traps for polling and receiving. Cisco Prime Collaboration Assurance forwards traps as SNMPv2 traps. However, trap processing with SNMPv3 is not supported in Cisco Prime Collaboration Assurance.</p> <p>See SNMP Trap Notifications for details on mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration Assurance for alarms and events.</p>
E-Mail Notifications	<p>Cisco Prime Collaboration Assurance generates e-mail messages containing information about the alarms. When you create an e-mail subscription, you can choose whether to include the subject line only or the complete e-mail message.</p> <p>Note If you have installed Cisco Prime Collaboration Assurance in Enterprise mode, you will get an email notification with the subject line in the following format:</p>
<p><i>[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY.</i></p> <p>For example: <i>[PC-ALERT-#CPCM-Ent-Cluster#]50.0.50.230:Gatekeeper Registration Failure:CRITICAL</i></p> <p>If the Cluster name or Device IP is not available, it can be left empty.</p>	
	<p>In a NAT environment, the Private IP Address of the device is also displayed.</p> <p>If you have installed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to.</p>

Type	Description
Syslog Notifications	<p>Cisco Prime Collaboration Assurance generates syslog messages for alarms that can be forwarded to syslog daemons on remote systems.</p> <p>In a NAT environment, the Private IP Address of the device is also displayed.</p> <p>If you have installed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to.</p> <p>See Syslog Notifications for sample syslog messages and description.</p>

SNMP Trap Notifications

When an alarm or an event is received in the Cisco Prime Collaboration Assurance server, it is converted to the trap format defined in the CISCO-EPM-NOTIFICATION-MIB. Other MIB objects are not supported. All the trap receivers receive the same traps in same trap format.

The CISCO-EPM-NOTIFICATION-MIB can be downloaded from [Cisco.com](#).

The table below describes the mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration Assurance for alarms.

Table 48: CISCO-EPM-NOTIFICATION-MIB Summary for Alarms

Trap Field Name	OID	Type	Prime Collaboration Alarm	Content as in Trap Forwarder (EPM MIB)
cenAlarmIndex	1.3.6.1.4.1.9.9.311.1.1.2.1.1	Unsigned32	-	MIB index
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdmin String	-	<p>The version of this MIB. The version string will be of the form <i>major version . minor version</i> .</p> <p>Note Always set to 9.0</p>
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	Timestamp	Timestamp	The time when the alarm was triggered.
cenAlarmUpdated Timestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Timestamp	lastmodified timestamp	The last time when the alarm was modified.
cenAlarmInstanceId	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdmin String	ID	The unique alarm ID generated by Cisco Prime Collaboration Assurance.

cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32	lastcleartime	Indicates whether the alarm is active (1) or cleared (2)
cenAlarmStatus Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdmin String	lastcleartime	A short description of the status of the alarm: <ul style="list-style-type: none"> • 1-Active • 2-Cleared
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Integer	-	The alarm type is direct (2).
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32	category	The alarm categories. It is represented as an integer value.
cenAlarmCategory Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	SnmpAdmin String	category	This is a string representation of AlarmCategory (number,description): <ul style="list-style-type: none"> • 3,Endpoint-Hardware alarms (peripheral errors) in all endpoints. • 4,Network Devices-Hardware alarms (interface errors) in all network devices. • 5,Service Infrastructure-Alarms in call and conference control (Cisco Unified CM and VCS), management (TMS), multipoint switches (CTMS), and multipoint control units (TPS, MCU). • 6,Conference-Endpoints alarms (that are part of the conference) and network alarms (jitter, latency, or drop).
cenAlarmServer AddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	InetAddress Type	-	The type of Internet address at which the server that is generating this trap, is reachable. This value is set to 1 for IPv4 management.
cenAlarmServer Address	1.3.6.1.4.1.9.9.311.1.1.2.1.12	InetAddress	-	Cisco Prime Collaboration Assurance IP address.

cenAlarmManaged ObjectClass	1.3.6.1.4.1.99.311.1.1.2.1.13	SnmpAdmin String	Source	Entity type of the source, such as Cisco VCS and so on.
cenAlarmManaged ObjectAddressType	1.3.6.1.4.1.99.311.1.1.2.1.14	InetAddress Type	Source	The type of Internet address at which the managed device is reachable. This value is set to 1 for IPv4 management.
cenAlarmManaged ObjectAddress	1.3.6.1.4.1.99.311.1.1.2.1.15	InetAddress	Source	IP Address of the managed object.
cenAlarmDescription	1.3.6.1.4.1.99.311.1.1.2.1.16	OctetString	Description	A detailed description of the alarm.
cenAlarmSeverity	1.3.6.1.4.1.99.311.1.1.2.1.17	Integer32	Severity	Indicates the severity of the alarm using an integer value. The valid integers are 0 - 7.
cenAlarmSeverity Definition	1.3.6.1.4.1.99.311.1.1.2.1.18	OctetString	Severity	Alarm severity string representation (number,description): <ul style="list-style-type: none"> • 0,critical • 1,major • 2,minor • 3,warning • 4,info • 5,normal • 6,unknown • 7,cleared
cenAlarmTriageValue	1.3.6.1.4.1.99.311.1.1.2.1.19	Integer32	-	Not used.
cenEventIDList	1.3.6.1.4.1.99.311.1.1.2.1.20	OctetString	-	List of event IDs that led to this alarm.
cenUserMessage1	1.3.6.1.4.1.99.311.1.1.2.1.21	SnmpAdmin String	isacknowledged	Indicates whether the alarm is acknowledged or unacknowledged.

cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	SnmpAdmin String	previous Severity	Previous severity of the alarm. For example, assume that while the conference was in-progress, a major alarm was triggered. After the conference is complete, the conference alarm is automatically Cleared. The alarm severity displays Major because the previous alarm severity for this conference was Major.
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	SnmpAdmin String	-	Not used.
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	Integer	-	2-alert. Indicates this trap is either an alarm or event notification.
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unsigned32	-	Not used.
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	SnmpAdmin String	-	Not used.
cenCustomer Identification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	SnmpAdmin String	ownerid	In the Enterprise mode, the Customer Identification details entered in the Cisco Prime Collaboration Assurance notification user interface is displayed. In the MSP mode, the customer name will be displayed.
cenCustomer Revision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	SnmpAdmin String	-	Not used.
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	SnmpAdmin String	id	The Unique alarm ID assigned by Cisco Prime Collaboration Assurance. See the Cisco Prime Collaboration Assurance Supported Alarms and Events table for the assigned alarm IDs.

The following table describes the mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration Assurance for events.

Table 49: CISCO-EPM-NOTIFICATION-MIB Summary for Events

Trap Field Name	OID	Type	Prime Collaboration Event	Content as in Trap Forwarder (EPM MIB)
cenAlarmIndex	136.14.199311.1.12.1.1	Unsigned32	-	MIB index
cenAlarmVersion	136.14.199311.1.12.1.2	SnmpAdmin String	-	The version of this MIB. The version string will be of the form <i>major version . minor version</i> . Note Always set to 9.0
cenAlarmTimestamp	136.14.199311.1.12.1.3	Timestamp	Timestamp	The time when the event was triggered.
cenAlarmUpdateTimestamp	136.14.199311.1.12.1.4	Timestamp	-	Not used.
cenAlarmInstanceID	136.14.199311.1.12.1.5	SnmpAdmin String	ID	The unique event ID generated by Cisco Prime Collaboration Assurance.
cenAlarmStatus	136.14.199311.1.12.1.6	Integer32	-	Not used.
cenAlarmStatus Definition	136.14.199311.1.12.1.7	SnmpAdmin String	-	Not used.
cenAlarmType	136.14.199311.1.12.1.8	Integer	-	The event type is direct (2).
cenAlarmCategory	136.14.199311.1.12.1.9	Integer32	category	The event categories. It is represented as an integer value.

cenAlarmCategory Definition	136.14.1.99311.1.12.1.10	SnmpAdmin String	category	<p>This is a string representation of AlarmCategory (number,description):</p> <ul style="list-style-type: none"> • 3,Endpoint-Hardware events (peripheral errors) in all endpoints. • 4,Network Devices-Hardware events (interface errors) in all network devices. • 5,Service Infrastructure-events in call and conference control (Cisco Unified CM and VCS), management (TMS), multipoint switches (CTMS), and multipoint control units (TPS, MCU). • 6,Conference-Endpoints events (that are part of the conference) and network events (jitter, latency, or drop).
cenAlarmServer AddressType	136.14.1.99311.1.12.1.11	InetAddress Type	-	The type of Internet address at which the server that is generating this trap, is reachable. This value is set to 1 for IPv4 management.
cenAlarmServer Address	136.14.1.99311.1.12.1.12	InetAddress	-	Prime Collaboration IP address.
cenAlarmManaged ObjectClass	136.14.1.99311.1.12.1.13	SnmpAdmin String	Source	Entity type of the source, such as CTS, Cisco VCS, and so on.
cenAlarmManaged ObjectAddressType	136.14.1.99311.1.12.1.14	InetAddress Type	Source	The type of Internet address at which the managed device is reachable. This value is set to 1 for IPv4 management.

cenAlarmManagedObjectAddress	136.14.199311.1.121.15	InetAddress	Source	IP Address of the managed object.
cenAlarmDescription	136.14.199311.1.121.16	OctetString	Description	A detailed description of the event.
cenAlarmSeverity	136.14.199311.1.121.17	Integer32	Severity	Indicates the severity of the event using an integer value. The valid integers are 0 - 7.
cenAlarmSeverityDefinition	136.14.199311.1.121.18	OctetString	Severity	Alarm severity string representation (number, description): <ul style="list-style-type: none"> • 0,critical • 1,major • 2,minor • 3,warning • 4,info • 5,normal • 6,unknown • 7,cleared
cenAlarmTriageValue	136.14.199311.1.121.19	Integer32	-	Not used.
cenEventIDList	136.14.199311.1.121.20	OctetString	-	Not used.
cenUserMessage1	136.14.199311.1.121.21	SnmpAdmin String	-	Not used.
cenUserMessage2	136.14.199311.1.121.22	SnmpAdmin String	-	Not used.
cenUserMessage3	136.14.199311.1.121.23	SnmpAdmin String	-	Not used.
cenAlarmMode	136.14.199311.1.121.24	Integer	-	3-event. Indicates this trap is either an alarm or event notification.
cenPartitionNumber	136.14.199311.1.121.25	Unsigned32	-	Not used.
cenPartitionName	136.14.199311.1.121.26	SnmpAdmin String	-	Not used.
cenCustomerIdentification	136.14.199311.1.121.27	SnmpAdmin String	-	Not used.
cenCustomerRevision	136.14.199311.1.121.28	SnmpAdmin String	-	Not used.
cenAlertID	136.14.199311.1.121.29	SnmpAdmin String	-	Not used.

Configure SMTP Server

You can configure the SMTP server to send and receive e-mail notifications for alarms by specifying the SMTP server name and the sender AAA E-mail address on the **E-mail Setup for Alarms & Events** page (**Alarm & Report Administration > E-mail Setup for Alarms & Events**). The value in the **Sender AAA E-mail Address** field helps you to identify the server you receive the e-mail from, in case of many servers.

Syslog Notifications

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

The following is a sample syslog message generated by the Cisco Prime Collaboration Assurance server for an alarm.

```
Local7.Emerg      10.78.110.27      Feb 19 14:42:49 pcollab-44798 pcollab-44798:
%local7-0-ALARM: 14$Description=Device temperature or voltage is outside the normal operating
range.
When an OutofRange event is generated, you will normally also see fan, power supply, or
temperature
events.::Status=1,active^Severity=critical^Acknowledged=no^AlarmURL=https://10.78.110.27/emsam/index.html
#pageId=com_cisco_ifm_web_page_alarms&queryParams=Id%3D84837&forceLoad=true^Device Work
Center=
https://10.78.110.27/emsam/index.html#pageId=com_cisco_emsam_page_inventory&deviceId=3681728
^CUSTOMER=customer2^CUSTREV=2,324^Default Alarm Name=OutofRange^Managed Object=150.50.3.2
^Managed Object Type=Router^MODE=2;Alarm ID=84837^Component=150.50.3.2/8<000><000>
```

This table describes the syslog notification parameters based on the above example:

Table 50: Syslog Notification Description

Parameter	Description
Local7.Emerg 10.78.110.27 Feb 19 14:42:49 pcollab-44798 pcollab-44798	IP address and hostname of the Cisco Prime Collaboration Assurance server where the syslog is generated
%local7-0-ALARM	<ul style="list-style-type: none"> Syslog Facility data: %local7 Severity: 0-Critical, 1-Major, 2-Minor, and 3-Warning Type is Alarm
14	Calendar year
Description	Alarm description
Status=1,active	Status of alarm; where 1 is active and 2 is cleared
Severity	Severity of alarm
Acknowledged	Indicates whether alarm is acknowledged or not
AlarmURL	URL to launch the Alarm page
Inventory Management	URL to launch the Inventory Management page
CONFERENCEDIAGNOSTICS	URL to launch Conference Diagnostics page, if it is a conferencealarm
CUSTOMER	Customer ID defined while configuring the notification

Parameter	Description
CUSTREV	Customer revision defined while configuring the notification
Default Alarm Name	Alarm name
Managed Object	IP address or hostname of the device, where an alarm is raised
Managed Object Type	Device type, such as router, endpoint and so on
MODE	Indicates if the syslog message is an alarm (2)
Alarm ID	Unique ID for alarm
Component	Device component where the alarm is raised

Notifications Limited to Specific Alarms

In some cases, you might want to send notifications for only a subset of the alarms that Cisco Prime Collaboration Assurance monitors. You can set the alarm that are of interest to you when you define the notification criterion:

- Specify an alarm set for a device-based notification criterion. You can create as many alarm sets as you would like.

You can use alarm sets to:

- Limit the number of alarm that Cisco Prime Collaboration Assurance notification monitors. When you do not use alarm sets, Cisco Prime Collaboration Assurance notification monitors all alarms to determine whether to send a notification.
- Aggregate the notifications that you want to send to different destinations. For example, you can create separate alarm sets for each of the following purposes:
 - Limit the amount of e-mail notification sent to specific individuals or departments to only those for certain alarms.
 - Write all occurrences of particular alarm to syslog.
 - Send SNMP traps when certain alarms occur.

When you create device-based notification criteria, you must include an alarm set as one of the criteria. The default alarm set, All, includes all alarms.

Add an Alarm Set

You can create alarm sets for which you can set up notifications.

To add and edit an Alarm set:

Step 1 Choose **Notification Setup**.
For Cisco Prime Collaboration Release 11.5 and later
 Choose **Alarm & Report Administration > Notification Setup**

Step 2 Click **Custom Notification** and enter the details.

Note When you create an alarm set that has several alarms, you might need to use multiple search criteria. In such situations, you need to use the Advanced Filtering option to enter multiple search criteria using the + icon, with Match selection as Any. The Quick Filter option might not work as desired.

Note When you add more alarms to an existing alarm set, do not use filter to search for alarms as filtering overwrites the original set of alarms.

Step 3 Click **Add** and provide the necessary information

Step 4 Click **Save** to save your changes.

Add a Device Notification Group

Perform the following procedure to add and edit device notification groups.



Note You can use existing notification groups as templates for creating new notification groups.

Step 1 Choose **Notification Setup**, then select the **Custom Notification**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration > Notification Setup**, then select the **Custom Notification**.

Step 2 Click **Add** to add a new criterion.

Step 3 In The New Device-Based Criterion wizard add the information on the Define General Information page:

Based on your mode of deployment, you can create domain-specific or customer-specific device notification groups. In the New Device-Based Criterion wizard, enter the required details and select a domain from the Associate to Domain drop-down list or a customer from the Customer drop-down list.

Note The Super administrator has access to all domains and can create notification groups for a domain or all the domains.

Step 4 Click **Next**.

The Select Devices/Device Groups pane is displayed.

If you check the check box for New devices that are added to all the groups should automatically be a part of the group, the devices that are added to or deleted from Cisco Prime Collaboration Assurance, are also added to or deleted from the notification criterion. This happens when the notification criterion includes a device group that the devices belong to.

Uncheck to maintain a static list of devices for any device groups included in the notifications criterion.

Step 5 Click **Add**.

Step 6 In the Select Device/Device Groups window, click **Include all Devices** or **Select Devices** radio button.

If you select the **Include all Devices** option, expand device group folders and select one or more devices, device groups, or clusters.

If you select the **Select Devices** option, expand device group folders and select check boxes for one or more devices, device groups, or clusters.

Note If you want to add cluster level email notification, you must select the cluster ID from the list of all the nodes in the cluster and cluster ID listed under **Infrastructure > UCM Clusters** device group folder.

If you select a device group, the notification criterion stays up-to-date when devices are added or deleted from Cisco Prime Collaboration Assurance *only* if you also select the Include updates to the group membership check box. New devices that are added to all the groups should automatically be a part of the group

Step 7 Click **Next**.

Step 8 In the Set up Destination pane, add the required information.

Step 9 Click **Next**.

Step 10 Review the information in the summary, then click **Save**.

After you save the device notification group, the details that you entered in the New Device-Based Criterion wizard is displayed on the Assurance Notification Criteria page. Customer column depicts the customer to which the notification group belongs.

General Information Field Descriptions

This table describes the fields in the General Information window.

Table 51: Add General Information

Graphical User Interface Element	Description
Criterion Name field	Enter a name for the notification criterion.
Customer Identification field	<p>Enter any desired identifying information. If you leave this field empty, it remains blank in e-mail and syslog notifications.</p> <p>In SNMP trap notifications, it is displayed as follows:</p> <p>Customer ID: -</p>
Customer Revision field	<p>Enter any desired identifying information. If you leave this field blank, it remains blank in e-mail and syslog notifications.</p> <p>In SNMP trap notifications, it is displayed as follows:</p> <p>Customer Revision: *</p>

Graphical User Interface Element	Description
Alarm Set Type list box	Choose one.
Alarm Severity check boxes	Check none, one, or more of the following: <ul style="list-style-type: none"> • Critical. • Major • Minor • Warning
Alarm Status check boxes	Check none, one, or more of the following: <ul style="list-style-type: none"> • Active. • Acknowledged. • Cleared. • User Cleared
OperationInterval	<p>Click the Always radio button to schedules the notification group to always be active.</p> <p>Choose the hours of the day during which you want this notification group to be active:</p> <ul style="list-style-type: none"> • From: HH:MM—Choose hour and minute that the subscription becomes active. • To: HH:MM—Choose the last hour and minute during which the subscription is active. <p>By default, the values are from 00:00 to 00:00 and the subscription is active for 24 hours.</p> <p>Use this field, for example, to send e-mail notifications during one shift and not during another.</p>

Set up Destinations Field Descriptions

This table describes the fields in the Set up Destinations page.

Table 52: Set Up Destination

Graphical User Interface Element	Description
Include Link to Notification Details check box	<p>Check to include URLs in the notification from which users can directly open the relevant page in Cisco Prime Collaboration Assurance for more information.</p> <p>Uncheck to omit URLs from notifications.</p>

Graphical User Interface Element	Description
Subscription Type radio buttons	<p>Click one at a time to enter data for each subscription type that you want to include in this subscription:</p> <ul style="list-style-type: none"> • Trap—Enter data in the Trap Subscription Type fields. • E-Mail—Enter data in the E-Mail Subscription Type fields. • Syslog—Enter data in the Syslog Subscription Type fields. <p>Cisco Prime Collaboration Assurance does not save the data you enter until you click Finish on the Subscription: Summary page. To go to the Subscription: Summary page, click Next.</p>
Trap Subscription Type fields	
IP Address/Fully Qualified Domain Name editable column	Enter an IP address or Fully Qualified Domain Name (FQDN) of the host.
Port editable column	Enter a port number on which the host can receive traps. A valid port value is a number from 0 to 65,535. You can enter the default port number value 162.
Comments editable column	(Optional) Enter a comment.
E-Mail Subscription Type fields	
SMTP Server field	<p>Enter a fully qualified DNS name or IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.)</p> <p>To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button.</p> <p>For instructions on how to configure a default SMTP server, see Setting System-Wide Parameters Using System Preferences.</p>
Sender Address field	Enter the e-mail address that notifications should be sent from. If the sender's e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.

Graphical User Interface Element	Description
Recipient Address(es) field	<p>Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon.</p> <p>If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.</p>
Send Recipient(s) Subject Only check box	<p>Check to include only the subject in the e-mail message.</p> <p>Uncheck to send a fully detailed e-mail message (default).</p> <p>For Cisco Prime Collaboration Release 11.1 and later</p> <p>Note You will get an e-mail notification with the subject line in the following format :</p>
<p><i>[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY.</i></p> <p>For example: <i>[PC-ALERT-CPCM-Ent-Cluster]50.0.50.230:Gatekeeper Registration Failure:CRITICAL</i></p> <p><i>CLUSTERNAME</i> is included in the subject line for Unified Communications Manager and Cisco VCS only. For all other device types <i>CLUSTERNAME</i> is left empty.</p> <p>If the <i>DEVICE IP</i> or <i>CLUSTERNAME</i> is not available, it is left empty.</p>	
Syslog Subscription Type fields	
IP Address/Fully Qualified Domain Name editable column	Enter an IP address or Fully Qualified Domain Name (FQDN) of the host.
Port editable column	<p>Enter a port number on which the syslog daemon is listening. A valid port value is a number from 0 to 65,535. You can enter the default port number value 514.</p> <p>The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.</p>
Comments editable column	(Optional) Include comments.



CHAPTER 17

Set Threshold Rules

This section explains the following:

- [Set Threshold Rules, on page 213](#)
- [Threshold Rules, on page 213](#)
- [Configure TelePresence Endpoint Threshold—Device Level, on page 215](#)
- [Configure TelePresence Endpoint Thresholds—Global, on page 216](#)
- [Configure Thresholds for Conference Troubleshooting, on page 216](#)
- [Enable Automatic Troubleshooting for TelePresence Endpoints, on page 217](#)
- [Overview of Device Pool Thresholds, on page 217](#)
- [Edit Device Pool Thresholds, on page 219](#)
- [Overview of Voice Call Grade Settings, on page 219](#)
- [Add Dynamic Syslogs, on page 220](#)
- [Correlation Rules, on page 222](#)
- [Create Custom Alerts, on page 225](#)
- [System, on page 227](#)

Set Threshold Rules

This section explains how to customize alarms and events to suit your business needs.

Threshold Rules

You can configure the devices to generate events when certain parameters cross predefined thresholds.

For Cisco Prime Collaboration Release 11.5 and later

You can perform the settings at **Alarm & Report Administration > Event Customization > Threshold Rules**.

The threshold rules page contains two tabs—Basic and Advanced. The Basic tab lists the inline events in Cisco Prime Collaboration Assurance that you can raise or suppress.

The Advanced tab lists all the available events and also allows you to create custom events. To create custom events: click **Add Event**; select a cluster or device from the drop-down; enter the required details; and click **Save**.

For Cisco Prime Collaboration Release 11.1 and later

For each of the events listed in both these tabs, you can add or edit custom threshold by expanding the event and clicking **Custom Rule**. In the Basic tab, you can only create threshold based on the device type selected whereas in the Advanced tab, you can also set threshold rules, such as scheduling alerts, setting frequency, severity, and so on, for the thresholds that you create. You can add, edit, or delete the custom threshold rules at the device level or device type level. For the changes to apply for all devices, check the Apply for All Devices check box.

In both Basic and Advanced tabs, you can add additional information about events in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as an email notification.

We do not recommend you to add special characters like dollar (\$), vertical bar (|), and tilde (~) in **Notes for Email**.

On clicking the **Custom Rule** in the Advanced tab, the Add Alert Settings page is displayed. Select the **Device Type**, **Cluster**, and click **Next**. In the Add Threshold Rules tab, enter the required details and click **Save**.

Apart from adding events and thresholds, you can also perform the actions mentioned in the table below:

Actions	Basic	Advanced
Change Severity	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click Change Severity .	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click Change Severity . You can also change the severity of custom threshold using the Custom Rule option and that of custom event using the Edit Threshold option.
Raise or Suppress events	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click Raise or Suppress .	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click Raise or Suppress .
Raise or Suppress thresholds	Yes Expand the event, select threshold, and select Raise , or Suppress from the drop-down.	Yes Expand the event, select threshold, and select Raise , Suppress , or Conditional from the drop-down.

Edit, Reset, and Delete existing thresholds	No You can edit or reset the threshold settings, but cannot delete. To edit or reset the threshold, expand the event, edit the threshold settings, and click Save Changes .	Yes To edit or reset the threshold, expand the event, edit the threshold settings, and click Save Changes . You can delete only the custom thresholds. To delete a threshold, expand the event, select the threshold, and click Delete .
Edit or Delete Events	No	Yes Expand the event, edit the settings, and click Save . You can delete only the custom events. To delete an event, select the check box and click Delete .
Clone for events	No	Yes Click Clone , fill in the details, and click Save . Note You can use the clone option only for CVP and Unified CCE devices. This option is disabled for events of the other device types such as Communication Manager, Media Sense, IM and Presence, Finesse, and so on.

Configure TelePresence Endpoint Threshold—Device Level

For Cisco Prime Collaboration Release 11.5 and earlier

Perform the following procedure to configure the thresholds for Cisco TelePresence endpoints at a device level, if you do not want the thresholds to be applied at a global level.

Step 1 Choose **Assurance Administration > Event Customization > Threshold Rules**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration > Event Customization > Threshold Rules**.

Step 2 In the **Basic** tab, expand the Jitter, Packet loss or Latency event and modify the values for Minor, Major, and Critical Thresholds.

You also have the option to Raise or Suppress the event.

Step 3 Click **Save Changes**.

You can also apply the changes to all the devices of a device type or for selected devices of a device type. To do this, click **Custom Rule** and select the Device Type. To apply for all the devices, select All Devices of this Type. To apply the changes for selected devices, click Select Devices, select the devices of your choice and click **Save**.

To search for a device, select **Quick Filter** from the **Show** drop-down list and type the Host Name or IP Address of that device.

Configure TelePresence Endpoint Thresholds—Global

For Cisco Prime Collaboration Release 11.1 and earlier

You can set up Cisco Prime Collaboration Assurance when the threshold value exceeds the configured limit for Rx packet loss, jitter, or latency for all TelePresence devices.

To configure thresholds for TelePresence endpoints:

Step 1 Choose **Assurance Administration > Conference Path Threshold Settings**.**Step 2** Modify the values for Rx Packet Loss, Average Period Jitter or DSCP and click **Save**.

You can also modify the Polling Interval for the thresholds. If you want to reset the values to default, click **Reset to Default**.

When the TelePresence threshold value exceeds the defined value, you can enable to start automatic troubleshooting. Go to **Assurance Administration > Event Customization > Threshold Rules**; in the Basic tab, expand the Jitter, Packet loss or Latency event and choose Minor, Major, or Critical from the Automatic Troubleshooting drop-down list. To disable, choose Disabled from the drop-down list.

What to do next

For information on how to configure Cisco TelePresence endpoints at a device level, see the “Configure TelePresence Endpoint Threshold—Device Level” section in the [Cisco Prime Collaboration Assurance Guide-Advanced, 11.x](#).

Configure Thresholds for Conference Troubleshooting

For Cisco Prime Collaboration Release 11.6 and later

You can configure thresholds in Cisco Prime Collaboration Assurance to display the metric violation in the path, or to start automatic troubleshooting when the threshold value exceeds the configured limit for Rx packet loss, jitter, or latency for all TelePresence devices.

To configure thresholds for TelePresence endpoints:

Step 1 Choose **Alarm & Report Administration > Conference Path Threshold Settings**.

The **Conference Path Threshold Settings** page is displayed.

Step 2 Modify the values for Memory Utilization and Rx Packet Loss if you want to change the color of the bubbles in path statistics.

You can also modify the values for CPU Utilization, Average Period Jitter, and DSCP for any metric violation in the path. A blue badge information icon is displayed in the Path View and Quick View if the threshold value exceeds the configured limit for Rx Packet Loss, Average Period Jitter, or DSCP for all devices.

Step 3 (Optional) Modify the values for Flows Statistics Polling Interval if you want to modify the polling interval.

Step 4 Click **Save**.

If you want to reset the values to default, click **Reset to Default**.

Enable Automatic Troubleshooting for TelePresence Endpoints

For Cisco Prime Collaboration Release 11.6 and later

Perform the following procedure to enable automatic troubleshooting of a conference when the threshold value exceeds the defined value for packet loss, jitter, and/or latency.

SUMMARY STEPS

1. Choose **Alarm & Report Administration > Event Customization > Threshold Rules**.
2. In the **Basic** tab, expand the Jitter, Packet loss, or Latency event and choose **Minor**, **Major**, or **Critical** from the **Automatic Troubleshooting** drop-down list.

DETAILED STEPS

Step 1 Choose **Alarm & Report Administration > Event Customization > Threshold Rules**.

Step 2 In the **Basic** tab, expand the Jitter, Packet loss, or Latency event and choose **Minor**, **Major**, or **Critical** from the **Automatic Troubleshooting** drop-down list.

To disable, choose **Disabled** from the drop-down list.

Overview of Device Pool Thresholds

A device pool is a logical group of devices. It provides a convenient way to define a set of common characteristics that can be assigned to devices, for example, the region in which the devices are located.

Within Cisco Prime Collaboration Assurance, device pools are displayed only after a cluster discovery is completed. If no device pools display in the thresholds window, schedule the inventory to run. By default, cluster device discovery is not scheduled.



Note If there are no devices attached to a device pool, Cisco Prime Collaboration Assurance does not display the device pool even after completing the cluster device discovery.

The device pool threshold settings in Cisco Prime Collaboration Assurance allow the user to configure the amount of aggregated events.

- If you raise the default or current percentage settings for any of the device pool thresholds, you decrease the amount of aggregated events you will receive.
- If you lower the default or current percentage settings for the device pool threshold, you will receive more aggregated events from this device pool.

If the number of impacted phones is equal to the threshold value, Cisco Prime Collaboration Assurance raises one service quality event.

For example, if the device pool contains 100 phones and 10 phones are impacted with a network problem, when the device pool threshold is set to 10% you will receive one aggregated event about this device pool.

After an aggregated event is raised, no other aggregated events will be sent until this event is cleared. To clear an aggregated event, all individual device or service quality events must be cleared first.



Note For the "ServiceQualityThresholdCrossed" event, Cisco Prime Collaboration Assurance rounds off the threshold value from decimal to whole number.

For Cisco Prime Collaboration Release 11.6



Note For both the "ServiceQualityThresholdCrossed" and "PhoneUnregThresholdExceeded" events, Cisco Prime Collaboration Assurance rounds off the threshold value from decimal to whole number.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the device pools that are displayed belong to the customer(s) you have selected using the global Customer Selection field.

For Cisco Prime Collaboration Release 12.1 and later



Note For both the "ServiceQualityThresholdCrossed" and "EndpointUnregThresholdExceeded" events, Cisco Prime Collaboration Assurance rounds off the threshold value from decimal to whole number.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the device pools that are displayed belong to the customer(s) you have selected using the global Customer Selection field.

Cisco Prime Collaboration Assurance considers these device pool threshold events as device events and not service level events.

Edit Device Pool Thresholds

Perform the following procedure to view and configure device pool thresholds by using Cisco Prime Collaboration Assurance.

-
- Step 1** Choose **Event Customization > Correlation Rules**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Alarm & Report Administration > Event Customization > Correlation Rules**.
- Step 2** Select EndpointUnregThresholdExceeded or ServiceQualityThresholdCrossed event.
If no device pools appear in this window, schedule the cluster inventory to run.
- Step 3** Check the check box next to the device pool you want to view or edit.
- Step 4** Click **Edit**.
- Step 5** To edit the current default thresholds:
- Select a group, change the default threshold, and click **Edit**.
 - In the Phone Unregistration Threshold/Service Quality Threshold dialog box, edit the threshold and click **Save**.
To reset all parameter types with Cisco Prime Collaboration Assurance default settings:
 - Check the check box for All Device Pools/CMEs and click **Revert**.
 - Click **Save**.
- Although the changes are saved in the database, they are not yet applied to the IP fabric.
- To be notified automatically when you receive this type of aggregated event, you can set up a notification to have an email sent when this event is raised. For details on how to set up a notification email, see Configure Notifications section in [Cisco Prime Collaboration Assurance Guide - Advanced](#).
-

Overview of Voice Call Grade Settings

The voice quality grading is performed based on Severely Conceal Seconds Ratio (SCSR) (%). It helps you to get better call quality measurement throughout the entire call duration than MOS based grading. It also supports various audio codecs especially wide-band codec. For more information on MOS to SCSR(%) change, see [Cisco Prime Collaboration Assurance and Analytics: Grade VoIP Calls for Efficiency and Reliability White Paper](#).

The call is categorized as long call/short call based on duration of call. If the duration of the call is greater than or equal to 20 seconds then it is long call and the duration of the call is less than 20 seconds then it is short call.

You can update the threshold value for long call SCSR (%) and short call SCSR (%). The threshold settings for short call SCSR (%) and long call SCSR (%) are different. The following table details the available call grades:

Call Grade	Explanation
------------	-------------

Poor	If the SCSR (%) value of call is greater than threshold value of long call SCSR (%) or short call SCSR (%) then call grade is Poor.
Acceptable	If the SCSR (%) value of call is greater than or equal to threshold value of long call SCSR (%) or short call SCSR (%) then call grade is acceptable.
Good	If the SCSR (%) value of call is less than threshold value of long call SCSR (%) or SCSR (%) then call grade is good.

To configure the threshold settings for long call SCSR (%) or short call SCSR (%), choose **Alarm & Report Administration > CDR Analysis Settings > Configure Voice Call Grade** and enter the threshold values in the appropriate fields. If you want to reset the threshold values to default settings, click **Reset to Default**.

Add Dynamic Syslogs

Cisco Prime Collaboration Assurance enables you to add unsupported syslogs. You must get the exact syslog details from the device before you use the syslog in Cisco Prime Collaboration Assurance; for example, you must enter the exact syslog name. The syslog name you enter is taken as the event name.

You can set the severity and the time by which the syslog must be cleared.



Note

Dynamic Syslog supports all the devices except TP_CONDUCTOR and non-Cisco devices.



Note

Syslog communication is supported through UDP.

We recommend that you do not add:

- Syslogs that are likely to create an excessive load on Cisco Prime Collaboration Assurance due to a possible flood of syslogs.
- More than 20 syslogs.

For Cisco Prime Collaboration Release 11.1 and later

You can add additional information about events or alarms in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as an email notification.

We do not recommend you to add special characters like dollar (\$), vertical bar (|), tilde (~) in **Notes for Email**.

To add syslogs:

Step 1 Choose **Assurance Administration > Event Customization > Syslog Rules**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration > Event Customization > Syslog Rules**.

Step 2 Click **Add Event**.

The New Syslog Event window opens. Enter the following:

- Syslog Name
- Event Description
- Event Severity
- Event Clear Interval

Step 3 (Optional) Check the **Raise Event for Each Occurrence** check box.

Use this option judiciously. Cisco Prime Collaboration Assurance raises an event for each syslog. If syslogs are raised with unique details each time, this is a feasible option.

Step 4 Click **Save**.

You can:

- Use the **Edit** option to change the event name, severity, and check or uncheck the **Raise Event for Each Occurrence** check box.
- Customize the syslog name or event severity. To do this, go to the Event Customization page. See the [Set Threshold Rules, on page 213](#) for details.

Example

Below is an example for unsupported syslog, which is raised when ITLRecovery certificate that has not been backed up in the cluster.

Enter the following values:

- Syslog Name - ITLRecoveryCertBackup
- Event Description - ITLRecoveryCertBackup Event
- Event Severity - Major
- Event Clear Interval -1 hour



Note Event Severity and Event Clear Interval values are configurable.

<187>9009: Jul 31 2017 16:05:38.777 IST :%UC_CERT-4-ITLRecoveryCertBackup: %[Message=][AppID=Cisco Certificate Monitor][ClusterID=ccm234][NodeID=cucm107886234]: This cluster has an ITLRecovery certificate that has not been backed up. Taking a manual backup of this certificate is recommended to avoid the need to manually delete the ITL file from every phone in the cluster after certain cluster reconfiguration operations

Correlation Rules

When an event is raised from connected devices, Cisco Prime Collaboration Assurance applies correlation rules. In the following table, for a device, when event A and event B (or a single event) occurs at a certain frequency within a specified time window, Cisco Prime Collaboration Assurance correlates these events and raises an alarm. The alarm is auto-cleared within 24 hours.

For example, whenever a Utilization threshold value changes, Cisco Prime Collaboration Assurance generates a High Utilization event. If the High Utilization event occurs thrice within the 20 minute time interval, High Utilization Detected alarm is raised.

The following are the predefined correlation rules in Cisco Prime Collaboration Assurance:

If you have added the Cisco Prime Collaboration Contact Center Assurance license, certain correlation rules can be exclusively applied for Cisco Prime Collaboration Contact Center Assurance. For details, see the “Contact Center Correlation Rules” section in the [Cisco Prime Collaboration Contact Center Assurance Guide](#).

Name of the Correlation Rule	Main Events Responsible for the Alarm to be Raised	Symptom Events that Occur Due to the Main Event	Name of the Correlated Alarm	The Correlated Alarm is Raised When ...	Window Time (in min) within which the Main Events and Symptom Events are Received	No of Occurrences
Call Throttling Detected	Code Yellow, CpuPegging	NA	CodeYellow	Both the main events occur.	20	1
Interface Flapping	OperationallyDown, OperationallyDown cleared	NA	Interface Flapping	OperationallyDown is followed by OperationallyDown cleared event alternatively for more than three instances.	20	3
Repeated Location Bandwidth Out Of Resource	LocationBWOutOfResources	NA	Repeated Location Bandwidth Out Of Resource	LocationBWOutOfResource is raised on Cisco Unified Communications Manager for three or more instances.	20	3

Name of the Correlation Rule	Main Events Responsible for the Alarm to be Raised	Symptom Events that Occur Due to the Main Event	Name of the Correlated Alarm	The Correlated Alarm is Raised When ...	Window Time (in min) within which the Main Events and Symptom Events are Received	No of Occurrences
WAN Link Outage Detected	Unresponsive	NA	Wan Link Outage Detected	Unresponsive event is triggered.	10	NA
Note This rule cannot be edited or deleted from user interface.						
VM Down	VMDown	Unreachable	VMDown	VMDown trap is received from vCenter and Unreachable event for VM is received, based on ICMP polling.	5	NA
ESX Host Down	HostConnection Failure	Unreachable, VMDown	ESXHost Down	HostConnection Failure trap is received from vCenter and Unreachable event for ESXHost is received, based on ICMP polling.	5	NA
Network Down	NetworkConnectivity Lost, LostNetwork Connectivity ToDVPorts	Unreachable	Network Down	One of the main event occurs and Unreachable event for ESXHost is received, based on ICMP polling.	5	NA

Name of the Correlation Rule	Main Events Responsible for the Alarm to be Raised	Symptom Events that Occur Due to the Main Event	Name of the Correlated Alarm	The Correlated Alarm is Raised When ...	Window Time (in min) within which the Main Events and Symptom Events are Received	No of Occurrences
UCS Chassis Down	ChassisInOperable, ChassisIOCardInaccessible, ChassisThermalThresholdNonRecoverable	Unreachable, VMDown, HostConnectionFailure, NetworkConnectivityLost	UCS Chassis Down	One of the main event occurs.	5	NA
Endpoint Unreg Threshold Exceeded Phone Unregistered Threshold Exceeded	NA	NA	Endpoint Unreg Threshold Exceeded Phone Unregistered Threshold Exceeded	NA	NA	NA
Service Quality Threshold Crossed	NA	NA	Service Quality Threshold Crossed	NA	NA	NA

In the Event Customization page, you can search and filter events using the search option available at the top of the page. However, for the events listed under Correlation Rules, the name-based search does not work as the names of the events are not unique and are same as events listed under the other tabs in the Event Customization page. To search for events under the Correlation Rules tab, use the name of the correlation rule.

For Cisco Prime Collaboration Release 11.1 and later

You can add additional information about events or alarms in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When

you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as email notification.

We do not recommend you to add special characters like dollar (\$), vertical bar (|), and tilde (~) in **Notes for Email**.

For all the correlation rules in Cisco Prime Collaboration Assurance, the alarm suppression logic is applied, by default. When event A or event B occurs within a specified time window, the correlated alarm is triggered first along with corresponding events. The alarm for the individual event is raised only if the correlation is not met, and after the specified time window. For example, whenever a Unified CCE component like logger, PG, or router goes down, Cisco Prime Collaboration Assurance generates the correlated alarm and a set of events. The alarm for that event is raised only if the correlation does not happen and after the time interval of 10 minutes. To disable the alarm suppression, select the correlated rule, and click **Edit**. In the Edit Correlation Rule page, check the Disable Alarm Suppression check box and click **Save**.



Note Disabling alarm suppression logic for a correlation rule does not mean that the events part of that correlation rule cannot be raised. If an event is part of two or more correlation rules and the alarm suppression logic is applied to one of the rules, then the event can still be raised as the other rules take precedence.

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. For the list of these triggers, see the [Setting Up Devices for Cisco Prime Collaboration Assurance 11.0](#) wiki page for Cisco Prime Collaboration Assurance 11.0 and [Configure Devices for Prime Collaboration Assurance 11.5](#) for Cisco Prime Collaboration Assurance 11.5. To view the list of events and alarms for VMware vCenter Server, see [Supported Alarms and Events for Cisco Prime Collaboration](#). For more information on VMware vCenter Server (vCenter), see the [vSphere - ESX and VCenter Datacenter Administration Guide](#).

Create Custom Alerts

You can create custom alerts and also include the threshold and alert trigger parameters. See [Custom Alert Parameters](#) for details about the parameters.

To create custom alerts

Step 1 For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration > Event Customization > Threshold Rules**.

You can also add events directly from a custom dashboard that you created.

Step 2 Click **Add Event**.

Step 3 In the New Performance Counter Event page:

- a) Specify the cluster and the server.
- b) Select the counter from the Available Counters drop-down list.

If you have installed Cisco Prime Collaboration Assurance in MSP mode, public IP address is displayed when you select the server and counter. However, you cannot create/add a custom event for such nodes if a specific performance counter/device is not added or managed in Cisco Prime Collaboration Assurance.

Also, in the Cluster drop-down list, only those products and clusters which belong to a specific customer (that is selected from the global filter drop-down) are displayed.

- c) Add a description and the recommended action. This is optional.
- d) Specify the threshold values, duration and frequency, and the schedule for monitoring.
- e) Click **Save**.

Note The threshold rules that are created for any performance counter for a device, are saved in the database. This generates the alarms when the counter value violates any of the threshold conditions defined in the threshold rule. For information on the purge policies, see the Purge Policies chapter in [Cisco Prime Collaboration Assurance Guide—Advanced](#).

Custom Alert Parameters

Table describes the parameters you can specify for the custom alert.

Setting	Description
Threshold	
	<p>Check the check box and enter the value that applies.</p> <ul style="list-style-type: none"> • Over—Check this check box to configure a maximum threshold that must be met before an alert notification is activated. In the Over value field, enter a value. For example, enter a value that equals the number of calls in progress. • Under—Check this check box to configure a minimum threshold that must be met before an alert notification is activated. In the Under value field, enter a value. For example, enter a value that equals the number of calls in progress. <p>Note Use these check boxes in conjunction with the Frequency and Schedule configuration parameters.</p>
Value	
	<p>Click the radio button that applies.</p> <ul style="list-style-type: none"> • Absolute—Choose Absolute to display the data at its current status. These counter values are cumulative. • Delta—Choose Delta to display the difference between the current counter value and the previous counter value. • Delta Percentage—Choose Delta Percentage to display the counter performance changes in percentage.
Duration	

Setting	Description
<ul style="list-style-type: none"> • Trigger alert only when value constantly... • Trigger immediately 	<ul style="list-style-type: none"> • Trigger alert only when value constantly...—If you want the alert notification only when the value is constantly below or over threshold for a desired number of seconds, click this radio button and enter seconds after which you want the alert to be sent. • Trigger immediately—If you want the alert notification to be sent immediately, click this radio button.
Frequency	
<ul style="list-style-type: none"> • Trigger on every poll • Trigger <> events within <> minutes 	<p>Click the radio button that applies.</p> <ul style="list-style-type: none"> • Trigger on every poll—If you want the alert notification to activate on every poll when the threshold is met, click this radio button. <p>For example, if the calls in progress continue to go over or under the threshold, the system does not send another alert notification. When the threshold is normal (between 50 and 100 calls in progress), the system deactivates the alert notification; however, if the threshold goes over or under the threshold value again, the system reactivates alert notification.</p> <ul style="list-style-type: none"> • Trigger <> events within <> minutes—If you want the alert notification to activate at certain intervals, click this radio button and enter the of alerts that you want sent and the number of minutes within which you want them sent.
Schedule	
<ul style="list-style-type: none"> • Trigger immediately (Non-stop monitoring) • Schedule between <> to <> 	<p>Click the radio button that applies:</p> <ul style="list-style-type: none"> • Trigger immediately (Non-stop monitoring)—If you want the alert to be triggered 24 hours a day, click this radio button. • Schedule between <> to <>—If you want the alert notification activated within a specific time frame, click the radio button and enter a start time and a stop time. If the check box is checked, enter the start and stop times of the daily task. For example, you can configure the counter to be checked every day from 9:00 am to 5:00 pm or from 9:00 pm to 9:00 am.

System

For Cisco Prime Collaboration Release 11.1 and later

and

For Cisco Prime Collaboration Release 11.5 and later

You can view all the predefined alarms and events of Cisco Prime Collaboration Assurance in **Alarm & Report Administration > Event Customization > System**.

System tab displays the following information:

- Name

- **Category**
- **Status**
- **Severity**
- **Default Severity**
- **For Cisco Prime Collaboration Release 11.1 and later**
- **Custom Rules**
- **For Cisco Prime Collaboration Release 11.5 and later**
- **Exception Indicator**
- **Notes for Email**

**Note**

You can add additional information about events or alarms in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as email notification.

We do not recommend you to add special characters like dollar (\$), vertical bar (|), and tilde (~) in **Notes for Email**.

You can perform the following actions:

Actions	Description
Change Severity	Check the box against Name—To select all the events; or check the boxes of the events of your choice and click Change Severity .
Raise or Suppress events	Check the box against Name—To select all the events; or check the boxes of the events of your choice and click Raise or Suppress .



CHAPTER 18

Monitor Alarms and Events

This section explains the following:

- [Monitor Alarms and Events, on page 229](#)

Monitor Alarms and Events

This chapter explains about monitoring the alarms and events.

Alarms and Alarm Summary

You can view Alarms and Alarm Summary pages through **Monitor > Alarms & Events**.

The Alarms tab displays the following information for each alarm in the Alarm browser:

Severity

Indicates the severity of the alarm which can be, critical, major, minor, warning. The collapsible icon for an alarm displays the General Info of the alarm, Messages, Annotation, Recommended Actions for an alarm.

To view events associated with an alarm, rest the mouse over the alarm severity, and click the quick view icon. The **Events for Alarm** page is displayed, containing the following details:

- Description - Alarm description.
- Status - Device that triggered the alarm.
- Time - Date and time when the alarm occurred.

This summary windows lists only the five latest events. To see the complete list, see **Event History**.

In the **Events for Alarm**, you can click:

- The **See Event History** link to display the events associated with the selected alarm.
- The **Monitor Endpoint** or **Monitor Conference** link to launch the Endpoints Monitoring or **Conference Monitoring** page. This link is displayed only for conference and endpoint alarms.

Clipboard icon/Is Annotated

Indicates the alarm has user notations.

Status

Indicates the status of the alarm.

It shows the alarm clearing status details.

Alarm Name

Name of the generated alarm. Rest the mouse over the alarm name and the Quickview icon that is displayed, to view details of the alarm selected.

Customer

If you have installed Cisco Prime Collaboration Assurance in MSP mode, the customer that the device belongs to, is displayed for both Alarms and Alarm Summary.

Device Name

Displays the name of the device that triggered the alarm.

Device IP

Displays the IP address of the device. You can launch the endpoint or the infrastructure device log in page using the link.

You cannot launch the endpoint or the infrastructure device log in page using this link, if you have deployed Cisco Prime Collaboration Assurance in MSP mode.

Component Name

Device name, or the name of component such as a device pool, an interface.

Last Updated

Displays the date and time when the alarm occurred.

Device Type

Displays the type of the device.

Owner

Displays the name of the person to whom this alarm is assigned. (If a name was entered.)

Description

Displays a short description about the alarm.

Category

Displays the category of alarm. For example: conference, endpoint, service infrastructure.

Endpoint Name

Indicates the name assigned to the endpoint for ease of identification. By default, the **Endpoints Name** column is hidden. To see all the columns, click the Settings option on the top right corner.

Model

Displays the device model, such as ciscoEX90, ciscoCTS500, ciscoC20, and so on.

Private IP address

If you have installed Cisco Prime Collaboration Assurance in MSP mode, private IP address of the device is displayed. By default, the **Private IP Address** column is hidden. To see all the columns, click the Settings option on the top right corner.

Overall, the alarm browser allows you to:

- View events associated with an alarm—Rest the mouse over the icon next to alarm status for the popup window to appear displaying all the events for the alarms.
- Clear or acknowledge an alarm.
- Assign the alarm—Check the desired check box, click **Assign to me** from the assign drop-down list.
- Add Annotation - Check the desired check box, click the **Annotate** drop-down list to add notes.
- Delete Alarm - Check the desired check box, click **Delete**.
- Set up Email Notification - Check the desired check box, click **Email Notification**. Enter the recipient addresses, comments, and subject, then click **Submit**. For a list of supported alarms and events, see [Supported Alarms and Events for Cisco Prime Collaboration](#).

Alarm Summary

Alarm Summary provides a summary of the alarms for each device.

The following factor distinguishes Alarm Summary from Alarms: When you select a device, the alarms and events that correspond to the selections appear in the Alarms and Events for *device* pane at the bottom of the page. You can export the alarms as a CSV or PDF file. To export the alarms, select the desired alarms, and click the export icon on the top right of the Alarm Summary pane.

The Alarm Summary displays the following information:

Severity

Alarm severity icon. Indicates the severity of the alarm.

Last 15 Minutes

Indicates that this device is one of the most recent in the table (within the last 15 minutes). Devices are sorted based on the time of the most recent event status changes.

Device Name

Device name or IP address.

Device IP

Device IP. Click on the quick view icon to launch the Device 360° View.

Type

Device type.

Severity Columns

- Critical - Total number of critical alarms.
- Major - Total number of major alarms
- Minor - Total number of minor alarms
- Warning - Total number of warning alarms.

Last Update Time

Time and date of alarm update (indicates activity, such as an alarm recurrence, alarm acknowledgment, the addition of a note, and so forth). Alarms are grouped by severity, and within severities, alarms with the latest change are listed first.

Endpoint Name

Indicates the name assigned to the endpoint for ease of identification. By default, the **Endpoints Name** column is hidden. To see all the columns, click the Settings option on the top right corner.

Private IP address

If you have installed Cisco Prime Collaboration Assurance in MSP mode, private IP address of the device is displayed. By default, the **Private IP Address** column is hidden. To see all the columns, click the Settings option on the top right corner.

Events

The Events tab displays the following information:

ID

Event unique identification number.

Severity

Event severities include: Critical, Major, Minor, Warning, and Informational. Click the title to sort the events list by severity (ascending or descending order). If any event is cleared, its severity changes to informational.

Status

The current status of the event.

Event Name

The name of the event. Rest your mouse over the quick view icon to view the event details. Click **Customize Event** to cross-launch to the **Event Customization** page, which displays the details of the selected event. Expand the event and click Custom Rule to edit the event details.

Customer

If you have installed Cisco Prime Collaboration Assurance in MSP mode, the customer that the device belongs to, is displayed in the Events pane.

Device Name

The name of the event. Rest your mouse over the event name to view the event details.

Device IP

Displays the IP address of the device. You can launch the endpoint or the infrastructure device using the link.

Component Name

Device name, or the name of component such as a device pool, an interface.

Last Updated

Displays the date and time when the event occurred.

Device Type

Displays the type of the device.

Category

Displays the alarm assigned category, such as conferences, endpoints, and so on.

Description

Description of the event.

Endpoint Name

Indicates the name assigned to the endpoint for ease of identification. By default, the **Endpoints Name** column is hidden. To see all the columns, click the Settings option on the top right corner.

Model

Displays the device model, such as cat4506, ciscoMCS7828I, and so on.

Private IP Address

If you have installed Cisco Prime Collaboration Assurance in MSP mode, the private IP Address of the device is displayed. By default, the **Private IP Address** column is hidden. To see all the columns, click the Settings option on the top right corner.

**Note**

- Click the refresh icon to view the latest list of events raised.
- If you have installed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to.
- At any point, to see the Alarm Browser or Alarm Summary, click the links available at the bottom right.

View Call Events

Cisco Prime Collaboration Assurance displays the Cisco TelePresence Management Suite (TMS) informational events. It displays call connected or disconnected information for Cisco TelePresence System Profile MXP Series devices, Cisco TelePresence Integrator C Series codecs, and Cisco TelePresence Video Communication Server (VCS).

Call events can be displayed for only one supported device at a time.

To view call events:

Step 1 For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **Inventory Management**

Step 2 Select a device, and Click **Call Events**.

Note Call events are displayed only for Cisco VCS, MXP, MCU devices, and codecs.

Step 3 The Call Events page displays the following details:

For MXP and Codecs:

- Start Time—The call start time
 - Remote Site—The site to which the call was made.
 - Call State
 - Duration
 - Call Direction—Whether an incoming or outgoing call.
 - Call Protocol—H323/SIP
 - Encryption Mode
 - Cause
 - Bandwidth
 - Call ID
- For VCS:

- Time
- Source Address
- Source Alias
- Destination
- Address
- Destination Alias
- Duration
- Call State
- Call
- Protocol
- Bandwidth
- Call Type

Notes for Alarms and Events

1. Alarms that are dependent on the polling interval, might have a situation where the alarm is raised and cleared before the next poll. Therefore, it is not being reported to Cisco Prime Collaboration Assurance.
2. **Behavior of SIPTrunk Out Of Service (OOS) Correlation Alarm :**

SIP Trunk OOS : This correlation alarm is introduced to track and combine multiple SIPTrunk OOS Alarms and generate one single correlated Alarm at the Cluster level. Correlation happens in a span of 2 minutes time window.

Following are the conditions for the correlation alarms to get cleared :

- SIPTrunk OOS Correlation alarm gets cleared when the associated individual SIPTrunk OOS alarms are cleared by processing InService Syslogs.
- There is a time base clear as well, where the correlation alarms are cleared automatically after 24 hours.

Using the conditions mentioned above, correlation alarm is cleared in any one of the following scenarios :

Scenario 1:

- SIPTrunk OOS alarms are raised in Cisco Prime Collaboration Assurance.
- Individual SIPTrunk OOS alarms are correlated and Corresponding SIPTrunk OOS correlation alarm is raised at the cluster level.
- SIPTrunk OOS gets cleared once the SIPTrunks are back and the SIPTrunk OOS also gets cleared with that.

Scenario 2:

- SIPTrunk OOS alarms are raised in Cisco Prime Collaboration Assurance.
- Individual SIPTrunk OOS alarms are correlated and Corresponding SIPTrunk OOS correlation alarm is raised at cluster level.
- SIPTrunk stays down for more than 24 hours.
- SIPTrunk OOS gets cleared after 24 hours based on 24 hours time based clear and the SIPTrunk OOS individual alarms will clear once the SIPTrunk is back Inservice and syslog is processed for that.

Scenario 3 :

- Individual SIPTrunk OOS alarms are raised and cleared rapidly within the 2 minutes correlation window.
- Correlation engine will still run and raise the SIPTrunk OOS correlation alarm and now as the associated individual alarm has already cleared, the SIPTrunk OOS will be left alone.
- Then the correlation alarm gets cleared automatically after 24 hours, based on 24 hours time based clear.

3. In a multi-node call manager cluster, if the same alert exists on more than one node at the same time, PCA displays one latest alert.
4. Polling frequency of RTMT alerts

For Cisco Prime Collaboration Release 12.1 and later

The default polling frequency of RTMT alerts for Small, Medium, and Large setups is 1 minute and the recommended polling frequency for Very Large setup is 2 minutes.



PART **V**

Monitor the Network

- [Monitor Video Endpoints, on page 239](#)
- [Monitor Conferences, on page 247](#)
- [Enable Cisco APIC-EM to Troubleshoot Conference, on page 269](#)
- [Monitor the Cisco Prime Collaboration Assurance Server, on page 273](#)



CHAPTER 19

Monitor Video Endpoints

This section explains the following:

- [Monitor Video Endpoints, on page 239](#)

Monitor Video Endpoints

The Endpoint Diagnostics dashboard displays the details of all video endpoints.

For Cisco Prime Collaboration Release 11.6 and later

You can add any of the endpoints to the watch list to troubleshoot them further.

The Add to Watch List and Remove from Watch List is also present in the Endpoint 360° View. The Add to Watch List enables you to add a conference to the watch list. It is enabled for both Not In Use and In Use endpoints. For Not In Use endpoints, the troubleshooting starts when the endpoint joins a conference. For In Use endpoints, the troubleshooting starts immediately.

For Cisco Prime Collaboration Release 11.5 and later



Note

You do not need to add any of the endpoints to the watch list to troubleshoot them further.

You can filter endpoints based on device type, using the Device Group pane on the left of the page. For more information, see [Manage Device Groups](#).

Endpoint Diagnostics Dashboard

The Endpoint Diagnostics dashboard displays the details of all the video endpoints.

You can filter endpoints based on device type, using the Device Group pane on the left of the page. For more information, see [Manage Device Groups](#).

Choose **Diagnose > Endpoint Diagnostics** to view the Endpoints Diagnostics dashboard. The following table describes the information displayed in the Endpoint Diagnostics dashboard.

Table 53: Endpoint Diagnostics Dashboard

Information	Description
Endpoints Summary Metrics	Provides the following details: <ul style="list-style-type: none"> • For Cisco Prime Collaboration Release 11.1 and earlier <ul style="list-style-type: none"> Managed endpoints • Unregistered endpoints • Endpoints currently in use • Endpoints with alarms • Endpoints added to the watch list
List of Endpoints	Provides detailed information about all the registered, unregistered, and unknown endpoints. You can use this pane to verify the registration, usage, and visibility status of the endpoints.
Endpoints Details	Provides the following details based on the endpoint type that you select: <ul style="list-style-type: none"> • System information • Peripherals • Scheduled conferences for next 3 days • Service and network infrastructure


Note For Cisco Prime Collaboration Release 11.5 and later

You can view the details of Peripherals (such as camera, and microphone) that are connected to a video or TelePresence endpoint that runs in TC/CE software. This is applicable to SX, MX, and EX series of endpoints.

For Cisco Prime Collaboration Release 11.6 and later

You can view the details of Peripherals (such as camera, and microphone) that are connected to a video or TelePresence endpoint that runs in TC/CE software. This is applicable to SX, MX, DX with CE image, and EX series of endpoints.

ciscoDX70 and ciscoDX80 with CE image does not support Endpoint diagnostics.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which that endpoint belongs to. If you have deployed Cisco Prime Collaboration Assurance in Enterprise mode, you can see the assurance domain to which that endpoint belongs to. You can filter on the Model, Device Pool, Cluster Name, and Switch IP Address columns. Click the Filter icon and then click the drop-down list arrow on these columns. The popup window displays the list.

You can export the endpoints diagnostics dashboard as a .csv or pdf file. This file contains the exact data that appears in the user interface.

You can click the quick view icon to view the Endpoint 360° View.

To change the visibility of an endpoint, click **Edit Visibility**.

The saved filters in Endpoint Diagnostics filters are not saved as expected. The saved filters are present only for the current session and will be cleared once refreshed/logged out.

For Cisco Prime Collaboration Release 12.1 SP2 and later

**Note**

The default visibility settings for endpoints is turned to OFF state for new installations (Cisco Prime Collaboration Assurance 12.1 SP2). During upgrade from the previous versions (Cisco Prime Collaboration Assurance 11.6, Cisco Prime Collaboration Assurance 12.1 FCS/ES1/ES2/ES3/ES4/SP1/...) to Cisco Prime Collaboration Assurance SP2, the Installation routine will retain the default visibility settings of the already managed endpoints.

For Cisco Prime Collaboration Release 12.1 SP2 and later

When you change the Visibility for TC/CE endpoints, a warning message indicating that "One or more TC_CE Endpoints have feedback subscription failures. Check Management Status Reason column." appears if there are any feedback subscription failures in any of the selected endpoints.

You see the current visibility of the endpoint. If you have made any changes, click **Save**. For more information, see [Realtime Visibility of an Endpoint](#). You can also see the visibility status of the endpoint in the Endpoint 360° View, if you point at the icon just before the endpoint name.

The **Add to Watch List** and **Remove from Watch List** is also present in the Endpoint 360° View. The **Add to Watch List** enables you to add a conference to the watch list. It is enabled for both Not In Use and In Use endpoints. For Not In Use endpoints, the troubleshooting starts when the endpoint joins a session. For In Use endpoints, the troubleshooting starts immediately.

You can perform the following tests on the endpoints:

- On-Demand Phone Test: Select endpoint(s) and click **Run Tests > Audio Phone Feature Test**. For more information on the On-Demand Phone Tests, see [Phone Tests—Batch and On Demand Tests](#).
- Synthetic - End-to-End Call Test: Select an endpoint, and click **Run Tests > Audio Test Call**. For more information on the End-to-End Call Tests, see [Create an End-to-End Call Synthetic Test](#).
- Video Test Call: Select two video endpoints, and click **Run Tests > Video Test Call**. For more information on the Video Test Call, see [Manage a Video Test Call](#).

**Note**

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the Video Test Call feature is not available.

You can view the list of unknown endpoints by selecting Predefined > Unknown Endpoints in the Device Group Selector pane on the left side of the user interface.



Note Polycom endpoint is monitored only when it is registered with Cisco VCS. It is not monitored when registered with Polycom call controllers. Automatic call detection is supported using HTTP feedback (through Cisco VCS). Realtime monitoring information such as conference statistics and conference information is not supported.

By default, the auto refresh functionality is disabled for the Endpoints Diagnostics page. To enable or disable auto refresh for every two minutes, check the **Auto Refresh** check box at the top right corner of the user interface.

If you disable auto refresh functionality and log in to the application later, the functionality is still disabled. Check the **Auto Refresh** check box again, for it to work as expected.



Note **For Cisco Prime Collaboration Release 11.5 and later**

When an audio or a video endpoint is moved from one Unified Communications Manager cluster to another Unified Communications Manager cluster, Cisco Prime Collaboration Assurance only displays the device information of the cluster where the endpoint is currently registered. You can view the device information of some of the fields (for example, Device Pool) only after nightly cluster discovery. As a result, Cisco Prime Collaboration Assurance displays an unregistered endpoints count mismatch between the previous Unified Communications Manager cluster and the current cluster. You can view the correct unregistered endpoints count, after the previous entries are purged in Unified Communications Manager.

Troubleshooting

For Cisco Prime Collaboration Release 12.1 SP2 and later

1. **Issue:** If conference diagnostics does not show any call for TC/CE endpoints which are registered to Call Manager.

Recommended Actions: Follow the below troubleshooting steps

- Verify that the endpoint is associated to the CUCM cluster from Endpoint Diagnostics by checking “Cluster Name” column.
- Verify that the respective TC/CE endpoint visibility is set to “Full Visibility” from Endpoint Diagnostics.
- Verify that the “Management Status Reason” column does not show any feedback subscription failure message “Failed to register PCA IP address as HTTPS feedback receiver”.
- If the message “Failed to register PCA IP address as HTTPS feedback receiver” appears, login into TC/CE endpoint and launch URL:

`https://IPAddress/getxml?location=/Status/HttpFeedback`

Verify that the response appears as shown below in feedback slot-2.

```
HttpFeedback item="2" maxOccurrence="n"><Expression item="1"
maxOccurrence="n">/History/CallLog/History</Expression><Expression item="2"
maxOccurrence="n">/History/CallLogs/Call</Expression><Expression item="3"
maxOccurrence="n">/Status/Call[Status='Connected']</Expression><Expression item="4"
maxOccurrence="n">/Status/H323/Gatekeeper</Expression><Expression item="5"
maxOccurrence="n">/Status/SIP/Registration</Expression><Expression item="6"
maxOccurrence="n">/Event/CallSuccessful</Expression><Expression item="7"
maxOccurrence="n">/Event/Message/Prompt/Response</Expression><Expression item="8"
```

```
maxOccurrence="n"/>Event/CallDisconnect</Expression>
<Format>XML</Format>
<Status>OK</Status>
<URL>http://PCAIADDRESS:8889/feedback/cseries</URL></HttpFeedback>
```

- If the XML response does not show the above attributes along with the Cisco Prime Collaboration Assurance IP Address, rediscover the endpoint from Inventory Management and repeat the above point to verify. If problem persists, contact Cisco TAC for assistance.

2. **Issue:** Feedback subscription is not removed from the endpoint due to unknown reasons.

Recommended Actions: Login into the respective endpoint via SSH as admin user.

Enter the following command:

```
xcommand HttpFeedback Deregister FeedbackSlot: 2
```

For more information, see the respective TC or CE Administration Guides.

View User 360 Details

This view displays the end-user information (such as the username, email-id, office phone, and mobile phone numbers) associated with Cisco Unified Communications Manager or TelePresence Management Suite (TMS) endpoints. Photograph and location details for the end user are displayed only if Cisco Prime Collaboration Assurance is integrated with LDAP and the username details matches with LDAP details.



Note End-user information associated with TMS can be retrieved, only if 'TMS Provisioning Extension' component is installed on the TMS.

To access this view,

-
- Step 1** From the global search drop-down, select **User**. You can also launch User 360 from Username column on **Endpoint Diagnostics** page.
 - Step 2** Enter * to list all the users. A string search can provide more specific results. For example, when you enter **test**, it lists all the users whose first name, last name, or username includes the string test.
 - Step 3** Click the User 360 View launch anchor against the username.
-

Access the following tabs in this view:

- **Endpoints**—Displays the managed endpoints associated with the end user. This endpoint includes,
 - **Last Call Quality**—Categorized as good, accepted, or poor; this field describes the call quality of the most recently ended call. Cross launches to **CMR Report**-for endpoints registered to CUCM or **Alarms** page-for endpoints registered to TMS is available.
 - **Calls (24 Hours)**—Number of calls the endpoint was involved in the last 24 hours. This field has cross launches to the **CDR Report**-for endpoints registered to Unified CM and **All Conference Summary Report**-for endpoints registered to TMS.

- **Registration Status**—Displays the registration status of the end user. For a registered end user whose call is in progress, a green icon with call in progress indicator is shown. A red icon for an unregistered end user and a gray icon if the status of the end user is unknown.
- **Service**—Service of the most recently ended call. (Audio only or Audio and Video)
- **Endpoint Model**—Displays the endpoint model. When you click, it cross-launches to **Endpoint Diagnostics** page.
- **Active Conferences**—Displays the endpoints of the end user that are currently engaged in a call. The details of the device are tracked from Conference Diagnostics. This Active Conferences includes,
 - The image of the endpoint and destination number. When you click the image, it cross launches to **Endpoint Diagnostics** page.
 - **Quality stats**—Alarm icon that indicates the current highest severity of the call quality alarms.
 - **For Cisco Prime Collaboration Release 11.1 and earlier**
 - **Tools**—Links you to the troubleshooting page.
- **Alarms**—Displays,
 - Severity
 - Source from which the alarm was received
 - Name of the alarm
 - and the Timestamp.

**Note**

For endpoints registered with Unified CM, a sync for the new users happens automatically. But for endpoints registered with TMS, manual rediscovery of TMS is necessary to sync the details of the new users.

Manage a 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, conference statistics, endpoint statistics. Only the CTS, C and EX series codecs are supported for this call.

**Note**

- This feature is not supported for E20 codec series.
- 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 Assurance in MSP mode.
- The “Video Test Call” feature is not supported for Endpoints registration through the Mobile and Remote Access (MRA) solution.

Table 54: Managing a Video Test call

Task	Description
<ul style="list-style-type: none"> • Start a video test call from Endpoint Diagnostics (Under Diagnose) • Start a video test call from Conference Diagnostics (Under Diagnose) 	<p>Select the video endpoints, and click Video Test Call, to create a test call between two selected endpoints.</p> <p>Note</p> <ul style="list-style-type: none"> • This button gets enabled only after you have selected two video endpoints. • You cannot create a video test call by selecting more than two endpoints. <p>or</p> <p>Select a particular conference on the Conference Diagnostic page, and click Video Test Call, to create a test call for that scheduled conference.</p> <p>Note This button gets activated only after you select a scheduled conference. To see the list of the list of scheduled conferences, filter for scheduled conferences. Remember to select a conference for a future time and date only.</p> <p>The Add Test Call pop up window appears, where you can click on the IP address of the endpoint to launch its application. The default option is to run the test call immediately but you can schedule the call also.</p> <p>For CTS endpoints select the SIP protocol only. For Ex and C Series endpoints you can choose between H.323 and SIP protocols, provided these endpoints are registered using these protocols. When you click the Add Call button, a message appears to notify you that the call has been added successfully.</p> <p>The scheduled call details can be seen on the Conference Diagnostics page. You can see events and alarms, conference statistics, endpoint statistics . This information is available for completed test calls also. You can stop the call immediately if it causes a problem on the network.</p>

Task	Description
Stop a running video test call	<p>You can stop a video test call which is in progress if it hampers your network. To stop a call, select the test call from the Conferences Diagnostic page, by setting the filter to Test Call Conferences. Hover around the conference subject to launch the 360° Conference View, and click the Stop Call icon to stop the in progress video test call.</p> <p>Test call lasts for around 5 minutes, after which it automatically stops.</p>
<p>Edit a scheduled video test call from Video Test Call Configurations page</p> <p>Synthetic Tests > Video Test</p> <p>You can also view or delete video test calls from the same page.</p>	<p>To edit a video test call, click Edit, and reschedule or run the call immediately by clicking Save. A message appears to notify you that the call has been modified successfully.</p>



CHAPTER 20

Monitor Conferences

This section explains the following:

- [Monitor Conferences, on page 247](#)

Monitor Conferences

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Assurance tracks the lifecycle of video collaboration conferences in your network. It correlates conference data received from various sources and provides end-to-end details on the conference.

Cisco Prime Collaboration Assurance receives conference events from call and conference control components, such as Cisco Unified CM and Cisco TelePresence Video Communication Server (VCS). It also retrieves conference details from applications, such as management applications, call and conference control components, conferencing components, and endpoints.

The number of conferences that can be monitored in Cisco Prime Collaboration Assurance depends on the deployment model, such as small, and medium. For information on supported active conferences, see the [System Capacity for Cisco Prime Collaboration Assurance](#).



Note

In the 150k and 80k profile, if you use JTAPI to control all the endpoints to discover devices in Cisco Prime Collaboration Assurance, the server will crash due to OutofMemory condition. Hence, add only those endpoints intended for monitoring the session functionality.

The conference data retrieved from the video collaboration applications includes both scheduled and unscheduled conferences. Cisco Prime Collaboration Assurance differentiates conferences in the following ways:

- **Ad hoc** - An end user dials the extension of the Cisco TelePresence system at the other end. There is no scheduling involved.
- **Scheduled** - Scheduled before the conference through the company's groupware application, such as Microsoft Exchange, Outlook, and so on. You can also schedule the conference directly, using Cisco TelePresence Management Suite (TMS).
- **Static** - Preconfigured Cisco TelePresence conference available all the time. Each static meeting has its own associated meeting number. On some applications, such as Cisco TelePresence MSE, Multipoint Control Unit (MCU), Cisco TelePresence Server (TS), these meetings are called permanent meetings.

Cisco Prime Collaboration Assurance classifies the conferences structure as follows:

- Point-to-point - Conference between two endpoints.
- Multipoint - Conference with more than two endpoints. Between endpoints, you may have MCU.
- MultiSite - Conference with more than two endpoints, without MCU. The endpoints are connected directly. Any endpoint can participate in a MultiSite call with the center endpoint being MultiSite capable. The center endpoint acts as a conferencing device (like MCU). This type of conference structure is supported for MultiSite capable endpoints such as Cisco Codec C and EX Series TelePresence Systems, Cisco TelePresence MX Series, and Cisco Profile Series with a MultiSite license.

The conferences status can be:

- In-progress
- Scheduled
- Completed
- No Show, a scheduled conference without any participants joining the conference until the end time. The scheduled conferences are moved to No show only after the scheduled end time and after Cisco Prime Collaboration Assurance is synchronized with Cisco TMS, after the scheduled end time.

If an endpoint did not join an In-Progress conference, a no-show icon is displayed on the endpoint. This status is shown even after the conference moves to Completed state

If an endpoint joins a conference, but later disconnects from the call before the conference is over, a disconnect icon is visible on this endpoint in the conference topology. Disconnected could mean that there was a problem, or the caller had to leave the conference early.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Conference Diagnostics

The following are required for conference diagnostics:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the [Configure Devices for Cisco Prime Collaboration Assurance](#).
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- Cisco Telepresence Endpoints discovered as TC/CE device type in Cisco Prime Collaboration Assurance should not be included in the JTAPI user controlled devices list. We recommend you to keep the IP Phones into the JTAPI user controlled list.
- Conference Diagnostics feature is supported for CUCM registered Telepresence (TC/CE) endpoints using the HTTPS feedback sent from the endpoint directly.
- Conference Diagnostics will not work if the subscription fails on the endpoint.

- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 Service Pack 1.



- Note**
1. Cisco Prime Collaboration Assurance does not support Conference Monitoring for Cisco Jabber endpoints that are registered with Unified Communications Manager. You can view the utilization report and usage statistics of Cisco Jabber Video for TelePresence (Movi) endpoints only.
 2. The default Interval of Session Import Polling is 24 hours.
 3. Ensure that TS and TX endpoints are not included in the JTAPI.

Data Collection for Video Conferences

Cisco Prime Collaboration Assurance periodically polls the following video service infrastructure devices to get information on the conferences:

- Management devices (Cisco TMS)—Cisco Prime Collaboration Assurance gets information on the scheduled point-to-point and multipoint conferences. For Cisco TMS, if an unscheduled endpoint is added when the conference is in progress, Cisco Prime Collaboration Assurance shows the conference details for the newly added endpoint.

Cisco Prime Collaboration Assurance collects scheduled conferences data for five days (for the past one day, the current day, and for three days ahead).



- Note** If you are using Cisco TMS 13.0 or 13.1 configure the Booking API feature. For Cisco TMS 13.2 and above, you need not configure the Booking API feature.

- Multipoint Switches—Cisco Prime Collaboration Assurance gets information on the multipoint conferences. It also identifies and supports cascading of multipoint conferences.
- Multipoint Control Units (MCU and Cisco TS)—Conferences that are scheduled using these systems are always listed as ad hoc conferences in Cisco Prime Collaboration Assurance. These types of conferences are listed on the Conference Monitoring page only after the conference is started. Cisco Prime Collaboration Assurance polls these systems after receiving an event from the endpoints.

Cisco Prime Collaboration Assurance polls MCU and Cisco TS whenever these systems receive a call. Cisco Prime Collaboration Assurance polls MCUs that are not managed by Cisco TelePresence Conductor directly.

For conferences that are hosted by MCUs controlled by Cisco TelePresence Conductor, Cisco Prime Collaboration Assurance polls only the Cisco TelePresence Conductor.

Cisco Prime Collaboration Assurance does not support cascading of MCU conferences. Only Cisco TelePresence Conductor controlled MCU cascading is supported.

- Call and Conference Controls (Cisco Unified CM and Cisco VCS)—Cisco Prime Collaboration Assurance gets information on the participants using call processors. It collects details, such as when a user joins

the conference or disconnects from it. Cisco Prime Collaboration Assurance polls call and conference controllers periodically.

Cisco Prime Collaboration Assurance receives Connect or Disconnect events in real time from Cisco Unified CM and Cisco VCS. Whenever Connect or Disconnect events are missed, as a backup mechanism, Cisco Prime Collaboration Assurance polls Cisco Unified CM and Cisco VCS periodically for all In Progress calls. Hence, they are synchronized.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Cisco Prime Collaboration Assurance receives Connect or Disconnect events in real time from the endpoint (TC/CE) directly instead of Cisco Unified Communications Manager JTAPI.



Note

The following browsers are supported for the conference monitoring windows:

- Internet Explorer- versions 10, 11
- Mozilla Firefox- versions 31, 38
- Google Chrome- versions 39, 40

Cisco Unified CM

All endpoints must be added as JTAPI controlled devices in Cisco Unified CM. Otherwise, call detection for the endpoints does not happen in Cisco Prime Collaboration Assurance. The configured JTAPI user must have permission to access all endpoints that are managed in Cisco Prime Collaboration Assurance.

Cisco Prime Collaboration Assurance listens to the JTAPI events from the Cisco Unified CM. The endpoints are polled once the call is In Progress. Cisco Prime Collaboration Assurance depends on the JTAPI event to move the conference to the completed status.

Cisco Prime Collaboration Assurance manages multiple Cisco Unified CM clusters. Configure unique cluster IDs as it monitors conferences within a cluster and among clusters (intracluster and intercluster conferences).

Cisco Prime Collaboration Assurance must manage the cluster publisher to monitor a cluster. The JTAPI must be configured on the cluster publisher and the Computer Telephony Integration (CTI) service must be running in at least one node in a cluster. The CTI control limits depend on the visibility (Full) that you have set on the devices. For the visibility limits, see the [System Capacity for Cisco Prime Collaboration Assurance](#).

If JTAPI is not configured on Cisco Unified CM, then the endpoints registered to it are not shown as part of conferences. In this case, set the JTAPI configuration.



Note

To view the correct Usage Status details of endpoints that are added as JTAPI controlled devices, and to make the endpoints visible in the controlled list in Cisco Unified CM, you must reset the visibility of the endpoints. Use the **Edit Visibility** option under **Diagnose > Endpoint Diagnostics** to change the visibility of the endpoint from Full Visibility to Off, and then to Full Visibility again.

You can also rediscover Cisco Unified CM to make the endpoints visible and to display the correct Usage Status on Cisco Prime Collaboration Assurance servers.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Cisco TC/CE

For Cisco TC/CE endpoints registered to Cisco Unified Communications Manager, the events are received directly from the endpoint instead of Unified Communications Manager JTAPI.

Cisco VCS

Cisco Prime Collaboration Assurance listens to HTTP feedback events from the Cisco VCS. The endpoints are polled once the call is In Progress. Cisco Prime Collaboration Assurance depends on the HTTP feedback event to move the conference to the completed status.

Cisco Prime Collaboration Assurance manages multiple Cisco VCS clusters. You must configure unique cluster names as it monitors conferences within a cluster and among clusters (intracluster and intercluster conferences).

Cisco Prime Collaboration Assurance identifies and supports Cisco VCS Expressway traversal calls. For these calls, the media signal flows through Cisco VCS Control and Cisco VCS Expressway and the call details are displayed in the conference topology.

See the Cisco TelePresence Video Communication Server Control online help for details on traversal calls.

If there is a call outside the enterprise firewall, Cisco VCS Expressway is used. This device is configured to the Cisco VCS Control device. The Cisco VCS Control and Cisco VCS Expressway are displayed in the conference topology. However, the endpoints that are registered to the Cisco VCS Expressway are displayed as Unknown endpoints.

If Cisco Prime Collaboration Assurance is not subscribed to VCS through feedback subscription, VCS does not notify the PCA when a registered endpoint joins or leaves a conference, or registers or unregisters to VCS. In this case, set the visibility of those endpoint(s) to full as required, and contact your network administrator to check PC's feedback subscription to VCS.

**Note**

Cisco Prime Collaboration Assurance ignores Cisco VCS Expressway Connect/Disconnect events.

Import Conferences from Cisco TMS

The Cisco TMS contain details on the scheduled conferences. Cisco Prime Collaboration Assurance periodically polls these devices to retrieve the conference details. You can configure the frequency of the periodic polling based on your business needs.

To enable uninterrupted monitoring of the conferences, you can manage a Cisco TMS cluster using the Manage Clusters option (**Inventory > Inventory Management > Manage TMS Clusters**).

For Cisco TMS, if an unscheduled endpoint is added when the scheduled conference is in progress, Cisco Prime Collaboration Assurance shows the conferences details of that endpoint.

Cisco Prime Collaboration Assurance imports scheduled conferences data for five days (for the past one day, the current day, and for the next three days).

Note the following points when importing conferences from Cisco TMS:

- Cisco Prime Collaboration Assurance supports only the default email template for the Booking Confirm email in Cisco TMS. Conferences are not imported from Cisco TMS if the default email template is not used.

- "Reservation Only" meeting details are not imported from Cisco TMS. Cisco Prime Collaboration Assurance does not support this type of meeting because resources are not allocated for it while scheduling.

In addition to the periodic polling, if you want to import the conference details immediately, you can choose (**Diagnose > Conference Diagnostics > Import Conferences**).


Note

The Import Conferences task impacts Cisco Prime Collaboration Assurance System performance. Use Import Conferences only if it is required.

One job is created for the Import Conferences task. You can monitor this job at **System Administration > Job Management**. The job type is displayed as Synch_TMS-MEETING_UniqueJobID on the Job Management page.

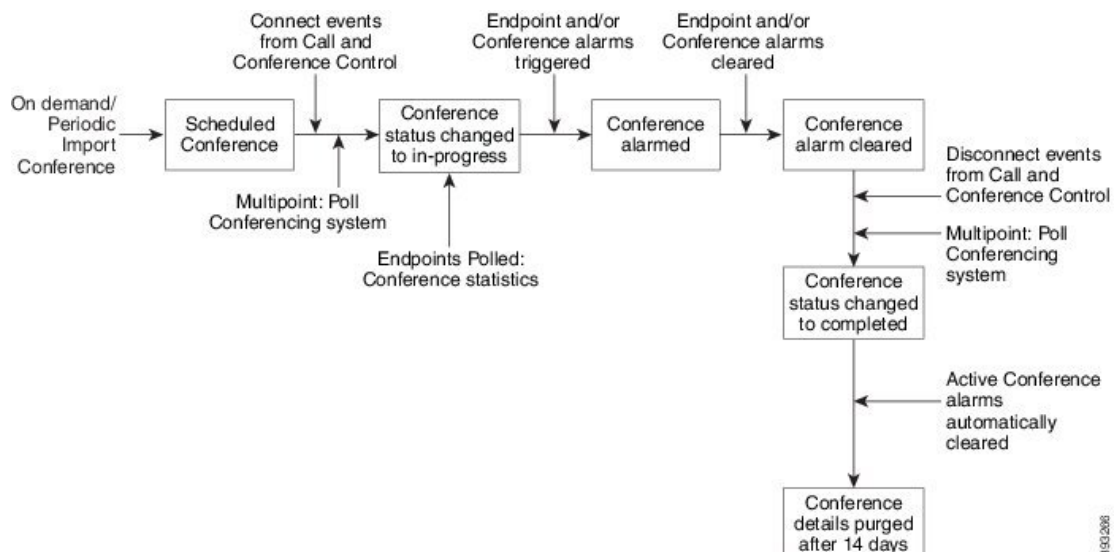
TMS_Conference_Import regular jobs run periodically and poll complete details of all conferences.

However, the TMS_Frequent_Conference_Import job runs frequently and retrieves only the changes in conferences after the previous polling. (You can change the frequency of polling on System Setup page).

Conference Workflow and Scenarios

The following chart shows the end-to-end scheduled conference workflow.

Figure 4: Scheduled Conference Workflow



The following are a few scenarios where Cisco Prime Collaboration Assurance does not contain up-to-date details on conferences or display different conference structure data:

- Cisco Prime Collaboration Assurance shows a scheduled conference (point-to-point, multipoint, or multisite) as an ad hoc conference if the conference gets scheduled and was In Progress after the last Cisco TMS poll and before the next scheduled or on-demand polling of the Cisco TMS takes place.
- For scheduled multipoint conferences, if Cisco Prime Collaboration Assurance is not synchronized with the management applications, the conference is shown as an ad hoc conference and it collects information from the participating Cisco MCU after Cisco Prime Collaboration Assurance receives a Connect event.

- If a conferencing system has moved either to the Unmanaged or Unknown state from the Managed state, then the multipoint conferences are displayed as multiple point-to-point conferences.
- Cisco TMS and Cisco MCU displays the conference status as Active immediately after the scheduled time is passed. However, Cisco Prime Collaboration Assurance does not change the conference status to In Progress until an endpoint joins the conference.
- Cisco Prime Collaboration Assurance displays conferences that include Unmanaged endpoints. However:
 - For point-to-point conferences, one of the endpoints must be managed in Cisco Prime Collaboration Assurance.
 - For multisite conferences, the endpoints that conference the other endpoints must be managed in Cisco Prime Collaboration Assurance.
 - For multipoint conferences, the conferencing devices must be managed in Cisco Prime Collaboration Assurance.
- If you have used Cisco TMS to reserve only TelePresence rooms, then Cisco Prime Collaboration Assurance does not display these conferences. (In Cisco TMS, this conference call type is identified as *Reservation Only*.)
- If Cisco VCS Expressway is in the Inaccessible state, Cisco Prime Collaboration Assurance can still monitor the conferences. However, the endpoints are displayed as Unknown endpoints.
- The Conference Diagnostic feature does not support endpoints, which are configured with multiple lines in Cisco Unified Communications Manager. However, you can manage these endpoints in the Cisco Prime Collaboration Assurance Inventory database.



Note The conference monitoring feature is supported only on Cisco Unified CM 8.5 and later.

- If there is a conference between a TelePresence and one or more WebEx participants, the Conference Diagnostics page does not display the details of the WebEx participants available in the call.
- Only the Cisco TelePresence Conductor with Cisco VCS (Policy Service) Deployment is supported. Cisco TelePresence Conductor with Cisco VCS (B2BUA) and Cisco TelePresence Conductor with Cisco Unified CM Deployment is not supported.

Conference Scenarios

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

Table 55: Conference Scenarios

Conference Classification	Conference Type	Conference Structure	Conference Topology Elements
Cisco Unified CM <i>intracluster</i> and <i>intercluster</i> conferences	Ad hoc, Scheduled	Point-to-point	Cisco TelePresence System 500, 1000, 3000, TX9000 Series.

Conference Classification	Conference Type	Conference Structure	Conference Topology Elements
Cisco Unified CM <i>intracluster</i> and <i>intercluster</i> conferences	Ad hoc, Scheduled Static	Multipoint	Cisco TelePresence System 500, 1000, 3000, TX9000 Series.
Cisco VCS <i>intracluster</i> and <i>intercluster</i> conferences	Ad hoc, Scheduled	Point-to-point	<p>Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20, and Cisco Jabber.</p> <p>If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the conference topology.</p>
Cisco VCS <i>intracluster</i> and <i>intercluster</i> conferences (with MCU)	Ad hoc, Scheduled Permanent (displayed as static)	Multipoint	<p>Cisco C series, EX Series, Cisco MCU, Cisco MSE¹, or Cisco TelePresence Server.</p> <p>If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the conference topology.</p>
Cisco VCS <i>intracluster</i> and <i>intercluster</i> conferences (without MCU)	Ad hoc, Scheduled	Multisite	<p>Cisco C series, EX Series, Cisco MX, Cisco MXP Series, Cisco IP Video Phone E20.</p> <p>If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the conference topology.</p>

Conference Classification	Conference Type	Conference Structure	Conference Topology Elements
Conferences between Cisco Unified CM and Cisco VCS clusters ²	Ad hoc	Point-to-point Multipoint	<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> conferences	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> conferences	Ad hoc, Scheduled Note Scheduler must be 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 • 1.8 or Cisco TelePresence Server

Conference Classification	Conference Type	Conference Structure	Conference Topology Elements
Conferences outside the enterprise firewall - Cisco VCS Expressway	Ad hoc Permanent (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	<p>Point-to-point</p> <p>When a call is put in a conference mode or when merged with another call, it becomes Multipoint. The conference does not show the MCU. When the first participant leaves the call, the conference shows it is connected to the MCU, while the second and third participants continue in the same call as a point-to-point call.</p> <p>Note This scenario is applicable when in-built video bridge capability is not present in the endpoint.</p>	<p>Multipoint conferencing devices and video endpoints.</p> <p>For a list of the supported endpoints, see Supported Devices for Cisco Prime Collaboration Assurance.</p>

Conference Classification	Conference Type	Conference Structure	Conference Topology Elements
Conferences 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 Assurance does not monitor a Multisite conference 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.

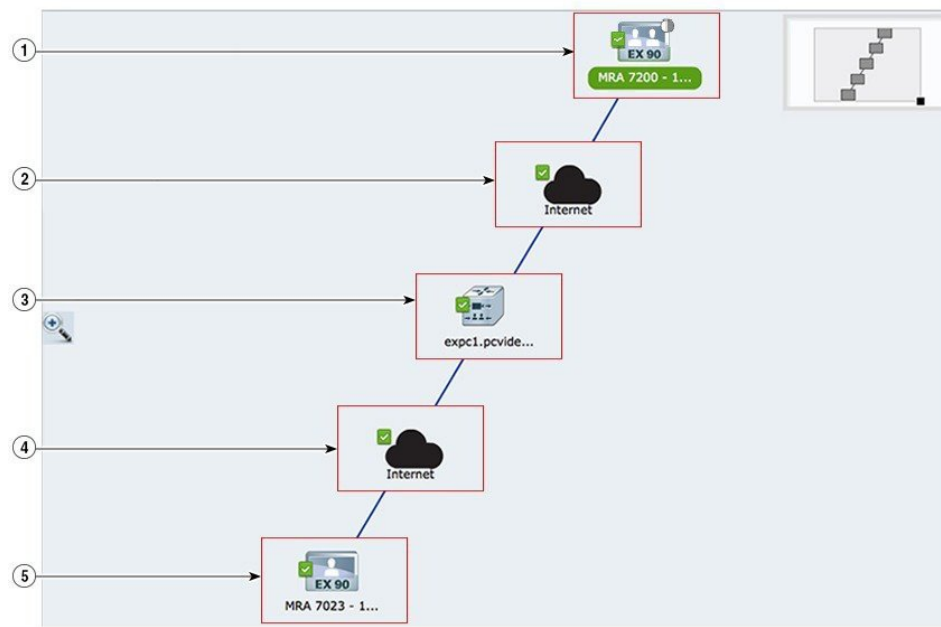


Note

- Cisco Jabber devices support only ad hoc conferences.

The following image describes the conference topology between two MRA endpoints.

Figure 5: Conference Topology Between MRA Endpoints



1, 5	MRA endpoints that connect with each other through cloud server. Note You cannot view the conference statistics for MRA endpoints.
2, 4	Internet cloud servers that connect the MRA endpoints. The MRA endpoints can connect only with the help of cloud servers. You cannot view the conference statistics since the system cannot get the IP addresses of the endpoints from the cloud servers.
3	Cisco VCS Expressway Core that acts as the call controller device. The topology displays the Cisco VCS Expressway Core and the associated endpoints.

The various Collaboration Edge conferences involving MRA endpoints and VCS Expressway Core are as follows:

- Point-to-point: Conference between two MRA endpoints that are connected with each other through cloud servers and Cisco VCS Expressway Core
- Multipoint: Conference with more than two MRA endpoints that are connected through cloud servers, Cisco VCS Expressway Core, and TPS or MCU
- Multisite: Conference with more than two MRA endpoints that are connected without TPS or MCU

**Note**

Each of the above conferences may also have one non-MRA endpoint connected at either end.

Table 56: Conference Scenarios for MSP Mode

Conference Classification	Conference Type	Conference Structure	Conference Topology Elements
Customer calls in a NAT environment.	Ad hoc	Point-to-point	Conference Border Controller (SBC) and video endpoints. For a list of supported endpoints, see Supported Devices for Cisco Prime Collaboration Assurance .

Conference Diagnostics Dashboard

To access the Conference Diagnostic dashboard, choose **Diagnose > Conference Diagnostics**.

The Conference Diagnostic dashboard provides details on a conference and the endpoints that are involved in that conference.

You can monitor conferences based on device type, by selecting the desired group from the Group drop-down filter. You can further filter based on the conference type using the Show filter in the Video Collaboration Conferences pane.

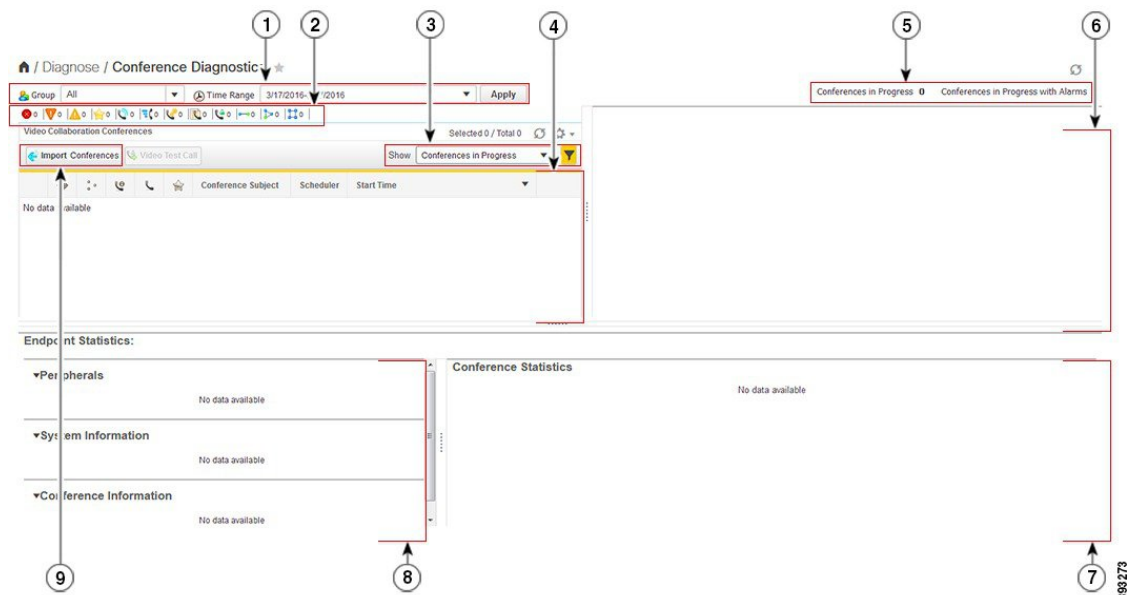
The All Video Collaboration Conferences table contains information for the current date (24 hours) by default. Rest your mouse pointer over the Import Conferences button to see details of when the data was last imported into the Cisco Prime Collaboration Assurance database.



Note The Conference Diagnostics feature in Cisco Prime Collaboration Assurance does not support the phones configured with Shared Directory Numbers.

The following image shows the Conference Diagnostics Dashboard.

Figure 6: Conference Diagnostics Dashboard



1	<p>Predefined Group filter drop-down list. Also includes a launch point for a calendar. By default, the All Video Collaboration Conferences table contains information for the current date (24 hours).</p> <p>You can view conferences for the past 30 days and the next 3 days.</p>	2	<p>Quick summary pane for alarms and conferences.</p>
---	---	---	---

3	Predefined filters drop-down list. Also, includes Refresh icon and Table setting icon. Using the Table setting icon, you can customize the table column and fix any row to either the top or bottom.	4	Video Collaboration Conferences
5	Count for total number of in-progress conferences (normal and alarmed) and in-progress alarmed conferences for the specified date.	6	Conference topology pane.
7	Conference statistics pane.	8	Endpoint statistics pane. This pane contains details on peripherals, system, and conferences.
9	Launch point for the import conference task. Rest your mouse pointer over the Import Conferences button to see details on when the data was last imported into the Cisco Prime Collaboration Assurance database.		

The summary pane displays the conference details for the current day (00:00:00 hours to 23:59:00 hours). You can view the icon-based summary of the data available in the Video Collaboration Conferences table. You can view the DSCP value for Cisco Unified IP Phones 8941 and 8945, Cisco DX Series, and Cisco TelePresence TX Series. Select the conference (**Diagnose > Conference Diagnostics**) with the preceding endpoint (s). In the Conference Statistics pane, the DSCP In field displays the DSCP value received from the endpoint in the conference.

The Video Collaboration Conferences table displays the details of in-progress conferences for the current date (00:00:00 hours to 23:59:59 hours). The latest conference detail is listed at top of the table.

If you want to view details for the previous or the next day, you can choose the date, using the calendar. You can choose any of the filters from the Show drop-down list to view other conference details.

Cisco Prime Collaboration Assurance keeps conference details for the last 30 days.



Note

On deletion of a CUCM cluster or CUCM node or VCS or Video endpoint all the past and ongoing conferences associated with the endpoint(s) will be purged. Consequently, the associated sessions are not visible in Conference Diagnostics page.

Apart from video collaboration conferences, you can see conferences between an IP Phone or Software Client and TelePresence Endpoint in the Conference Diagnostics Dashboard. Ensure that you set the visibility of these devices to Full Visibility. To know more about visibility, see [Realtime Visibility of an Endpoint](#).

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you see the In-progress conferences shown as Ad Hoc Conferences when the call was scheduled in TMS was made by selecting MCU as a conferencing device.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you see the details of a point-to-point call between two customers (through phones registered to different Unified CMs) using Conference Border Controller(s). Ensure that the Conference Border Controller(s) is or are in managed state in Inventory Management to get the details of such calls.

Support for a New Method of Conferencing - Ad hoc Calls

This feature provides monitoring of new ad hoc conference calls on the Conference Diagnostics page (**Diagnose > Conference Diagnostics**).

Prerequisite - The Multipoint Control Unit (MCU) and endpoints must be in a Managed state in Cisco Prime Collaboration Assurance.

When a call is put in a conference mode (by pressing the conference button) or when merged with another call, it becomes a Multipoint ad hoc call. Cisco Unified CM allocates the MCU that behaves as a conferencing device for the call. In this case, the conference topology displays the MCU. When the first participant leaves the call, the second and third participant continues in the same call which becomes a Point-to-Point ad hoc call. In this case, the conference topology does not display the MCU.

When the Multipoint Control Unit (MCU) is in Suspended state in Cisco Prime Collaboration Assurance and a conference is made, instead of a single ad hoc call, Cisco Prime Collaboration Assurance shows two Point-to-Point calls with the second call leg between the endpoint and Multipoint Control Unit (MCU). After a few minutes, the call is connected between the endpoint that triggered the call and the Multipoint Control Unit (MCU). Other endpoints are not shown in the topology. This scenario is applicable when inbuilt video bridge capability is not present in the endpoint.

Monitoring of Cisco Unified Communications Manager—Cisco TelePresence Conductor Integrated Conferences

This feature enables you to monitor conferences that are created by a Cisco Unified CM that is integrated with a Cisco TelePresence Conductor.

Prerequisites:

- Cisco TelePresence Conductor, and Multipoint Control Unit (MCU) should be in Managed state in Cisco Prime Collaboration Assurance.
- The conference bridges on the Cisco TelePresence Conductor should be discovered as part of the Logical discovery of the conductor. If you are using the Add Device or Import feature to discover the Cisco TelePresence Conductor, ensure that you perform a subsequent rediscovery using the Rediscover feature with the Enable Logical discovery check box selected.
- Configure Cisco Unified CM to use a Cisco TelePresence Conductor to manage the conference bridge resources for ad hoc and rendezvous conferences. For information, see [Cisco TelePresence Conductor with Cisco Unified CM Deployment Guide \(XC2.3\)](#).



Note Logical Discovery is not supported in MSP mode.

For a call that includes conferencing device - Multipoint Control Unit (MCU), you can view the details of the associated conductor from the Endpoints Quick View of the conferencing device (MCU) under the Conference topology pane on the Conference Diagnostics page (**Diagnose > Conference Diagnostics**).

Cascading of Cisco TelePresence Server

This feature allows you to monitor Cisco TelePresence servers during ad hoc conference calls on the Conference Diagnostics page (**Diagnose > Conference Diagnostics**).

Prerequisite -

- The Cisco TelePresence Server (TPS), Cisco TelePresence Conductor, and endpoints should be in a Managed state in Cisco Prime Collaboration Assurance.
- Ensure that you set the visibility of the devices to Full Visibility.

During an ad hoc conference, when a primary TPS server is unable to respond to a call over a Cisco TelePresence Conductor, it cascades the call to a secondary TPS server. Cascading occurs when multiple TPS servers share the load during a conference call. The conference topology creates link between the primary and secondary TPS servers with associated participants and displays all the cascaded TPS servers as conference bridges.



Note Conference troubleshooting is not supported in Cisco Prime Collaboration Assurance.

Realtime Visibility of an Endpoint

The visibility feature for a managed endpoint determines to what level Cisco Prime Collaboration Assurance monitors the operations of the endpoint. Only endpoints in the Managed state can be edited for visibility. If you edit the visibility settings for endpoints whose visibility level exceeds the maximum visibility, the changes are not updated. Visibility setting controls the polling of endpoints in addition to conference monitoring. Polling is performed only for devices that are configured for real-time full visibility and not all devices.

Cisco Prime Collaboration Assurance supports the following types of visibility:

- **Full Visibility** - Call detection using JTAPI/ HTTP feedback and realtime monitoring information such as conference statistics, and conference information is supported.



Note The following endpoint stats listed in the table below are not supported:

1. Cisco Jabber Video for TelePresence (Movi)
2. MRA Endpoints

- Off - Call detection using JTAPI/ HTTP feedback and realtime monitoring information are not supported. These endpoints are displayed on the Conference Monitoring page with a fully dimmed icon.

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) 	Full	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
For Cisco Prime Collaboration Release 11.6 and later Cisco TelePresence 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 	Full	Full

There is full visibility (default and maximum) for Total Endpoints . There is no visibility for IP Phones and Software Clients by default. The maximum visibility for IP Phones and Software Clients is full.

For a point-to-point ad hoc conference, if visibility is Off for one endpoint and Full for the other, the endpoint with Off visibility is shown with a fully dimmed icon in the conference topology.

For a Multipoint conference, an endpoint with Off visibility is not displayed in the conference topology.

For scheduled point-to-point or multipoint conferences, endpoints with Off visibility are shown with a fully dimmed icon in the conference topology.

To view the visibility of an endpoint, choose **Inventory > Inventory Management** and then view the Visibility column in the inventory table for the corresponding endpoint.



Note If you are not able to view this column, click the Settings button, click **Columns**, and then click **Visibility** in the list that appears.

To change the visibility of an endpoint, choose **Inventory > Inventory Management** and select an endpoint, and then click **Edit**. You can see the current visibility of the endpoint. If you have any made any changes, click **Save**.



Note If you select more than one endpoint, you cannot view the current visibility of the endpoints.

Any changes to the visibility settings are implemented from the next conference onward.

The visibility feature is applied on the Conference Diagnostics page only. That is, even if you have set visibility to Off, the endpoint is listed in the Endpoint Diagnostics and Inventory pages.

Limitations

1. The Conference Diagnostic feature does not support endpoints, which are configured with multiple lines in Cisco Unified Communications Manager. However, you can manage these endpoints in the Cisco Prime Collaboration Assurance Inventory database.
2. The Conference Diagnostics feature in Cisco Prime Collaboration Assurance does not support the phones configured with Shared Directory Numbers.
3. The number of meetings should not exceed the maximum limit set for the profile. For more information, see [System Capacity for Cisco Prime Collaboration Assurance](#).
4. Session Monitoring will continue to use non-secure JTAPI communication to monitor sessions in UCM Mixed mode.
5. Ensure to set the visibility of the devices to “Full Visibility” state.
6. Cisco Prime Collaboration Assurance shows a scheduled conference (point-to-point, multipoint, or multisite) as an ad hoc conference if the conference gets scheduled and was In Progress after the last Cisco TMS poll and before the next scheduled or on-demand polling of the Cisco TMS takes place.
7. A few of the Call scenarios are not supported. For more information, see the section on "[Conference Workflow and Scenarios](#)".

360° Conference View

The 360° Conference View provides a complete view of pertinent data about endpoint, infrastructure devices, alarms, and call records. It also enables you to cross launch other Cisco Prime Collaboration Assurance features. To see the 360° conference View for a conference, rest your mouse pointer over the Conference Subject column in the Video Collaboration Conferences table and click the 360° Conference View icon.

The 360° Conference View contains the following tabs:

- **Alarms** — Displays the alarm severity, the source that triggered the alarm, the description of the generated alarm, and the time stamp.
- **Endpoints** — Displays the endpoint name, IP address, physical location, conference duration, and device model.
- **Infrastructure** — Displays the details of the infrastructure devices in use. You can launch the Infrastructure Devices login page using the IP address link. You can also launch the Inventory page to view the inventory details of the device by clicking the Device Name.

You can perform the following actions in the 360° Conference View:

- Click the See Alarms icon to launch the Alarm browser. The Alarm browser lists all alarms for the selected conference (includes both conference and endpoints alarms).
- Click the Monitor Endpoint icon to launch the Endpoint Diagnostics page.
- Click the Add to Watch list icon to add a conference to the watch list. It is enabled for scheduled and in-progress conferences.
- If you have scheduled a recurring conference, add each instance of the recurring conference to the watch list. For example, if you have scheduled a recurring conference for every day over 5 days, add the conference to the watch list for every day (5 days).

**Note**

Adding conference to the watch list does not trigger the troubleshooting workflow.

Conference Topology

The conference topology displays the endpoints that are part of a conference. If it is a multipoint conference, the conferencing devices are displayed along with the endpoints. Also, if the call is a traversal call, Cisco VCS is displayed.

To launch the conference topology, select a conference in the Video Collaboration Conferences table.

The alarm badge displayed on the link and endpoints indicates a fault in the delivery of packets and the peripherals, respectively.

The following figure shows the different statuses displayed in the conference topology.

Figure 7: Session Topology

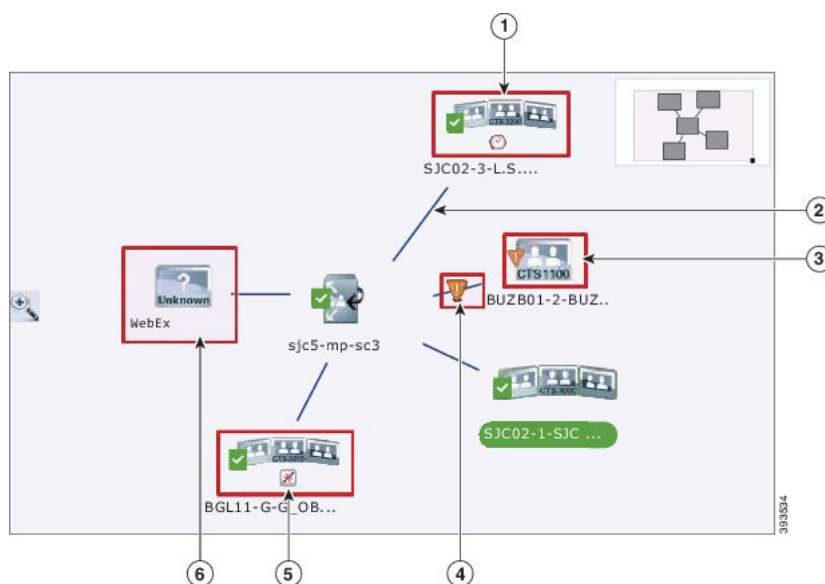


Table 57:

Number	Description	Number	Description
1	A No-Show icon associated with an endpoint.	2	An active link between an endpoint and a Multipoint Switch without alarms.
3	An endpoint with a major alarm that participates in the session. The problem is in peripheral devices.	4	An active link between an endpoint and a Multipoint Switch with a major alarm.

Number	Description	Number	Description
5	A Disconnect icon associated with an endpoint.	6	Unknown endpoint; an endpoint that is not currently managed in Cisco Prime Collaboration Assurance. The inventory details for these endpoints may not be available in the Cisco Prime Collaboration Assurance database. The endpoints and controllers must be in the Managed state also the registration status should be available in the Device 360° view. The endpoints that are registered to the Cisco VCS Expressway are also displayed as Unknown endpoints. A managed endpoint in Cisco Prime Collaboration Assurance can make a call to an unsupported endpoint.

If there is a fault in the network, the alarm badge is displayed on the network line. You can launch a quick view on the topology to identify the network link direction where the fault has occurred.

Network Link Quick View

To launch the quick view, rest your mouse pointer over the alarm badge and click the quick view icon. The network link quick view contains the following tabs:

- Link Summary — Displays the alarm status between the endpoints for point-to-point conferences and between an endpoint and Multipoint Switch for multipoint conferences.
- Alarms Summary — Displays the alarm severity, the source that triggered the alarm, and the description of the generated alarm.
- Call Details — Displays the endpoint name, phone number, and protocol. These details are displayed for the endpoints connected through the selected network link.

Endpoints Quick View

You can launch a quick view for endpoints in the Managed and Unknown states. To launch the quick view, rest your mouse pointer over an endpoint and click the quick view icon.

For devices in Managed state, the following details are displayed:

- **Endpoint Summary** — Displays the endpoint details such as system type, IP address (IPv4 or IPv6), physical location, usage status, directory number (SIP URI or H323 ID), cluster ID, and so on.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which that endpoint belongs to, and the Private IP and Public IP addresses respectively. You can click the Public IP address to launch the endpoint's Management Application.

- **Alarms Summary** — Displays the Alarm Severity, the Category of the alarm, and the Description of the generated alarm.

From the quick view, you can add an endpoint to the watch list, launch the Endpoint Diagnostics page, and view the alarms for the selected endpoint.

Conferencing Resource - Cisco Prime Collaboration Assurance also lets you view information about the region that the MCU belongs to.

Endpoint Statistics

You can monitor the Quality of Service (QoS) of the endpoints in this pane. Endpoint statistics are displayed for in-progress and past conferences. Also, the peripheral status and system information are available for the scheduled conferences.

This page displays information on the peripheral status, endpoint system details, conference details, and conference statistics for a selected endpoint in the conference topology pane.

In a Multisite conference, the conference statistics (audio and video) and conference information are displayed for each connected endpoint when the center endpoint (conferencing device) is selected.



Note Conference statistics details (present and past) are not displayed for Cisco IP Phones.

Conference Statistics

The Conference Statistics pane displays the statistics information, such as packet loss, latency, jitter, and so forth, for:

- **Audio** — Primary codec, secondary codec 1 and 2, auxiliary and primary legacy.
- **Video** — Primary codec and secondary codec 1 and 2.

The information displayed varies, based on the endpoint type that you have selected.

A black vertical line indicates the threshold value. You can define the threshold value for Rx packet loss, average period jitter, and average period latency using the **Alarm & Report Administration > Event Customization > Threshold Rules** option.

Red indicates that the value has exceeded the defined threshold. Gray indicates the current value. This color is used for those parameters that do not contain threshold values.

An alarm badge indicates the actual fault in the network. For past conferences, Cisco Prime Collaboration Assurance does not display the threshold value or alarm badge-in conference statistics.

All conference and endpoint statistics data older than one day are purged.



CHAPTER 21

Enable Cisco APIC-EM to Troubleshoot Conference

This section explains the following:

- [Enable Cisco APIC-EM to Troubleshoot Conference, on page 269](#)

Enable Cisco APIC-EM to Troubleshoot Conference

This chapter provides information about enabling Cisco APIC-EM to troubleshoot conference.

Overview of Cisco APIC-EM

For Cisco Prime Collaboration Release 11.6 and later

Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) provides centralized automation of policy-based application profiles. Cisco APIC-EM works with existing network infrastructure and automates the deployment and compliance checking of network policies across the entire network. For more information, see [Cisco Application Policy Infrastructure Controller Enterprise Module](#). For information on deployment of Cisco APIC-EM in your network, see [Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide](#).

Cisco Prime Collaboration Assurance integrates with Cisco APIC-EM to trace and monitor any in-progress voice or video conference media path, and automatically troubleshoots the network elements that cause quality degradation in a media path.

The following are the key features of Cisco APIC-EM:

- Monitors midpoints or enterprise network devices (routers, switches, and hosts) for media path troubleshooting.
- Relies upon 5-tuple (Source IP Address, Destination Address, Source Port, Destination Port, and Protocol) that are received from Cisco Prime Collaboration Assurance to perform Path Trace.



Note

For more information on Path Trace and its limitations, see the *Performing Path Traces* section in the [Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide](#).

- Requires both SNMP and CLI credentials to manage the devices.
- Provides media path and path statistics information (device statistics, interface statistics, and PerfMon statistics) for a given flow directly to Cisco Prime Collaboration Assurance.
- Performs on-demand PerfMon configuration on midpoints for a given flow to fetch media flow statistics. The PerfMon configuration is removed when the troubleshooting conference ends.



Note For more information on the platform on which the PerfMon data can be collected, see the http://apic-em/wiki/Category:Testing/Platform_Support#APIC-EM_PLATFORM_SUPPORT wiki page.

- Enables path troubleshooting for destination endpoint that is in unknown state.



Note • You can upgrade to Cisco Prime Collaboration Assurance 11.5 Service Pack 1 from 11.5 release only.

Cisco APIC-EM Controller Integration Settings

Cisco Prime Collaboration Assurance allows you to troubleshoot the quality issues of media conference using Cisco APIC-EM Controller Integration Settings under **Alarm & Report Administration > APIC-EM & Prime Integration**.

Before you begin

Ensure that the user is assigned with the role `ROLE_POLICY_ADMIN` in Cisco APIC-EM.

Step 1 Choose **Alarm & Report Administration > APIC-EM & Prime Integration**.

Step 2 Enter the valid Cisco APIC-EM credentials in **APIC-EM Controller Integration Settings** pane and click **Save**.

a) If Cisco APIC-EM APIs are accessible with the credentials entered, Cisco Prime Collaboration Assurance saves the configuration details in the database and displays the popup message.

APIC-EM credentials are saved successfully.

b) If Cisco APIC-EM APIs are not accessible with the credentials entered, Cisco Prime Collaboration Assurance displays a warning message.

APIC-EM is not accessible with the credentials provided. Please verify the credentials and try again.

Step 3 Click **Reset** to clear the Cisco APIC-EM configurations details in **APIC-EM Controller Integration Settings** pane.

Note Cisco APIC-EM version 1.2.x has been validated with Cisco Prime Collaboration Assurance Release 11.5 Service Pack 1.

Cisco APIC-EM Controller Integration Settings Pane - Field Descriptions

Table 58: Field Descriptions for Cisco APIC-EM Controller Integration Settings Pane

Field	Description
IP Address	Cisco APIC-EM Controller Management IP Address of the cluster. Enter reachable host IP address or virtual IP address address of APIC-EM cluster.
HTTP Username and Password	Login credentials of Cisco APIC-EM Server.

Troubleshooting

Issue: Test connectivity fails.

Recommendations:

- Ensure that Cisco APIC-EM APIs are accessible with the credentials provided in field of **APIC-EM Controller Integration Settings Pane**.
- Ensure that you are assigned with the role `ROLE_POLICY_ADMIN`.

Conference Troubleshooting with Cisco APIC-EM

The following procedure contains the high-level steps to troubleshoot a conference.

Before you begin

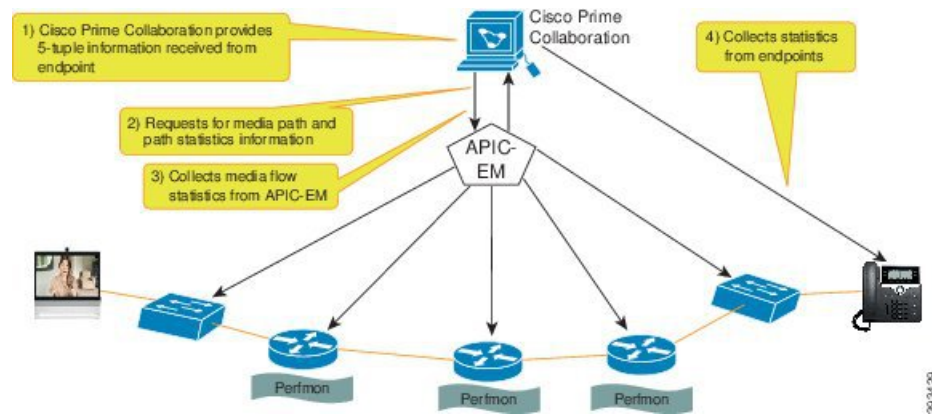
Ensure that Cisco Prime Collaboration Assurance is integrated with Cisco APIC-EM. For more information, see [Cisco APIC-EM Controller Integration Settings, on page 270](#).

-
- | | |
|---------------|---|
| Step 1 | <p>Cisco Prime Collaboration Assurance initiates SDN Path Trace by providing 5-tuple information received from endpoint for the given call leg.</p> <p>Cisco APIC-EM creates a flow to keep track of the request.</p> |
| Step 2 | <p>Cisco Prime Collaboration Assurance uses the flow to collect the media path and path statistics information.</p> <p>Cisco APIC-EM enables performance monitoring configuration on the devices (ingress or egress interface) involved in the path for a given flow. The PerfMon configuration is removed when troubleshooting ends.</p> |
| Step 3 | <p>Cisco Prime Collaboration Assurance collects the media flow statistics (for example, Packet Loss, Jitter, and CPU utilization) for each node from the Cisco APIC-EM Controller periodically.</p> |
| Step 4 | <p>Cisco Prime Collaboration Assurance continues to poll the endpoints to collect the media statistics from the endpoints.</p> |
-

Example

The following image shows the interaction between Cisco Prime Collaboration Assurance and Cisco APIC-EM to troubleshoot a conference.

Figure 8: Interaction between Cisco Prime Collaboration Assurance and Cisco APIC-EM





CHAPTER 22

Monitor the Cisco Prime Collaboration Assurance Server

This section explains the following:

- [Monitor the Cisco Prime Collaboration Assurance Server, on page 273](#)

Monitor the Cisco Prime Collaboration Assurance Server

For Cisco Prime Collaboration Release 11.5 and later

You can monitor the Cisco Prime Collaboration Assurance Server health using the Cisco Prime Collaboration Assurance application. You can get information on CPU, memory, disk utilization, logical storage areas, and process details.

Prerequisites:

- Enable SNMP v1, v2c, or v3 in Cisco Prime Collaboration Assurance. For more information on enabling SNMP v1, v2c, and v3, See the *Configuring Cisco Prime Collaboration Assurance Server* section in [Configure Devices for Prime Collaboration Assurance](#).
- Enable SNMP v1/v2c using admin access. Root access is not needed to enable SNMP v1/v2c.
- Enable SNMP v3 using root access. You need to raise a TAC case to get the root access.
- Connect to Cisco Prime Collaboration Assurance Server from a SNMP Manger using SNMP v1, v2c, or v3 RO community string in settings.

Monitor Cisco Prime Collaboration Server Health

The MIB details required to monitor the health of Cisco Prime Collaboration Assurance Server are listed in the following table:

Component	Table	OID	MIB
CPU	systemStats	1.3.6.1.4.1.2021.11	UCD-SNMP-MIB
Memory	memory	1.3.6.1.4.1.2021.4	UCD-SNMP-MIB
Disk Storage	hrDeviceTable	.1.3.6.1.2.1.25.3.2	HOST-RESOURCES-MIB
	hrDiskStorageTable	.1.3.6.1.2.1.25.3.6	

Component	Table	OID	MIB
Logical Storage areas	hrStorageTable	.1.3.6.1.2.1.25.2.3	HOST-RESOURCES-MIB
Process	hrSWRunTable	.1.3.6.1.2.1.25.4.2	HOST-RESOURCES-MIB

Example:

- To monitor the CPU utilization

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
# snmpwalk -v2c -c public <PCA IP> UCD-SNMP-MIB::systemStats
```

Example

```
snmptable -v 2c -c public 10.64.91.115 UCD-SNMP-MIB::systemStats
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u user1  
-a MD5 <PCA IP> UCD-SNMP-MIB::systemStats
```

Example

```
snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u jane  
-a MD5 <PCA IP> UCD-SNMP-MIB::systemStats
```

Sample Output

```
UCD-SNMP-MIB::ssIndex.0 = INTEGER: 1
UCD-SNMP-MIB::ssErrorName.0 = STRING: systemStats
UCD-SNMP-MIB::ssSwapIn.0 = INTEGER: 0 kB
UCD-SNMP-MIB::ssSwapOut.0 = INTEGER: 0 kB
UCD-SNMP-MIB::ssIOSent.0 = INTEGER: 609 blocks/s
UCD-SNMP-MIB::ssIOReceive.0 = INTEGER: 0 blocks/s
UCD-SNMP-MIB::ssSysInterrupts.0 = INTEGER: 994 interrupts/s
UCD-SNMP-MIB::ssSysContext.0 = INTEGER: 5508 switches/s
UCD-SNMP-MIB::ssCpuUser.0 = INTEGER: 6
UCD-SNMP-MIB::ssCpuSystem.0 = INTEGER: 0
UCD-SNMP-MIB::ssCpuIdle.0 = INTEGER: 87
UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 15940286
UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 14270
UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 1046654
UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 193992466
UCD-SNMP-MIB::ssCpuRawWait.0 = Counter32: 6614683
```

```
UCD-SNMP-MIB::ssCpuRawKernel.0 = Counter32: 0
```

- To monitor the memory utilization

If you have enabled SNMP v1 or v2c, enter the following commands :

Syntax

```
# snmpwalk -v2c -c public <PCA IP> UCD-SNMP-MIB::memory
```

Example

```
snmpwalk -v 2c -c public 10.64.91.115 UCD-SNMP-MIB::memory
```

If you have enabled SNMP v3, enter the following commands :

Syntax

```
snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u user1  
-a MD5 <PCA IP> UCD-SNMP-MIB::memory
```

Example

```
snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u jane  
-a MD5 <PCA IP> UCD-SNMP-MIB::memory
```

Sample Output

```
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 25165816 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 25165724 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 14236500 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 848220 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 26013944 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 516240 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 3495964 kB
UCD-SNMP-MIB::memSwapError.0 = INTEGER: noError(0)
UCD-SNMP-MIB::memSwapErrorMsg.0 = STRING:
```

- To monitor the disk storage details

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
snmpwalk -v 2c -c public <PCA IP> [OID]
```

Example

```
snmpwalk -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.3.2
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmptranslate -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> [OID]
```

Example

```
#snmptranslate -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> .1.3.6.1.2.1.25.3.2
```

Sample Output

Table 59: SNMP table: HOST-RESOURCES-MIB::hrDeviceTable

hrDeviceIndex	hrDeviceDescr	hrDeviceType	hrDeviceID	hrDeviceStatus	hrDeviceErrors
1552	HOST-RESOURCES-MIB::hrDeviceTypes::hrDeviceDiskStorage	SCSI disk (/dev/sda)	SNMPv2-MIB::hrDeviceID	running	?
1538	HOST-RESOURCES-MIB::hrDeviceTypes::hrDeviceDiskStorage	VMware Virtual IDE CDROM Drive	SNMPv2-MIB::hrDeviceID	running	?

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
snmptranslate -v 2c -c public <PCA IP> [OID]
```

Example

```
snmptranslate -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.3.6
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmptranslate -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> [OID]
```

Example

```
#snmptranslate -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> .1.3.6.1.2.1.25.3.6
```

Sample Output

Table 60: SNMP table: HOST-RESOURCES-MIB::hrDiskStorageTable

hrDiskStorageAccess	hrDiskStorageMedia	hrDiskStorageRemoveable	hrDiskStorageCapacity
readWrite	unknown	true	0KBytes
readWrite	unknown	false	262144000 KBytes

- To monitor the logical storage areas

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
snmp table -v 2c -c public <PCA IP> [OID]
```

Example

```
snmp table -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.2.3
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmp table -v 3 -A authpassword -X privpassword -x AES -l authPriv -u  
user1 <PCA IP> [OID]
```

Example

```
#snmp table -v 3 -A authpassword -X privpassword -x AES -l authPriv -u  
user1 <PCA IP> .1.3.6.1.2.1.25.2.3
```

Sample Output

Table 61: SNMP table: HOST-RESOURCES-MIB::hrStorageTable

hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageUnits	hrStorageSize	hrStorageUsed	hrStorageAlloc
1	HOST-RESOURCES-MIB::hrStorageTypePhysicalMemory	Physical memory	1024 Bytes	14236500	13338404	?
3	HOST-RESOURCES-MIB::hrStorageTypeVirtualMemory	Virtual memory	1024 Bytes	39402316	13338496	?

- To monitor the process details

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
snmp table -v 2c -c public <PCA IP> [OID]
```

Example

```
snmp table -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.4.2
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmp table -v 3 -A authpassword -X privpassword -x AES -l authPriv -u  
user1 <PCA IP> [OID]
```

Example

```
#snmp table -v 3 -A authpassword -X privpassword -x AES -l authPriv -u  
user1 <PCA IP> .1.3.6.1.2.1.25.4.2
```

Sample Output

Table 62: SNMP table: HOST-RESOURCES-MIB::hrSWRunTable

hrSW RunIndex	hrSW RunName	hrSW RunID	hrSW RunParameters	hrSW RunType	hrSW RunStatus	hrSW Runpath
2367	postgres	SNMPv2-SMI : : zeroDotzero	""	application	runnable	postgres: cmuser cpcm 127.0.0.1 (51478) idle
2643	postmaster	SNMPv2-SMI : : zeroDotzero	""	application	runnable	postgres: primea cqdb 127.0.0.1 (50175) FETCH



PART VI

Dashboards and Reports

- [Cisco Prime Collaboration Assurance Dashboards](#), on page 281
- [Cisco Prime Collaboration Assurance Reports](#), on page 377



CHAPTER 23

Cisco Prime Collaboration Assurance Dashboards

This section explains the following:

- [Cisco Prime Collaboration Assurance Dashboards, on page 281](#)

Cisco Prime Collaboration Assurance Dashboards

The Cisco Prime Collaboration Assurance dashboards provide consolidated information for devices, applications, and endpoints. With these dashboards, you can:


- Monitor all endpoints for a user using a single interface.
- Determine service experience for all endpoints.

For Cisco Prime Collaboration Release 11.5 and later

Determine Call Quality for all endpoints.

For data to be populated in the dashboards, you must complete the following tasks:

- Discover the devices
- Import the conference (for Conference-related dashboards)
- Poll the devices

Click the Toggle Navigation icon  on the **Cisco Prime Collaboration Assurance** page to view a list of dashlets and reports. You can click the pin icon at the top left to hide or display the left pane. You can also view indexes, set favorites, and use the search option in the same menu.



Note

To view the complete title of the Cisco Prime Collaboration Assurance on the black ribbon frame, you must change the screen resolution of the computer. Click the Toggle pin button on the top left pane on the Index to view the title.

The following table describes the Cisco Prime Collaboration Assurance dashboards.

Dashboard	Description	Prime Collaboration Assurance Deployment
OpsView (Monitor> System View> OpsView)	Provides high-level information about the Cisco Unified CM and VCS clusters.	Prime Collaboration Assurance Advanced
Service Experience (Monitor> System View> Service Experience)	Information about sessions and alarms.	Prime Collaboration Assurance Advanced
Alarm (Monitor> System View> Alarm)	Information about management devices.	Prime Collaboration Assurance Advanced
Performance (Monitor> System View> Performance)	Provides details on critical performance metrics of each managed element.	Prime Collaboration Assurance Advanced
Contact Center Topology (Monitor> System View> Contact Center Topology)	Information about the Contact Center components such as CUIC, Finesse, MediaSense, CVP and UCCE.	Prime Collaboration Contact Center Assurance
Utilization Monitor (Monitor> Utilization Monitor)	Information about endpoints and their utilization, conferencing devices, and license usage.	Prime Collaboration Assurance Advanced

For Cisco Prime Collaboration Release 11.5 and later

Dashboard	Description	Cisco Prime Collaboration Deployment
OpsView (Network Health Overview > OpsView)	Provides high-level information about the Cisco Unified CM and VCS clusters.	Cisco Prime Collaboration Assurance Advanced
Call Quality (Network Health Overview > Call Quality)	Information about quality of service.	Cisco Prime Collaboration Assurance Advanced
Alarm (Network Health Overview > Alarm)	Information about alarm summaries.	Cisco Prime Collaboration Assurance Advanced
Performance (Network Health Overview > Performance)	Provides details on critical performance metrics of each managed element.	Cisco Prime Collaboration Assurance Advanced
Contact Center Topology(Network Health Overview > Contact Center Topology)	Information about Unified Contact Center Topology View.	Cisco Prime Collaboration Contact Center Assurance

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can view the following dashboard from the Cisco Prime Collaboration Assurance home page:

Dashboard	Description
Customer Summary (Monitor> System View> Customer Summary)	Information about alarm, endpoints, and inventory aggregated per customer.
TelePresence Exchange (Monitor> System View> Telepresence Exchange)	Information about cluster node, call and session control devices, region summary, and conferencing devices. Note If CTX devices not managed, no data is populated in any of the dashlets.

For Cisco Prime Collaboration Release 11.5 and later

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can view the following dashboard from the Cisco Prime Collaboration Assurance home page:

Dashboard	Description
Customer Summary(Network Health Overview > Customer Summary)	Information about alarm, endpoints, and inventory aggregated per customer.
TelePresence Exchange(Network Health Overview > TelePresence Exchange)	Information about cluster node, call and Conference control devices, region summary, and conferencing devices.

You can view detailed information on endpoints, infrastructure devices, and a logical top-level view of the network of a particular customer through the Customer Summary dashboard. This launches the other dashboards for individual customers mentioned in the preceding table.



Note

- The Enterprise dashboards (Service Experience, Alarm, Contact Center Topology, and Utilization Monitor, depending on the licenses you have) in Cisco Prime Collaboration Assurance do not filter content by default through the global customer selection field.
- **For Cisco Prime Collaboration Release 11.5 and later**
The Enterprise dashboards (Call Quality, Alarm, Contact Center Topology depending on the licenses you have) in Cisco Prime Collaboration Assurance do not filter content by default through the global customer selection field.
- If you select another customer through global selection the user interface will refresh and the home page showing the Customer Summary dashboard is displayed.
- To change the customer you need to click the customer name from the Customer Summary dashboard.

You can view data either as a chart or in a tabular format. By default, reports are displayed as charts that are interactive; that is, you can click on the data to launch the associated page. When you view a report in the tabular format, you can export data in the CSV format.

In the dashboard, you can view data for:

- A day - Data collected from 00:00:00 hours to current time.
- A week - Data collected during the last seven days including today, starting from 00:00:00 hours.
- Four week - Data collected during the last 28 days including today, starting from 00:00:00 hours.

**Note**

On all the pages, the time displayed is the Cisco Prime Collaboration Assurance server time.

Ops View

The Ops View or Cluster View in the Home page (**Monitor > System View > OpsView**) provides high-level information about the Cisco Unified CM and VCS clusters that are available in the system. Based on your mode of deployment, you can view the details of all the clusters in your system or clusters for a specific customer. The Ops View displays the unregistered count of the hard and soft endpoints as separate entity.

For Cisco Prime Collaboration Release 11.5 and later

The Ops View or Cluster View is in the Home page (**Network Health Overview > OpsView**).

For Cisco Prime Collaboration Release 11.6 and later

The OpsView tab also displays the details of SIP trunks that are connected to Unified Communications Manager cluster.

Prerequisites:

- The cluster must be discovered in Cisco Prime Collaboration Assurance for the cluster data to be displayed in the Ops View.
- A user must be associated to a domain or customer that has one or more Cisco Unified CM or VCS clusters in the system. However, this is not applicable for globaladmin users as they have access to all the domains.
- Add the Cisco Prime Assurance Server as a syslog receiver in the CUCM. This ensures that the Ops View is dynamically updated to reflect the trunk status changes in a cluster.

**Note**

In case the Ops View is blank, refer to the note in the section *Getting Started with Prime Collaboration Assurance* in the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#).

You can view the details of the cluster either in Treemap view or List view.

You can use the treemap view to...	You can use the list view to ...
<p>View high-level summary of the faults and also the split up of Critical, Major, Minor, and Warning alarms. By clicking on the Total alarms count link, you can cross launch to the Alarms browser, in the Alarms & Events page.</p> <p>Note The Total alarm count displayed in the Ops View not only includes the alarms raised on the cluster nodes, but also the alarms raised on the individual devices (provided it is associated with the Cisco Unified CM or VCS cluster).</p>	<p>View high-level summary of the faults and also the split up of Critical, Major, Minor, and Warning alarms. By clicking on the Total alarms count, you can cross-launch to the Alarms browser, in the Alarms & Events page.</p>
<p>View the registration information (number of endpoints that are registered, unregistered-hard endpoints or soft clients, registered with backup, and unknown) of all the different types of devices in the cluster—phones, media resources (hardware and software), MGCP gateways (including each port), CTI Route Points, CTI ports, and Voice Mail Ports.</p> <p>Click the registration status counts for Endpoints to cross launch to the Endpoint Diagnostics page and the registration status counts for the other device types to cross launch to the Connected Devices tab with all the devices for that device type filtered.</p>	<p>View the number of Registered, Unregistered-hard endpoints or soft clients, Registered with Backup, and Unknown phone counts for each device type. Click the phone counts for Endpoints to launch the Endpoints Diagnostics page and the phone counts for all the other device types (Media Resources, Voice Mail Ports, and MGCP Gateways) to launch the Connected Devices tab with all the devices for that device type filtered.</p> <p>The CTI Ports and CTI Route Points device types are displayed by default.</p>
Launch the Summary View for that cluster, by clicking on the cluster name.	Launch the Summary View for that cluster, by clicking on the cluster name.

**Note**

- The data displayed in the Treemap view depends on the components that are available in the system. However, the information about Alarms is displayed for all the clusters.
- When you click a VCS cluster in the treemap view or list view, only the Topology page is launched. The Summary, Endpoint by Device Pool, Connected Devices, Route Pattern Summary, and Device Search tabs are applicable only for Cisco Unified CM clusters.
- For deployment of more than ten clusters, the treemap view displays title links for each cluster.

In the treemap view, you can also view the above mentioned details in a quick view, by clicking on the Alarms component for alarm details and device type components for the registration status information.

The treemap view auto refreshes every two minutes. To disable the auto refresh functionality, uncheck the **Auto Refresh** check box at the top right corner of the treemap view.

Color Codes in the Treemap View:

In the treemap view, the device types and alarms in a cluster are classified based on the following severity categories:

For severity...	The color displayed is ...	If there are...
Critical	Red	<ul style="list-style-type: none"> • One or more critical alarms in the cluster. <p>Or</p> <ul style="list-style-type: none"> • More than or equal to 10% Unregistered hard endpoints. <p>Or</p> <ul style="list-style-type: none"> • For Cisco Prime Collaboration Release 11.6 and later <p>At least one Unified Communications Manager SIP trunk in “No Service” state.</p> <p>Note When the Red color is displayed, Ops View displays the hard and soft Unregistered endpoint count separately.</p>
Major	Orange	<ul style="list-style-type: none"> • One or more major alarms in the cluster. <p>Or</p> <ul style="list-style-type: none"> • Less than 10% Unregistered hard endpoints. <p>Or</p> <ul style="list-style-type: none"> • For Cisco Prime Collaboration Release 11.6 and later <p>At least one Unified Communications Manager SIP trunk in “Partial Service” state, and no Unified Communications Manager SIP trunk in “No Service” state.</p> <p>Note When the Orange color is displayed, Ops View displays the hard and soft Unregistered endpoint count separately.</p>

For severity...	The color displayed is ...	If there are...
Minor/Warning	Yellow	<ul style="list-style-type: none"> • One or more minor/warning alarms in the cluster. Or • Any device in the Registered with BackUp state. Or • For Cisco Prime Collaboration Release 11.6 and later <p>At least one Unified Communications Manager SIP trunk in “UNKNOWN-Options Ping Enabled” state, and no Unified Communications Manager SIP trunk in “No Service” and “Partial Service” state.</p>
Normal	Green	<ul style="list-style-type: none"> • No critical, major, or minor alarms. Or • All devices are in the registered or unknown state. Or • For Cisco Prime Collaboration Release 11.6 and later <p>All the Unified Communications Manager SIP trunk in “Full Service” state.</p> <p>Or</p> <ul style="list-style-type: none"> • No Unified Communications Manager SIP trunk defined for a cluster.



Note For Cisco Prime Collaboration Release 11.6 and later

For the SIP Trunks that are associated with Unified Communications Manager cluster, the list view displays the column names for the following states:

- No Service
 - Partial Service
 - UNKNOWN-Options Ping Enabled
 - Full Service
-

Troubleshooting

1. **Issue:** The Ops View does not display the clusters

Recommended Action: Check that the following conditions are met:

- Ensure the cluster has been discovered and Cisco Unified CM is in managed state in Inventory Management
- Ensure the CDT discovery is completed for the clusters, and are displayed in Inventory Management
- The Endpoint Diagnostics displays all the endpoints

2. **Issue:** The Registration status does not display the correct count

Recommended Action: Check that the following conditions are met:

- Ensure the CDT discovery had updated the count information
- You must re-trigger the CDT discovery if the CDT discovery is not completed successfully
- Ensure Cisco Unified CM is enabled to send syslogs to Cisco Prime Collaboration Assurance.

3. **Issue:** The leaf color of the UCM SIP Trunk does not change as expected.

Recommended Action: Check that the following conditions are met:

- Check if the Prime Collaboration Assurance is added as a syslog receiver in the CUCM since the trunk status change comes as a syslog update to Cisco Prime Collaboration Assurance.
- Another workaround is to rediscover the CUCM.

4. **Issue:** Sometimes the globaladmin user is unable to view the **OpsView Dashlets** page.

Recommended Action: Run the following script:

A new script **opsview_globaladmin.sh** is created.

Recommended path: Save the script at the following path: **/opt/emms/emsam/bin**

Summary

The Summary tab provides the system utilization status for each Unified CM node in the cluster.

It includes the following dashlets:

- [Summary](#)
- [Call Processor Health Summary](#)
- [Alarm Summary](#)
- [Registration Summary](#)
- [License Summary](#)

Summary

Provides high-level cluster information along with inter-cluster details such as the number of H323 & MGCP Gateways Configured, SIP Trunks Configured, and the Device Pools.

You can also view the cluster version, database replication status, and number of Unified CM nodes in the cluster. Click **Cluster Call Activity** to view the last 24 hours call activity graph for all the Unified CM nodes in the cluster.

Call Processor Health Summary

Provides information on CPU usage, Virtual Memory usage, Disk usage, and the number of calls attempted or completed (in the current hour and peak hour). Click **Call Activity** to view the last 24 hours call activity graph for the selected Unified CM node. Click the CPU Usage, VM Usage, or Disk Usage value to launch the Performance tab with the System Summary dashboard for that cluster type selected.

You can also view long term call activity trend for the Cisco Unified CM cluster—select one or more cluster nodes and choose **Call Activity** from the **Trend** drop-down list.



Note For those fields that are not applicable for IM & Presence, it is displayed as N/A.

Alarm Summary

Provides a high-level summary of the faults on all clusters managed by Cisco Prime Collaboration Assurance. You can click the alarm data in the Total column to cross-launch to the Alarms browser, in the Alarms & Events page.

Registration Summary

Provides information about the registration status of the phones, media resources (hardware and software), MGCP gateways (including each port), CTI Route Points, CTI Ports, and Voice Mail Ports in the cluster.

The following information is displayed for the endpoints:

- Number of endpoints that are registered
- Number of endpoints that are registered with backup
- Number of endpoints that are unregistered
- Number of endpoints that are unknown or rejected

You can click the endpoints data for each of the above mentioned registration status to launch the Connected Devices tab for that device type.

License Summary

Provides licensing information for the Cisco Unified CM cluster. For versions 9.0 and above, click the **Click here for CUWL License Details** link to launch the login page for Cisco Prime License Manager.

For versions below 9.0, it retrieves and displays the licensing information—Licence Type, Units Authorized, Units Used, and Units Remaining.

Endpoint by Device Pool

The Endpoint by Device Pool tab provides the summary of phones in the cluster at the device pool level.

It displays the following information:

- Total number of endpoints configured to this device pool
- Number of endpoints that are registered
- Number of endpoints that are registered with backup
- Number of endpoints that are unregistered
- Number of endpoints that are in unknown or rejected states
- Service Quality Endpoints and Events.

You can click the endpoints data for any of the above-mentioned registration status to cross launch to the **Endpoint Diagnostics** page.

Click the endpoints data in the **SQ Issues** column to launch the **Impacted Phones Report** page. This page lists all the phones in the device pool that are impacted by voice quality issues.

The events count link in the **SQ Issues** column launches the **SQ Alert Report** page. This page lists the details of the events raised for that particular device pool in the cluster.



Note

- A flag is displayed against the device pool name whenever the Phones Unregistered Threshold Exceeded or Service Quality Threshold Exceeded alarm for that device pool is raised.
- The count of Endpoints and Events in the **SQ Issues** column is shown only for the last 4 hours.

Topology—Cisco Unified Communications Manager or Cisco TelePresence Video Communication Server Cluster

The cluster topology displays a logical top-level view of the following clusters:

- Cisco Unified Communications Manager (Unified CM)
- Cisco TelePresence Video Communication Server (VCS)

You can use the Cluster Topology View to:

- View devices registered to the Unified CM or VCS, the states in which the devices are, and the registration status of the devices in the cluster.
- View alarms and act on alarms on individual devices and the cluster level.
- View database replication status.
- Search for devices in a cluster.

Prerequisites

- All devices should be in managed state in Cisco Prime Collaboration Assurance.
- The Unified CM publisher should be in Managed state.
- For VCS cluster to be shown in Ops View (now called Network Health Overview), the cluster name (FQDN of VCS) has to be configured on VCS.



Note

- Only the public IP address and DNS name is displayed in the topology.

Access the Unified CM or VCS Cluster Topology

To access the Cisco Unified CM Topology View, choose **Monitor > System View > OpsView**. Click on a Unified CM cluster name, and then go to the **Topology** tab.

To access the Cisco VCS Topology View, choose **Monitor > System View > OpsView**. Click on a VCS cluster.

For Cisco Prime Collaboration Release 11.5 and later

To access the Cisco Unified CM Topology View, choose **Network Health Overview > OpsView**. Click on a Unified CM cluster name, and then go to the **Topology** tab.

To access the Cisco VCS Topology View, choose **Network Health Overview > OpsView**. Click on a VCS cluster.

You can also view the Topology tab from Device 360 View of Unified CM or VCS. Click the Cluster ID value in the Device 360 View. This launches the Cluster View page for that cluster. Now click **Topology** to launch the Topology View.

Cluster Topology—Components

For a Unified CM or VCS cluster, the following components or details (if applicable) appear:

Unified CM Cluster	VCS Cluster
Cluster Name	Cluster Name
Unified CM	VCS
Endpoints	Endpoints
Unknown Devices	Cisco TelePresence Management Suite (TMS)
Application Servers	Cisco TelePresence Conductor

Unified CM Cluster	VCS Cluster
Gateways (H323, MGCP, and SIP)	Cisco TelePresence Server
	Cisco Multipoint Control Unit
Cisco TelePresence Manager	-
Cisco IM and Presence	-
Cisco TelePresence Conductor	-
Cisco TelePresence Server	-
Cisco Multipoint Control Unit	-
Cisco Unity Connection	-
Cisco Unified Border Element	-
Cisco TelePresence Multipoint Switch	-
Cisco Unified MeetingPlace	-
Cisco Unified MeetingPlace Express	-
Cisco MediaSense	-
Cisco Unified Customer Voice Portal	-
Cisco Emergency Responder	-
Cisco Unity Express	-
Cisco Unified Contact Center Express	-
Cisco Unified Contact Center Enterprise	-

For Cisco Prime Collaboration Release 11.5 and later



Note

For a Unified CM or VCS cluster, Cisco TelePresence Manager, Cisco TelePresence Multipoint Switch, and Cisco Unified MeetingPlace Express does not appear.

When you hover an Inter Cluster Trunk (ICT), the tool tip displays the following information:

- Source
- Gatekeeper IP
- Target
- Protocol
- Trunk Name

Click on the ICT icon to launch the Topology view for the ICT cluster. If you are using Internet Explorer version 11, when you click on the ICT icon, it will take a few moments to launch the Unified CM topology as the browser gets refreshed.



Note If you do not have privileges for domains or customers to view the cluster, the ICT Cluster Topology view does not appear.

The link status of the links between the following are shown:

- Unified CM cluster—Unified CM, and MGCP, Voice Mail ports (Cisco Unity Connection with SCCP), Media Devices, CTI Ports, and CTI Route points
- VCS cluster—VCS, and MCU, and Cisco TelePresence Server

On hovering over the link, a tool tip appears to show the status of the link.

When a link between devices and Unified CM is down, you can click the link, to launch the Registered Devices tab. The list of devices is automatically filtered to show the devices with Registration Status as Unregistered. To view the registration status of other devices, filter on the Registration Status field.

If a Warning or Critical icon appears on the link, it denotes:

- Warning icon - Either Registration, or Link status is down.
- Critical icon - Registration and Link status, both are down.

View Information in the Cluster

You can view the following information from the cluster.

Viewing Options

You can choose to view:

- The IP Address or DNS of the devices or hide both the labels by selecting from the drop-down list available. By default, DNS is displayed. Hide label does not hide the labels for Inter Cluster Trunks and unmanaged endpoints.
- All devices or devices with alarms only (select Show Devices with Alarms check box). This is applicable only for devices in the cloud, and not the Unified CM or VCS node, Inter Cluster Trunks (ICTs), or Unmanaged Devices group.
- Cluster map in Distributed, Hierarchic or Circular layout by selecting from the drop-down list available. By default, the page displays Circular layout.

The preceding viewing options are preserved when you launch the cluster view from an earlier used browser.

If any group has more than 50 devices, by default it appears in a collapsed form. You have to expand to view the devices.

The page is refreshed every two minutes by default.

Endpoints in the Cluster

All endpoints part of the cluster are shown as a single group with an icon. Point to the group icon, to view the following details in the tool tip:

- Total Endpoints
- Registered Endpoints
- Unregistered Endpoints (Hard and Soft)
- Unknown Endpoints

You can click on the quick view icon of the endpoint group, and then click on the counts to launch the Endpoint Diagnostics page, which displays information filtered on the selected endpoints.

List of Unmanaged Devices in the Cluster

You can view the list of unmanaged devices in the cluster by clicking on the Unmanaged group icon. The Unmanaged Devices pop up window appears. The Unmanaged Devices table shows the Device IP Address/Host name, Type (device type), and Linked to information. You can search for a device using the Quick Filter or Advanced Filter

You can add or discover a device from the Unmanaged Devices page. Click the Add Device button to discover the devices from the Inventory Management.

Device Details

If you point your cursor on any device, you can view the IP Address, Host name, Status, and Capability of that device. Click on the device icon to launch its Device 360 degree view.

Database Replication Status for Cisco Unified Communications Manager Clusters

A green tick icon shows that Database replication successful between Cisco Unified Communications Managers in the cluster. A red cross shows that Database replication error between Cisco Unified Communications Managers in the cluster. This feature is applicable for Unified CM cluster only.

Alarm Details

Alarm icons appear next to the device when an alarm is raised on the device or the cluster. When an alarm is raised, it remains in the Topology View until it is cleared or manually cleared.

To view the alarms of a device, click on the device, The Device 360 degree view pop up window of the device appears, listing the alarms under the Alarm tab in the bottom pane of the window.

To view the cluster-level alarms, click on the alarm icon in the cluster cloud. The Cluster Alarm pop up window is displayed. Now click **Alarm Details** to cross launch to the Alarms & Events page. The Alarms are filtered according to the cluster.

You can also go to the Summary tab (Choose OpsView, and click on the cluster). In the Alarm Summary dashlet, click on the value of the **Total** column of the cluster. The Alarms & Events page is displayed. The Alarms are filtered according to the cluster.

Cluster level alarms are available for Unified CM clusters only.



Note Information alarm is not displayed.

Device icons are grayed out in the following conditions:

- When the device is in Unreachable state in Inventory Management.
 - When the *deviceunreachable* alarm is raised on the device.
-

Search for Devices

You can search for devices by host name, and IP address using the search box in the Topology View pane. The device which matches the search query is highlighted with a box and moved to the center. If the search query matches two or more devices, all these devices are highlighted with a box.

When the searched device is part of a group that has more than 50 devices then:

- If the group is not been expanded before, then the entire group is highlighted. You have to expand the group to see the device, which is highlighted after expansion of group.
- If the group is expanded before, then the group expands by default, and the device is highlighted.



Note Search for phones is not supported.

Connected Devices

The Connected Devices tab helps you perform a device search based on the Device Type, Registration Status, and IP filter.

Performance

The **Performance** tab displays pre-defined dashboards based on the Unified CM publisher node you select in the Ops View. You cannot select any other cluster node from the **Cluster or Device** drop-down list. It also allows you to create custom performance dashboards.

For custom dashboards that you create, you can enable historical trending. See section [Create Custom Performance Dashboards](#).

Route Pattern Summary

The Route Pattern Summary displays information regarding utilization and call volume for each route group. It also displays the route lists or gateways configured in the cluster.



Note Click the route group name link to launch the **Report** pop-up window. This window displays the utilization, call volume, and channel usage for the selected route group.

You can view the following information:

- Route List or Gateway

- Route Pattern associated with the Route Group

Device Search

The Device Search tab helps you perform a search for devices in the selected Unified CM cluster. For more details, see section [Unified CM Device Search, on page 185](#).

Endpoint Registration Summary

Provides a summary of the status of all the endpoints in the network. You can view a summary for hard endpoints (such as E20, Phones), soft clients (Cisco Unified Personal Communicator, Cisco IP Communicator, iPhone, Android, Cisco Jabber, and Client Services Framework [CSF]), and Jabber endpoints separately also.

Prerequisites

- All devices should be in managed state in Cisco Prime Collaboration Assurance.
- The cluster should be discovered in Cisco Prime Collaboration Assurance.

For Cisco Prime Collaboration Release 11.5 and later

Prerequisite

- The cluster should be discovered in Cisco Prime Collaboration Assurance.

The dashboard displays the summary as a pie chart or table. It provides information about the endpoints in the following modes:

- Unregistered—Endpoints that are not registered with Cisco Unified Communications Manager and VCS. Displayed in red. The count displayed for “Unregistered from UCM” includes the devices that are in Energy Save mode.
- Registered—Endpoints that are registered with Cisco Unified CM and Cisco VCS. Displayed in green. The count displayed for “Registered Hard Phones” includes the Cisco TelePresence endpoints.
- Unknown—Endpoints that are in Unknown state (registration status of the endpoints is unknown). Displayed in grey.

For Cisco Prime Collaboration Release 11.1 and earlier

Click the pie chart to view the Endpoint Health Troubleshooting window, which has the links to the following pages:

- Endpoint Diagnostics
- Phone Report
- UCM Troubleshoot
- VCS Troubleshoot

The phone counts shown in the UC Topology View, Diagnostics Summary View, and Endpoint Registration Summary dashlet will be in synchronized, with a maximum of 10 minutes delay. You can schedule cluster discovery to trigger this synchronization manually, if required. Cluster discovery will also resynchronize the registration status for all phones. If cluster discovery is not scheduled manually, synchronization takes place as part of nightly cluster discovery.

Availability Summary

Provides the most recent data about the devices listed under the Unified Communications device group.

The Availability Summary dashlet tracks a subset of supported critical events for each device type in Cisco Prime Collaboration Assurance and displays the device as **Down**. To view the list of events, see the [Service Availability Summary Events](#). For event description and device type, see the [Supported Alarms and Events for Cisco Prime Collaboration Assurance](#).

The X axis displays the number of applications. The Y axis displays the application type.

Green indicates applications that are active. Red indicates applications that are down.

Click the bar to open a popup that provides links to Cluster View and Alarms browser.

**Note**

This dashlet does not display any data when there are no devices added in Cisco Prime Collaboration Assurance.

Service Experience/Call Quality

The Service Experience dashboard helps you identify the most impacted TelePresence endpoints with call quality alarms, poor call quality locations, sessions with alarms, and call failure locations.

It contains the following dashlets:

- [Top 5 Poor Voice Call Quality Locations](#)
- [Top 5 Call Failure Locations](#)
- [Top 10 TelePresence Endpoints with Call Quality Alarms](#)
- [Conference with Alarms](#)

**Note**

The Call Quality dashlets display incorrect information if the location of the device is different from the location of the device pool that is assigned to the device. Ensure that you configure the same location at the device and the device pool level. The Location field displays the location that is configured on a device pool instead of the location that is configured on the device, when you set the device location to one of the system locations (Hub_None, Phantom, or Shadow).

For Cisco Prime Collaboration Release 11.5 and later

The Service Experience dashboard is renamed as Call Quality.

Top 5 Poor Voice Call Quality Locations

Provides information about the top five locations that experienced the poorest call quality in the last hour. You can view the call data older than the last hour from the CDR & CMR reports under Assurance Reports.

For Cisco Prime Collaboration Release 11.5 and later

Provides information about the top five locations that experienced the poorest call quality in the last hour. You can view the call data older than the last hour from the CDR & CMR reports under Reports.

The X axis shows the location. The Y axis shows the number of poor calls. The Z axis shows the percentage of poor calls, represented as bubbles. If the percentage of failed calls in a location is less than 0.5, the location is ignored.

If you have deployed Cisco Prime Collaboration Assurance in the Enterprise Mode, the Top 5 Poor Voice Call Quality Locations report contains data associated with a specific domain that you have selected in the global selection drop-down list (top-right of the home page).

If you have deployed Cisco Prime Collaboration Assurance in MSP Mode, the Top 5 Poor Voice Call Quality Locations report contains customer name, data that is associated with a specific customer (that is selected from Home > Customer Summary).

**Note**

Cisco TelePresence call details are not included in this dashlet.

Click the bubble in the Z axis to view the following details:

- Cluster
- Poor calls
- Total calls

For Cisco Prime Collaboration Release 11.1 and earlier

Click **Troubleshoot** to open the Call Quality Troubleshooting page. The Call Quality Trend pane shows the poor calls for the last 24 hours, per location. The Impacted Devices pane shows the devices that were involved in the call for that particular hour. Click any bar in the Impacted Devices pane to open the Call Details pane.

**Note**

To view the call details, phone access switch must be monitored or discovered from the phone using CDP neighbor discovery.

Top 5 Call Failure Locations

Displays the top five locations that experienced the most call failures in the last hour. Cisco Prime Collaboration Assurance aggregates the available CDR data at fixed time intervals and displays it in this dashlet.

The top five locations are chosen taking into account all the Cisco Unified Communications Manager clusters that are added in Cisco Prime Collaboration Assurance. For example, if three Cisco Unified Communications Manager clusters are added in Cisco Prime Collaboration Assurance, and each cluster has 30 locations, then the top five locations are chosen from among these 90 locations.

If there are fewer than five locations that are experiencing call failures, only those locations are shown. If the percentage of failed calls in a location is less than 0.5, the location is ignored.

If you have deployed Cisco Prime Collaboration Assurance in the Enterprise Mode, Top 5 Call Failure Locations report contains data associated with a specific domain that you have selected in the global selection drop-down (top-right of the home page).

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the Top 5 Call Failure Locations report contains customer name, data that is associated with a specific customer (that is selected from Home > Customer Summary).

You can click the bubble in the Z axis to view the following details:

- Cluster
- Failed Calls
- Total Calls

For Cisco Prime Collaboration Release 11.1 and earlier

Click **Troubleshoot** to open the Call Failure Troubleshooting page.

Top 10 TelePresence Endpoints with Call Quality Alarms

Displays the top 10 endpoints with call quality alarms (for packet loss, jitter, and latency).

You can click on the alarm data to launch the Alarms page.

Conference with Alarms

Displays the number of in-progress conferences with alarms.

You can launch the **360 Conference View** from this dashlet.

Alarm Dashboard

The Alarm dashboard helps you identify the most impacted TelePresence endpoints with alarms, devices with alarms, and infrastructure alarm summary.

For Cisco Prime Collaboration Release 11.5 and later

The Alarm dashboard helps you identify the most impacted TelePresence endpoints with alarms, devices with alarms, and device alarm summary.

It contains the following dashlets:

Top 10 TelePresence Endpoints with Alarms

Displays the top 10 TelePresence endpoints with alarms. You can click on the bar chart to open a quick view that has the summary of all the alarm severity count. The alarm count includes alarm with the severity Cleared.

By clicking on the Total alarms count, you can cross-launch to the Alarm browser to view the alarm details. You can view the graph for endpoints and service infrastructure devices.

Top 10 Devices with Alarms

Displays the top 10 devices with alarms. You can click on the bar chart to open a quick view that has the summary of all the alarm severity count. The alarm count includes alarms with the severity Cleared.

By clicking on the Total alarms count, you can cross-launch to the Alarm browser to view the alarm details. You can view the graph for endpoints and service infrastructure devices.

You can launch the Inventory Management and click either on the Endpoint or Service Infrastructure links to view the device details.



Note Clusters are not treated as devices and are not shown in this dashlet.

Infrastructure Alarm Summary/Device Alarm Summary

Displays the number of infrastructure devices with and without alarms. In addition, you can also view the number of devices, based on the alarm severity.

You can click on the total device data to launch the Inventory page. You can also click on the devices with alarms data to launch the Alarms and Events page.

By default, the information is displayed in a pie chart. The pie chart is updated when the user interface is refreshed. You can change this display to a table.

For Cisco Prime Collaboration Release 11.5 and later



Note Infrastructure Alarm Summary dashlet is renamed as Device Alarm Summary.

Utilization Monitor

The Utilization Monitor (**Monitor > Utilization Monitor**) page provides information about the trunks utilization, trunk/route groups utilization, location CAC bandwidth utilization, conferencing devices, and conductor bridge pool utilization.



Note Cisco Prime Collaboration Assurance supports SNMPv2c and SNMPv3 for managing the gateway. However, performance polling (GSU) with SNMPv3 is not supported in Cisco Prime Collaboration Assurance.

Trunk Utilization

For Cisco Prime Collaboration Release 11.1 and earlier

Provides information about the most utilized trunks in terms of channel usage.

You can view the utilization, associated gateway IP and name, and associated route group details.

Cisco Prime Collaboration Assurance allows you to configure maximum capacity for SIP trunks. Click the SIP Trunks Capacity Settings link, under SIP Trunk Max Capacity tab, select the Gateway that is a Border Element and select the IP of the Border Element. Specify the maximum number of calls that can go through the SIP Trunk.



Note You must have admin privileges to access the SIP Trunks Capacity Settings link.

Click the percentage link in the Utilization column to display a graph that plots trunk utilization against time. The data for the last polling cycle is displayed.

You can view popups that display the usage as a percentage when you place the cursor on the X axis coordinates for each four-minute interval. To open a detailed performance graph showing trunk or route usage, click the points on the graph or the channel utilization bar that correspond to the X axis coordinates.



Note HSRP-enabled devices are not supported in Cisco Prime Collaboration Assurance.

The following table provides an overview of the utilization report for various types of SIP trunks in Cisco Prime Collaboration Assurance.

Table 63: Utilization Report for SIP Trunk Types

SIP Trunk Type	Utilization Report	
	Data Source	Support
Intercluster Trunks	CDR	Available. These trunks do not display the data if the intercluster trunk is a Unified Communications Manager, and if you need to display the data correctly, these trunks should associate with a Voice Gateway.
SIP trunk connected to Cisco Unified Border Element (CUBE)	Polling the CUBE directly	Available
UCM SIP trunk (These trunks are not provided by service provider but are created by Enterprise administrator. For example, ICT, Trunk to WebEx, etc).	RTMT UCM SIP Performance Counter	NA. Only RTMT performance dashboard to check Call Volume at a given time.
SIP trunk not connected to CUBE (for example, ACME).	RTMT UCM SIP Performance Counter	NA. Only RTMT performance dashboard to check Call Volume at a given time.



Note You cannot monitor T1/E1 Channel Associated Signaling (CAS) trunk utilization on Cisco Integrated Services Routers (ISR) and Cisco ISR G2, as these platforms do not provide the required SNMP instrumentation.

For Cisco Prime Collaboration Release 11.5 and earlier



Note Cisco Prime Collaboration Assurance supports utilization only for the SIP Trunks that are connected to Cisco Unified Border Element (CUBE). Cisco Prime Collaboration Assurance does not support utilization for SIP trunks that are configured in Unified Communications Manager.

T1/E1 Trunks

For Cisco Prime Collaboration Release 11.5 and later

Provides information about the most utilized T1/E1 trunks in terms of channel usage.

You can view the utilization, associated gateway IP and name, and associated route group details.

Click the percentage link in the Utilization column to display a graph that plots trunk utilization against time. The data for the last polling cycle is displayed.

You can view popups that display the usage as a percentage when you place the cursor on the X axis coordinates for each four-minute interval. To open a detailed performance graph showing trunk or route usage, click the points on the graph or the channel utilization bar that correspond to the X axis coordinates.



Note HSRP-enabled devices are not supported in Cisco Prime Collaboration Assurance.



Note You cannot monitor T1/E1 Channel Associated Signaling (CAS) trunk utilization on Cisco Integrated Services Routers (ISR) and Cisco ISR G2, as these platforms do not provide the required SNMP instrumentation.

The following VG ISR4K Cube device versions does not support ISDN mib which will impact the T1/E1 trunk utilization (in Utilization Monitor API):

- 16.8.x
 - 16.7.x
 - 16.6.x
-

CUBE SIP Trunk

For Cisco Prime Collaboration Release 11.5 and later

Provides information about the most utilized SIP trunks in terms of channel usage.

You can view the SIP trunk utilization, the default value of the maximum concurrent calls, the value of maximum concurrent calls that is configured on Cisco Unified Border Element (CUBE), and associated CUBE IP details.



Note The 'Max Concurrent Calls (Configured on CUBE)' column contains the maximum calls that you configure at the dial-peer level in CUBE.

Cisco Prime Collaboration Assurance allows you to configure maximum concurrent calls for CUBE-connected SIP trunks. In the SIP Trunk page, check the check box corresponding to the SIP trunk that you want to configure. Click the **Set Max Concurrent Call** button to specify the maximum number of concurrent calls that can go through the SIP Trunk in Cisco Prime Collaboration Assurance.

Click the percentage link in the Utilization column to display a graph that plots SIP trunk utilization against time. The data for the last polling cycle is displayed.

You can view popups that display the usage as a percentage when you place the cursor on the X axis coordinates for each four-minute interval. To open a detailed performance graph showing trunk or route usage, click the points on the graph or the channel utilization bar that correspond to the X axis coordinates.

For Cisco Prime Collaboration Release 12.1 and later

You will be able to view the CUBE SIP Trunks with session server group configuration on the **Utilization Monitor** page **Monitor > Utilization Monitor > CUBE SIP Trunk** tab in Cisco Prime Collaboration Assurance User Interface.

In the **CUBE SIP Trunk** page, check the check box corresponding to the server group configuration to enable the Raise/Suppress buttons. By default, the alarms will be in **Raise** state. The state is updated only when you change it.

The **Alarm Status** column indicates whether the alarm can be raised or not.

The following table provides an overview of the utilization report for various types of SIP trunks in Cisco Prime Collaboration Assurance.

Table 64: Utilization Report for SIP Trunk Types

SIP Trunk Type	Utilization Report	
	Data Source	Support
Intercluster Trunks	CDR	Available. These trunks do not display the data if the intercluster trunk is a Unified Communications Manager, and if you need to display the data correctly, these trunks should associate with a Voice Gateway.
SIP trunk connected to Cisco Unified Border Element (CUBE)	Polling the CUBE directly	Available
UCM SIP trunk (These trunks are not provided by service provider but are created by Enterprise administrator. For example, ICT, Trunk to WebEx, etc).	RTMT UCM SIP Performance Counter	NA. Only RTMT performance dashboard to check Call Volume at a given time.
SIP trunk not connected to CUBE (for example, ACME).	RTMT UCM SIP Performance Counter	NA. Only RTMT performance dashboard to check Call Volume at a given time.



Note

Cisco Prime Collaboration Assurance supports utilization only for the SIP trunks that are connected to Cisco Unified Border Element (CUBE). Cisco Prime Collaboration Assurance supports utilization for SIP trunks that are configured in Unified Communications Manager in the UCM SIP Trunk page.

For Cisco Prime Collaboration Release 11.6 and later

Cisco Prime Collaboration Assurance supports utilization for both CUBE-connected SIP trunks as well as SIP trunks that are configured in Unified Communications Manager.

Modify the Default Value of SIP Trunk Maximum Concurrent Calls

As a super administrator, system administrator or network operator, you can configure the default value of maximum concurrent calls for CUBE-connected SIP trunks.

Prerequisite - Root access feature is mandatory to perform this task, hence you should raise a TAC case to obtain root access.

To configure the default value of the maximum concurrent calls for SIP Trunks:

1. Log in as a root user.
2. Navigate to the `/opt/emms/cuom/gpf` folder and edit the `gpf.properties` file.
3. Find the line **SipTrunkMaxCapacity=100** and change the value from '100' to your desired numeric value.
4. To restart Cisco Prime Collaboration Assurance server, login as *root* and execute the following commands:

a. Stop the processes:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh stop
```

b. Check the status of the processes - Verify whether the processes have stopped:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh status
```

c. Restart the processes:

```
root@<hostname>~# /opt/emms/emsam/bin/cpcmcontrol.sh start
```

UCM SIP Trunks

For Cisco Prime Collaboration Release 11.6 and later

Provides information on all the SIP trunks that are connected to the Unified Communications Manager cluster.

UCM SIP Trunk is added as a tab on the Utilization Monitor page **Monitor > Utilization Monitor > UCM SIP Trunk** in Cisco Prime Collaboration Assurance User Interface.

You can view the SIP trunk utilization (audio and video maximum calls, and total active calls), the default value of the maximum concurrent calls, the SIP trunk status and flag.



Note

The 'Utilization' column contains the utilization details for both audio and video calls.

Status	Description
Single	The SIP trunk is running on one node in the cluster.
Multiple	The SIP trunk is running on multiple nodes in the cluster.
Run On All Nodes	The SIP trunk is running on all nodes in the cluster.



Note For SIP trunks with 'Single or Multiple' status, you can expand the particular SIP trunk from the SIP Trunk Name column to view an additional table that contains information on the remote destinations, and audio and video call status for each of the nodes.

Cisco Prime Collaboration Assurance allows you to configure maximum concurrent calls for audio or video for one or more SIP trunks. In the SIP Trunk page, check the check box corresponding to the SIP trunk that you want to configure. Click the **Max Concurrent Call** button to specify the maximum number of concurrent calls that can go through the SIP trunk in Cisco Prime Collaboration Assurance. The Audio Max Calls and the Video Max Calls columns are populated with the entered value. If you do not configure the audio and video maximum calls value by using the Max Concurrent Call option, a default value from Unified Communications Manager is used to populate the two columns.



Note

- From the OpsView tab, you can also cross-launch to the UCM SIP Trunks page.
- UCM SIP Trunks is not supported in MSP mode.

Route Group Utilization

Provides information about the most utilized route groups in terms of channel usage.

You can also view the utilization and associated cluster details. Click the percentage link in the Utilization column to display a graph that plots route group utilization against time. The data for the last polling cycle is displayed.

You can select a route group to view the Associated Gateways/Trunks table. The table contains information on the trunk, gateway name, and gateway IP. Click Save to add the selected trunk to the route group.



Note Even if trunks are associated to the route group, if polling does not happen then No Data Available error is displayed.



Note The Utilization column displays the “Trunks Not Selected” message if you do not select the trunk for a route group.

You can view popups that display the usage as a percentage when you place the cursor on the X axis coordinates for each four-minute interval. To open a detailed performance graph showing trunk or route usage, click the points on the graph or the channel utilization bar that correspond to the X axis coordinates.

For Cisco Prime Collaboration Release 11.1 and earlier

Cisco Prime Collaboration Assurance allows you to calculate the Route Group aggregation. Click the Route Group Aggregation Settings link, and in the Trunk Utilization Settings page, click the Route Group Aggregation tab. Select the Unified Communication System (UCS) cluster, Route Group, then select the Trunks that belong to the specified Route Group.



Note You must have admin privileges to access the Route Group Aggregation Settings link.

If Cisco Unified Border Element (CUBE) is configured with POTS dial-peers and/or T1/E1 voice interfaces, and you still cannot view any values in the Gateway field under the Trunk Utilization settings, enter the IOS IP address in the file `/opt/emms/emsam/conf/cube_ip.txt` for identifying it as CUBE.

Troubleshooting

Issue: Unable to see the correct route groups.

Recommendation: Ensure that the route groups are associated to a route list in Unified Communication Manager and then rediscover.

Trunk Group Utilization

Provides information about most utilized trunk groups in terms of channel usage.



Note When polling for trunk groups does not happen, the No Data Available error message is displayed.

You can create user-defined trunk groups. Click the Trunk Group Settings link, and in the Trunk Utilization Settings page, click the Custom Trunk Group Management tab. Select the trunks and click the Add New Group button. The New Group dialog box is displayed. Fill in the details and click Save. A message notifies you that the group is created successfully. You can add other devices to an existing user-defined trunk group by clicking the Add to Group button. All user-defined groups are listed in the Custom Trunk Group pane on the left side of the user interface. You can use the search field available under the Custom Trunk Group pane to search for a user-defined trunk group. If these user-defined trunk groups are among the top ten utilized trunk groups, their utilization information appears on the dashlet under Trunk Groups.



Note You must have admin privileges to access the Trunk Group Settings link.

Click the percentage link in the Utilization column to display a graph that plots trunk utilization against time. The data for the last polling cycle is displayed.

You can view popups that display the usage as a percentage when you place the cursor on the X axis coordinates for each four-minute interval. To open a detailed performance graph showing trunk or route usage, click the points on the graph or the channel utilization bar that correspond to the X axis coordinates.

For Cisco Prime Collaboration Release 11.6 and later



Note In both Route Group Utilization and Trunk Group Utilization pages, the Unified Communications Manager SIP trunks are also listed that are used to calculate the utilization for both route groups and trunk groups.

Location CAC Bandwidth Usage

Provides information about the locations at which bandwidth usage is the highest.

You can view the location name, associated cluster, maximum bandwidth, utilization, and number of failed calls details.

Click the Failed Calls icon in the Calls Failed column to launch the Location Out of Resource performance graph.

By default, the table is sorted based on the number of failed calls.

If the maximum bandwidth value is set to Unlimited or None, polling does not occur and the table does not display any data.

Data is polled every 4 minutes.

Location polling in Cisco Prime Collaboration Assurance is performed from a Unified CM node where Location Bandwidth Manager service is enabled. The Location Bandwidth Manager run on any Unified CM subscriber or as a standalone service on a dedicated Unified CM server in the cluster. A minimum of one instance of Location Bandwidth Manager must run in each cluster to enable Enhanced Locations CAC in the cluster.



Note

In Cisco Unified Communications Manager if the **Use Video Bandwidth for Immersive** parameter is set to True, Cisco Prime Collaboration Assurance does not poll the Immersive counters and the table does not display any data for Immersive Bandwidth.

Conferencing Devices

Displays the conferencing devices in your network.

You can see the following details:

- **Status**—Displays whether the device is normal, suspended or contains errors. You can click on the status icon to launch the Alarm browser.

This icon is displayed when there is a critical service infrastructure, unreachable, or inaccessible alarm.

- **Name and IP Address**—You can click on the device name or IP address to launch it in a browser.

Rest your mouse pointer over the Name column and click the quick view icon to view the:

- Media Processing Engine, Call Control Process, Conference Manager, Security Key Exchange.
- Audio Load, Video Load, Media Load, Video ports in use, Battery Status, Temperature Status and Voltage status (for MCU only).
- CPU and memory utilization.
- Device Type
- Video Ports Used
- Audio Ports Used
- Master Conductor

Click the utilization value of Video Ports or Audio Ports Used columns to launch the Detailed Video Port Utilization or Detailed Audio Port Utilization graph. You can choose to view Utilization in percentage or Absolute Utilization, or both (click **All**). You can also use the slider and select a small time interval also (such

as a minute) to view actual data for that interval. You can use this information to increase the number or ports according to the utilization.

Utilization is shown from when the device is in Managed State for the first time in Cisco Prime Collaboration Assurance. For example, the graph enables you to view data for 5 days by default, but data is shown for 4 days as the device is in Managed state for 4 days only.

Conductor Bridge Pool Utilization

Provides information about the cumulative utilization of the conference bridges for each conductor pool in your network.

You can see the following details:

- **Status**—Displays the status of the conductor pool, depending on the status of the conference bridges associated with each conductor pool. You can click on the status icon to cross-launch the Alarm browser to view the individual status of the conference bridges in the conductor pool.
- **Pool name**—You can click on the pool name to cross-launch the device window in a separate browser.
- **Video Ports Used**—Click the utilization value of Video Ports/Screen License Utilization columns to launch the Detailed Video Port Conductor Utilization graph. You can choose to view the Utilization in either percentage or absolute value. You can also use the slider and select a small time interval also (such as a minute) to view actual data for that interval. You can use this information to increase the number or ports according to the utilization. Utilization is shown from when the device is in Managed State for the first time in Cisco Prime Collaboration Assurance. For example, the graph enables you to view data for 7 days by default.



Note

Cisco Prime Collaboration Assurance supports only the Screen License mode for Cisco TelePresence Conductor.

- Conference Bridge Type
- Conductor Name



Note

At least one conference bridge has to be present in the conductor pool to display the utilization monitor.

TelePresence Endpoint

This dashboard helps you to identify the No Show endpoints, most commonly used and least used TelePresence endpoints, and endpoint models.



Note

IP Phones and Software Clients details are not included in the TelePresence Utilization reports.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Telepresence Endpoint

The following are required for Telepresence Endpoint:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the [Configure Devices for Cisco Prime Collaboration Assurance](#).
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 Service Pack 1.

It contains the following dashlets:

Top 10 Utilized TelePresence Endpoints

Displays the top 10 utilized endpoints in your network.

You can view the graph either by duration or conference.

- By duration—The utilization is by usage hours. For example, if the utilization is shown as 0.634 hours, it means the endpoint has been utilized for approximately 38 minutes (0.634×60).
- By conference—The utilization is by number of conference. Here, only *completed* conference are considered. If the number of conference is one, the value of the x-axis is displayed in decimals (0.2, 0.4...). If the number of conference is more than one, the value of the x-axis is displayed in absolute numbers (1, 2, 3...).

You can click on the bar chart to launch the All Conference Summary Report for the selected endpoint.

Top 10 Utilized TelePresence Endpoint Models

Displays the utilization, based on specific endpoint models.

You can view the data:

- For a day—The maximum utilization is ten hours. That is, if the utilization is 120 minutes for a day, the average utilization for a day is 20% ($((120/[10*60])*100)$).
- For a week—The maximum utilization is 50 hours. That is, if the utilization is 1500 minutes for a week, the average utilization for a week is 50% ($((1500/[50*60])*100)$).
- For four weeks—The maximum utilization is 200 hours. That is, if the utilization is 10,800 minutes for a month, the average utilization for a month is 90% ($((10,800/[200*60])*100)$).

You can click on the bar chart to launch the Endpoint Utilization Report for the selected endpoint model.

Top 10 No Show TelePresence Endpoints

Displays the top 10 endpoints that did not participate in the scheduled conference.

You can click on the bar chart to launch the No Show Conference Summary Report for the selected endpoint.

Least 10 Utilized TelePresence Endpoints

Displays the least 10 utilized endpoints in your network.

You can view the graph either by duration or conference.

- By duration—The utilization is by usage hours. For example, if the utilization is shown as 0.634 hours, it means, the endpoint has been utilized for approximately 38 minutes ($0.634 * 60$).

If the utilization is zero, this is not shown in the bar chart. To see this data, you should launch the tabular format.

- By conference—The utilization is by number of conference. Here, only *completed* conference are considered. If the number of conference is one, the value of the x-axis is displayed in decimals (0.2, 0.4...). If the number of conference is more than one, the value of the x-axis is displayed in absolute numbers (1, 2, 3...).

You can click on the bar chart to launch the All Conference Summary Report for the selected endpoint.

Least 10 Utilized TelePresence Endpoint Models

Displays the utilization, based on specific endpoint models. If the utilization is zero, this is not shown in the bar chart. To see this data you should launch the tabular format.

You can view the data:

- For a day—The maximum utilization is ten hours. That is, if the utilization is 120 minutes for a day, the average utilization for a day is 20% ($((120/[10*60])*100)$).
- For a week—The maximum utilization is 50 hours. That is, if the utilization is 1500 minutes for a week, the average utilization for a week is 50% ($((1500/[50*60])*100)$).
- For four weeks—The maximum utilization is 200 hours. That is, if the utilization is 10,800 minutes for a month, the average utilization for a month is 90% ($((10,800/[200*60])*100)$).

You can click on the bar chart to launch the Endpoint Utilization Report for the selected endpoint model.

Number of TelePresence Conference

Displays the number of in-progress and completed conference. Click on the chart to launch the Conference Detail report for a particular conference.

The Conference data is aggregated for every two hours. For example, on a day, assume that you had only two conference. The first conference started at 01:00 hours and ended at 03:00 hours, and the second conference started from 02:20 hours and ended at 05:50 hours.

The data is displayed as:

- 0:00—Zero
- 2:00—1; an in-progress conference from 01:00 to 03:00 is displayed between 0:00 and 02:00 hours.
- 4:00—2; a completed conference from 01:00 to 03:00 and an in-progress conference from 02:20 to 05:50 are displayed between 02:00 and 04:00 hours.
- 6:00—1; a completed conference from 02:20 to 05:50 is displayed between 04:00 and 06:00 hours.

- 8:00—Zero; no conference occurred between 06:00 and 08:00 hours.
- 10:00—Zero
- 12:00—Zero
- ...
- 24:00—Zero; no conference occurred between 22:00 and 24:00 hours.

You can view the data as a chart or in a tabular format. You can also export the data into an Excel spreadsheet.

License Usage

The License Usage tab displays the licensing information for Prime License Manager (licenses usage of all UC applications), VCS (license usage for VCS clusters), CVP (license usage for CVP call servers), and Contact Center Enterprise License Usage (license usage for CCE). It contains the following portlets:

- [Prime License Manager](#)
- [VCS License Usage](#)
- [Customer Voice Portal License Usage, on page 312](#)
- [Contact Center Enterprise License Usage, on page 313](#)

Prime License Manager

The licensing information for voice is categorized under Prime License Manager licenses. This dashlet displays usage of all Unified Communications applications licenses (Cisco Unified CM and Cisco Unity Connection). Whenever the ELM and Unified CM co-reside, you must activate the Enterprise License Management Resource API manually. For a list, see [Setting Up Devices for Cisco Prime Collaboration Assurance](#) and [Configure Devices for Cisco Prime Collaboration Assurance](#).

You can see the following details:

- License Type—Displays the different types of licenses available, such as, CUWLPremium, CUWLStandard, UCM Advanced, and so on.
- Product —The product type to which the license type belongs.
- Status—The status for a license type - valid, violated, demo.
- Remaining—Count of licenses available or unused, for each license type.

This dashlet is populated once, after nightly CDT discovery is completed, by default. This dashlet is also refreshed after every CDT discovery.

Troubleshooting

Issue: Standalone Prime Licensing Manager (PLM) shows as a non-Cisco Device in Cisco Prime Collaboration Assurance 11.6.

Recommended Action: This is likely to happen when PLM has a SNMP community string configured. To discover PLM correctly, ensure there is no community string configured. If it is, delete it and proceed to discover PLM in Cisco Prime Collaboration Assurance. Basically, PCA does not support SNMP community string configuration for PLM discovery.



Note Not every co-resident PLM uses OS-Admin user to get license information. It depends on the user roles created on CUCM. In most customer deployments, the web administrator has privileges assigned to the CLI/OS Admin. The Cisco Prime Collaboration Assurance can get the license information from this user.

VCS License Usage

You can view the Traversal and Non Traversal license usage for all VCS clusters, individual VCS servers in a cluster, standalone VCS server(s), Cisco Expressway-Core, Cisco Expressway-Edge or a Cisco VCS with Cisco Collaboration Edge or Core. For Cisco Expressway-Core and Cisco Expressway-Edge clusters, you can also view the peak number of calls since last restart in the **Expressway Peak Concurrent Video Calls** column.



Note The licenses must be installed for the peak number of calls to be displayed. For VCS clusters, the column for peak number of calls displays N/A when the license is not installed or when the value is zero.

This dashlet does not auto refresh. You have to refresh the dashlet to get current data.

For VCS version 7.0 and later, any traversal or non-traversal call licenses that have been installed on a cluster peer are available for use by any peer in the cluster. For versions earlier than 7.0 licenses are not shared across the cluster; each peer can only use the licenses that are installed in it.

The number of licenses that can be installed on any one individual peer is limited to the maximum capacity of each VCS unit, as follows:

- 500 non-traversal calls
- 100 traversal calls
- 2,500 registrations

The registration licenses are not shared across a cluster. If a cluster peer becomes unavailable, the shareable licenses installed on that peer will remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer. This will maintain the overall license capacity of the cluster - however, each peer is still limited by its physical capacity as listed above. After this two week period, the licenses associated with the unavailable peer are removed from the cluster. To maintain the same capacity for your cluster, you should ensure that either the problem with the peer is resolved or new option keys are installed on another peer in the cluster.

Customer Voice Portal License Usage

The Customer Voice Portal (CVP) License Usage is categorized under Prime License Manager licenses. This dashlet displays the license usage of CVP call server.

Prerequisites:

- CVP with call server capability must be in managed state in Inventory Management.
- Contact Center Assurance License must be available.

This dashlet display entries based on polling data time interval. The default polling interval is 4 minutes.

This dashlet displays the latest count of polled records for the last 7 days.

You can view the following details:

- Device - CVP call server
- Ports In Use - Number of ports used
- Ports Available - Number of available ports
- Ports Requested - Number of ports requested
- Ports Requests Denied - Number of denied port request

When Contact Center Assurance License expires, the CVP license dashlet does not display the license usage of CVP call server. To continue to use this feature, you must purchase required number of Cisco Prime Collaboration Contact Center Assurance concurrent agent licenses. For more information on licensing, see the [Manage Licenses](#) chapter.



Note Click the values (other than zero) under the various columns to display the respective graphs that plot the columns field against time.

Troubleshooting

1. **Issue:** CVP License Usage dashlet displays **No Data Available**.

Recommended Action: check the following conditions are met.

- CVP device must be in managed state in Inventory Management.
- CVP device must have call server capability.

2. **Issue:** CVP License Usage dashlet display entries, but value of the ports display as zero or keeps changing.

Recommended Action: As CVP License Usage dashlet display entries based on polling data time interval, the value of ports display as zero or keeps changing.

Contact Center Enterprise License Usage

This dashlet displays the license usage of Unified Contact Center Enterprise (Unified CCE).

Prerequisites:

- Unified CCE Router or Unified CCE Peripheral Gateway must be in managed state in Inventory Management.
- Contact Center Assurance License must be available.

This dashlet displays the latest count of polled records for the last 7 days.

You can view the following details:

- Device - Device Name
- Capability - Capability of the device such as router or peripheral gateway
- Agents Logged On - Number of agents currently logged on

This dashlet displays entries based on polling data time interval. The default polling interval is 1 minute.

When Contact Center Assurance License expires, the Unified CCE license dashlet does not displays the license usage of Contact Center Enterprise. To continue to use this feature, you must purchase the required number of Cisco Prime Collaboration Contact Center Assurance concurrent agent licenses. For more information on licensing, see the [Manage Licenses](#) chapter.



Note Click the values (other than zero) under **Agents Logged On** column to display the respective graphs that plot the columns field against time.

Troubleshooting

1. **Issue:** Unified CCE License Usage dashlet displays **No Data Available**.

Recommended Action: Check the following conditions are met.

- Unified CCE device must be in managed state in Inventory Management.
- Unified CCE device must have either Unified CCE Router or Unified CCE PG capability or both.

2. **Issue:** Unified CCE License Usage dashlet displays entries, but **Agents Logged On** value display as zero or keeps changing.

Recommended Action: As Unified CCE License Usage dashlet displays entries based on polling data time interval, the value of **Agents Logged On** display as zero or keeps changing.

Customer Summary Dashboard

You can view detailed information on endpoints, infrastructure devices, and a logical top-level view of the network of a particular customer through the Customer Summary dashboard.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can view the following dashboards from the Cisco Prime Collaboration Assurance home page:

Dashboard	Description
Customer Summary	Information about alarm, endpoints, and inventory aggregated per customer.
For Cisco Prime Collaboration Release 11.1 and earlier TelePresence Exchange	Information about cluster node, call and session control devices, region summary, and conferencing devices. Note If CTX devices are not managed, no data is populated in any of the dashlets.

The Customer Summary dashboard provides information about alarm, endpoints, conference alarms and inventory aggregated per customer. It contains the following dashlets:

Dashlet	Description
Alarm Summary	<p>Displays the list of alarms consolidated per customer based on the severity. Each customer level it gives the total alarms based on the Severity. You can see the following details:</p> <ul style="list-style-type: none">• Customer• Total• Critical• Major• Minor• Warnings
Device Summary	<p>Displays the list of alarms consolidated per customer based on the severity. Each customer level it gives the total alarms based on the severity. You can see the following details:</p> <ul style="list-style-type: none">• Customer• Total• Managed• Unmanaged• Suspended
Endpoint Summary	<p>Displays the list of endpoints for each category, based on the Registration status, per customer. You can see the following details:</p> <ul style="list-style-type: none">• Customer• Total -Registered• Total -Unregistered• Hard Endpoints -Registered• Hard Endpoints -Unregistered• Soft Clients -Registered• Soft Clients -Unregistered

Dashlet	Description
Conferences in Alarms	<p>Displays the number of in-progress conferences with alarms. You can see the following details:</p> <ul style="list-style-type: none"> • Conference Structure • Conference Type • Watched Conferences • For Cisco Prime Collaboration Release 11.1 and earlier Troubleshooting Status • Conference Subject • Scheduler's Org • Start Time
Voice Call Quality Events Summary	Displays summary of active Service Quality (SQ) events with the impacted endpoints. Active SQ events data for the last four hours and the summary of impacted endpoints count are displayed.

Contact Center Assurance Dashboards

The Cisco Prime Collaboration Contact Center Assurance performance dashboards help you to monitor your network by providing near real-time information about the Contact Center components such as Cisco Unified Intelligence Center (CUIC), Finesse, MediaSense, Customer Voice Portal (CVP), Unified Contact Center Enterprise (Unified CCE), Unified Contact Center Express (Unified CCX), and Virtualized Voice Browser.

For Finesse, you can see these dashlets only—System Summary, CPU and Memory, Disk Usage, and Process.



Note If clustering has been configured for CUIC, Finesse, and MediaSense devices the dashboard will also display data for associated devices that belong to a cluster.

If you have deployed Cisco Prime Collaboration Assurance in Enterprise mode, to view the dashboards, go to **Monitor > System View > Performance**, select the product and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, to view the dashboards, go to **Monitor > System View > Customer Summary**, click a customer's name and then click Performance. Select the product and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list.

For Cisco Prime Collaboration Release 11.5 and later

If you have deployed Cisco Prime Collaboration Assurance in Enterprise mode, to view the dashboards, go to **Network Health Overview > Performance**, select the product and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, to view the dashboards, go to **Network Health Overview > Customer Summary**, click a customer's name and then click Performance.

Select the product and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list.

For Cisco Prime Collaboration Release 12.1 and later



Note The cluster has to be discovered with all the nodes for displaying the information on the report exported. The polling happens only for the discovered nodes.

Contact Center Assurance Topology Dashboard

Cisco Prime Collaboration Assurance Advanced provides you with the logical top-level view of an entire IP-based Contact Center, where the Unified Contact Center devices, managed by Cisco Prime Collaboration Assurance, are displayed in a simple topology.

The Contact Center topology lets you view the entire set of devices in an IP-based Contact Center, considered as primary data center (represented as side A in the topology), which is connected to a secondary data center (represented as side B) via the private and public clouds.

If you have deployed Cisco Prime Collaboration Assurance in Enterprise Mode, go to **Monitor > System View > OpsView > Contact Center Topology**.

For Cisco Prime Collaboration Release 11.5 and later

If you have deployed Cisco Prime Collaboration Assurance in Enterprise Mode, go to **Network Health Overview > Contact Center Topology**.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, all devices that are managed by Cisco Prime Collaboration Assurance, for a specific customer, are displayed in this dashboard. To navigate to the Contact Center Topology page: go to the Home page, click a customer (Customer Summary > Customer name). Click Contact Center Topology to view the corresponding Topology for that customer. Managed IP address is displayed for devices in the topology view.

For the clouds (public and private clouds) in the topology, the corresponding interface information, which has been configured, is displayed.

Click on the performance counter name or value (displayed below each device icon in the topology) to view the performance dashboard for that counter in a new tab. For more information on Performance dashboard, see [Create Custom Performance Dashboards](#).

The Contact Center Assurance topology focuses on relationship between various devices in a contact center. Rest your mouse-pointer over a device to view the IP address and host name details. The following devices are displayed in the Contact Center Topology dashboard.

For a list of devices, see [Supported Devices for Cisco Prime Collaboration Assurance](#).

For Cisco Prime Collaboration Release 11.6 and later

The following table lists the link status between devices in the Unified Contact Center:

Device 1	Device 2	Link Status
IPCC	VRU PG	Yes
IPCC	Agent PG	Yes
VRU PG	CVP Call Server	Yes

CVP	VXML Gateway	No
Agent PG	CUCM	Yes
CUCM	Media Sense	Yes
Agent PG	Finesse	Yes
AW/HDS	CUIC	Yes
UCCE Router	Public Cloud	Yes
UCCE Router	Private Cloud	Yes
UCCE Router	CTI	Yes
CTI	CTIOS	Yes
UCCE Router	MR PG	Yes
VRU PG	CVP Reporting Server	No
UCCE Router	Logger	No
UCCE Router	AW/HDS	Yes
CVP	Virtualized Voice Browser (VVB)	No



Note You can view Virtualized Voice Browser (VVB) devices in the Contact Center Assurance topology, when VVB is integrated with CVP 11.5 and later versions.

You can select Contact Center deployment router pair from the **Select Any Router** drop-down list. The topology is displayed for the selected router pair. If a router is deleted from inventory, then the drop-down list does not list the deleted router and corresponding side (Side A or Side B) to which that router belongs to does not appear in the topology.

This is applicable only if you have deployed Cisco Prime Collaboration Assurance in Enterprise mode.

Troubleshooting through Topology View

In the Contact Center Assurance topology view, alarm icons appear next to the device when an alarm is generated on the device. The topology also helps you troubleshoot the issue by allowing a quick launch to the Device 360° view when you rest the mouse over the device IP address. From the Device 360° view, you can see the Alarm and Interface. It also allows you to perform a trace route, ping the device, or go the Alarms and Events page. For details on Device 360° view, see “Managing Inventory” chapter in the [Cisco Prime Collaboration Assurance Guide - Advanced](#).

For a device with alarms, the highest severity of the alarm only will be displayed. When an alarm is generated, it remains in the Contact Center Assurance topology view until it is cleared. The cleared alarm is removed after you invoke the Cisco Prime Collaboration Assurance purge operation.

If you have deployed Cisco Prime Collaboration Assurance in the MSP mode, the shared components are managed under a common deployment. For the device that is shared, you can view the IP address only. If you do not have access to devices that are shared, you cannot launch Device 360° for them (shared devices will be in the view-only mode for those customers who have no access to such devices).

**Note**

- If you have deployed Cisco Prime Collaboration Assurance in the MSP mode, topology view is not supported in cases where you manage both shared (4 K Shared Contact Center) and dedicated deployment models.
- The topology view is automatically refreshed every two minutes.
- Cisco Prime Collaboration Assurance supports single Unified CCE enterprise deployment only.
- Expand/collapse icons are available for abstract devices only.
- Unified CCE Topology is not supported if more than one peripheral gateway (PG) server is managed in either side. Delete the additional peripheral gateways (PGs) from Inventory Management for the topology to launch successfully.

View Historical Trends

Historical trending is enabled by default for the dashlets (CPU Usage, Virtual Memory Usage, and Common Partition Usage) under the System Summary dashboard. Click **Zoom** at the bottom-right corner of the dashlet to view the Trend View graph.

Prerequisites

All devices should be in managed state in Cisco Prime Collaboration Assurance. In case of clusters, all the nodes should be in managed state.

For voice devices (Cisco Unified CM, Cisco Packaged Contact Center Enterprise, Cisco Unified Presence, Cisco Unity Connection, Cisco Media Sense, Cisco Finesse, Cisco Unified IC, and Cisco Unified Contact Center Express), along with the system-defined dashboards, you can also view trends for the device related metrics.

For Cisco Prime Collaboration Release 11.5 and later

For voice devices (Cisco Unified CM, Cisco Packaged Contact Center Enterprise, Cisco Unified Presence, Cisco Unity Connection, Cisco Media Sense, Cisco Finesse, Cisco Unified IC, Cisco Unified Contact Center Express, and Cisco Virtualized Voice Browser), along with the system-defined dashboards, you can also view trends for the device related metrics.

**Note**

- The device related metrics vary based on the device type you select.
- Historical trending is not supported for non-voice devices such as Cisco Unified CCE, Cisco Voice Portal, MCU/TPS, Cisco Unified Border Element, Cisco Voice Gateways, Cisco Unified Communications Manager Express, and ISDN Gateway.

Trend Dashboard

To view trends for metrics, select **Trend** from the Dashboard drop-down list and then from the Metrics Selection dialog box, select the metrics for which you want to enable trend, and click **Add**. You can select any number of metrics that you want, but we recommend that you select only a maximum of six metrics for every device type.

You can also perform the following:

- View data either as a chart or in a tabular format.
- Compare the trends for two or more performance metrics by clicking the **Merge** option.
- Click **Zoom** to view the trend graph in a detailed view. This option also helps you view the history, hourly average, maximum, and minimum data. Using the zoom selector graph displayed in the detailed view, you can adjust the pointer in the time window (x axis) of the graph to view the trend for the selected time period.
- Add more trends using the Add Graph (+) button at the top-right corner of the user interface.
- Change the chart type.

Customer Voice Portal (CVP)

Cisco Prime Collaboration Assurance provides you the call server based CVP dashboards, which are system defined and available when you add the Customer Voice Portal. It also allows you to create custom dashboards based on your monitoring needs. For details on the performance counters, see the [Operations Guide for Cisco Unified Customer Voice Portal](#).

To view the dashboards, go to **Monitor > System View > Performance**, select CVP and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list. Information related to the selected dashboard is displayed in different dashlets, and each dashlet displays the Server details, Current Usage and Maximum value received in the last three minutes.



Note

For the data to be displayed for CVP dashboards in Cisco Prime Collaboration Assurance, turn on the Cisco CVP Call Server and Cisco CVP VXML services in the Customer Voice Portal and enable the ICM, SIP, and IVR subsystems under the CVP Call Server on the operations console (OAMP).

System Summary

Displays information about total memory, page faults per second, handle count, Cisco ICM router calls, and services.

Available Bytes

Displays the amount of physical memory, in bytes, immediately available for allocation to a process or for system use.

Committed Bytes

Display the amount of committed virtual memory, in bytes.

Processor Time

Displays the amount of time a process takes to run, including all the small amounts of time the CPU spends on the process.

Threads

Displays a single sequence of instructions. A process (a running instance of a program) consists of one or more threads.

Page Faults Per Second

Displays the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation; hence this is also equal to the number of page fault operations.

Call Server ICM Aggregate Statistics

Displays total lookup requests, total number of calls, total number of switch legs, and VRU legs.

Call Server Stats ICM Total Lookup Requests

Displays the total number of external Unified CVP VXML Server call routing requests sent to the Unified ICM application since system start time. Calls originating in an external Unified CVP VXML Server need call routing instructions from the Unified ICM application.

Call Server Stats ICM Total Calls

Displays the total number of new calls received by the Unified ICM application for follow-on VRU treatment and routing to a Contact Center agent since system start time.

Call Server Stats ICM Total SIP Switch Legs

Displays the number of VoIP calls received by the ICM application from the Session Initiation Protocol (SIP) since system start time.

Call Server Stats ICM Total VRU Legs

Displays the number of calls that have received VRU treatment from the Unified ICM application since system start time. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED) or Speech Recognition Techniques to understand the customer request.

Call Server ICM Interval Statistics

Displays lookup requests, number of new calls received, number of SIP switch legs, and VRU legs

Call Server Stats ICM Interval SIP Switch Legs

Displays the number of calls received by the ICM application from SIP during the current interval. The Unified ICM application accepts VoIP calls that originate from the Session Initiation Protocol (SIP).

Call Server Stats ICM Interval Lookup Requests

Displays the number of external Unified CVP VXML Server call routing requests sent to the Unified ICM application during the current interval. Calls originating in an external Unified CVP VXML Server need call routing instructions from the Unified ICM application.

Call Server Stats ICM Interval VRU Legs

Displays the number of calls receiving VRU treatment from the Unified ICM application. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED) or speech recognition techniques to understand the customer request during the current interval.

Call Server Stats ICM Interval New Calls

Displays the number of new calls received by the Unified ICM application for follow-on Voice Response Unit (VRU) treatment and routing to a Contact Center agent during the current interval.

Call Server ICM Real Time Statistics

Displays information about active calls, VRU Legs, SIP Switch Legs, and the Lookup Requests.

Call Server Stats ICM Active VRU Legs

Displays the current number of calls receiving Voice Response Unit (VRU) treatment from the Unified ICM server. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED) or Speech Recognition Techniques to understand the customer request.

Call Server Stats ICM Active SIP Switch Legs

Displays the number of calls received by the Unified ICM Server from the SIP protocol. Active SIP Switch Legs indicates the current number of calls received by the ICM Server from the Unified CVP Call Server using the SIP protocol.

Call Server Stats ICM Active Lookup Requests

Displays the current number of external VXML Server call routing requests sent to the ICM Server. Calls originating from an external Unified CVP VXML Server need call routing instructions from the Unified ICM Server.

Call Server Stats ICM Active Calls

Displays the current number of calls being serviced by the ICM Server for a Unified CVP Call Server. This value represents a count of calls currently being serviced by the ICM for the Unified CVP Call Server for follow-on routing to a Contact Center agent.

Call Server Infrastructure JVM Real Time Statistics

Displays information about real time JVM threads in use, total memory, peak memory usage, peak threads usage, current memory usage and available memory.

Call Server Stats RT JVM Threads In Use

Displays the number of threads currently in use in the Java Virtual Machine. This number includes all of the Unified CVP standalone and thread pool threads, and those threads created by the Web Application Server running within the same JVM.

Call Server Stats RT JVM Total Mem

Displays the amount of memory in megabytes available to the Java Virtual Machine. The number indicates how much system memory is available for the Java Virtual Machine.

Call Server Stats RT JVM Peak Mem Usage

Displays the greatest amount of memory used by the Java Virtual machine since startup. The number reported is in megabytes and indicates the peak amount of memory ever used simultaneously by this Java Virtual Machine.

Call Server Stats RT JVM Peak Threads

Displays the greatest amount of threads used simultaneously in the Java Virtual Machine since startup. The peak number of threads used by the Java Virtual Machine includes all Unified CVP standalone and thread pool threads, and threads created by the Web Application Server running within the same JVM.

Call Server Stats RT JVM Current Mem Usage

Displays the current number of megabytes of memory used by the Java Virtual Machine.

Call Server Stats RT JVM Avail Mem

Displays the amount of available memory in the Java Virtual Machine. The number reported is in megabytes and indicates how much of the current system memory claimed by the Java Virtual Machine is not currently being used.

Call Server Infrastructure Thread Pool Real Time Statistics

Displays real time idle pool threads, maximum threads used, running pool threads, maximum threads that exists and core pool threads statistics.

Call Server Stats RT Idle Pool Threads

Displays the number of idle threads waiting for some work.

Call Server Stats RT Max Threads Used

Displays the maximum number of thread pool threads ever simultaneously tasked with some work to process.

Call Server Stats RT Running Pool Threads

Displays the number of running thread pool threads currently processing some work.

Call Server Stats RT Max Threads

Displays the maximum number of thread pool threads that will ever exist simultaneously.

Call Server Stats RT Core Pool Threads

Displays the number of thread pool threads that will never be destroyed no matter how long they remain idle.

Call Server IVR Aggregate Statistics

Displays maximum and average HTTP requests received per second interval, total HTTP requests received, maximum calls aggregate, and maximum HTTP requests processed.

Call Server Stats IVR Max HTTP Req Sec Inter Aggregate Statistics

Displays the current number of simultaneous HTTP requests processed per second by the IVR Service. Maximum number of active HTTP requests processed at the same time since the IVR service started. This is also known as high water marking.

Call Server Stats IVR Max HTTP Requests Inter Aggregate Statistics

Displays the current number of simultaneous HTTP requests processed by the IVR Service.

Call Server Stats IVR Avg HTTP Req Sec Inter Aggregate Statistics

Displays the average number of simultaneous HTTP requests processed per second by the IVR Service.

Call Server Stats IVR Max Calls Agg

Displays the maximum number of simultaneous calls processed by the IVR Service since the service started.

Call Server Stats IVR Total HTTP Req Agg

Displays the number of HTTP Requests received from all clients. This metric is the total number of HTTP Requests received by the IVR Service since system startup.

Call Server IVR Call Interval Statistics

Displays calls finished interval, maximum calls interval, minimum call latency interval, new calls interval, average call latency interval, and maximum call latency interval statistics.

Call Server Stats IVR Calls Finished Inter

Displays the number of Unified CVP Calls that have finished during this interval. A Call, for the purpose of the Call Finished metric, includes both the Switch leg and the IVR leg of the Unified CVP call. When both legs of the call are finished, the *Calls Finished* metric increases.

Call Server Stats IVR Max Calls Inter

Displays the maximum number of calls handled by the IVR service at the same time during this interval.

Call Server Stats IVR Min Call Latency Inter

Displays the minimum amount of time in milliseconds that the IVR Service takes to process a New Call Request or a Request Instruction Request.

Call Server Stats IVR New Calls Inter

Displays the number of New Call requests received from the IOS Gateway. A New Call includes the Switch leg of the call and the IVR leg of the call. This metric counts the number of New Call Requests received by the IVR Service.

Call Server Stats IVR Avg Call Latency Inter

Displays the average amount of time in milliseconds that the IVR Service takes to process a New Call or Call Result Request.

Call Server Stats IVR Max Call Latency Inter

Displays the maximum amount of time in milliseconds that the IVR Service takes to process a New Call Request or a Request Instruction Request.

Call Server IVR HTTP Interval Statistics

Displays maximum & average HTTP requests received per second interval and maximum & active HTTP requests interval statistics.

Call Server Stats IVR Max HTTP Req Sec Inter

Displays the number of HTTP Requests the IVR Service receives each second from all clients. Peak HTTP Requests per Second is the maximum number of HTTP Requests that were processed by the IVR Service in any given second. This is also known as high water marking.

Call Server Stats IVR Max HTTP Requests Inter

Displays the maximum number of HTTP Requests received from a client by the IVR Service during this time interval.

Call Server Stats IVR Avg HTTP Req Sec Inter

Displays the average number of HTTP Requests the IVR Service receives per second.

Call Server Stats IVR Active HTTP Requests Inter

Displays the current number of simultaneous HTTP requests being processed by the IVR Service. Peak Active Requests is a metric that represents the maximum simultaneous HTTP requests being processed by the IVR Service during this time interval.

Call Server IVR Real Time Statistics

Displays IVR active calls and active HTTP requests statistics.

Call Server Stats IVR Active Calls

Displays the number of active calls being serviced by the IVR service.

Call Server Stats IVR Active HTTP Requests

Displays the number of active HTTP requests being serviced by the IVR service.

Call Server SIP Agent Greeting Aggregate Statistics

Displays total greeting answered and total greeting failed.

Call Server Stats SIP Total Greeting Answered

Displays the total number of calls for which agent greeting was successful since the system start time.

Call Server Stats SIP Total Greeting Failed

Displays the total number of calls for which agent greeting failed since the system start time.

Call Server SIP Agent Greeting Interval Statistics

Displays interval greeting answered and interval greeting failed statistics.

Call Server Stats SIP Int Greeting Answered

Displays the number of calls for which agent greeting was successful during the interval.

Call Server Stats SIP Int Greeting Failed

Displays the number of calls for which agent greeting was failed during the interval.

Call Server SIP Aggregate Statistics

Displays information about average LAT first & second aggregate, fail XFR pre & post aggregate, connects received post aggregate, and NC subs aggregate statistics.

Call Server Stats SIP Avg LAT Second Agg

Displays the average latency computation for the calls that have been answered in the second and subsequent transfers.

Call Server Stats SIP Fail XFR Post Agg

Displays the number of failed re-invite requests on the inbound or outbound legs of the call since start time. After a SIP dialog is established, re-INVITE messages perform transfers. Re-invite requests can originate from the endpoints or initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for re-invite requests.

Call Server Stats SIP Conn Recpt Post Agg

Displays the number of Connect messages received by SIP service to perform a Unified CVP Transfer, since system start time. Connects Received includes the regular Unified CVP transfers, and Refer transfers. Any label coming from the ICM service is a Connect message, whether it is a label to send to the VRU or a label to transfer to an agent.

Call Server Stats SIP Avg LAT First Agg

Displays the average latency computation for the calls that have been answered in the first transfer.

Call Server Stats SIP Fail XFR Pre Agg

Displays the total number of failed transfers on the first CVP transfer since system start time. A SIP dialog is established after the first CVP transfer finishes. The metric does not include rejections due to SIP being out of service. The metric includes failed transfers that are after a label is returned from the ICM in a CONNECT message.

Call Server Stats SIP NC Subs Agg

Displays the number of SIP Invite messages received by Unified CVP since system start time. It includes the failed calls, and calls rejected due to the SIP service being out of service.

Call Server SIP Interval Statistics

Displays connects received interval, NC subs interval, average LAT second interval, fail XFR pre & post interval, and interval post call answered statistics.

Call Server Stats SIP Conn Recpt Inter

Displays the number of CONNECT messages received by SIP service in order to perform a call Transfer, in the last statistics aggregation interval. Connects Received includes the regular Unified CVP transfers as well as Refer transfers. Any label coming from the ICM service is considered a CONNECT message, whether it is a label to send to the VRU or a label to transfer to an agent.

Call Server Stats SIP NC Subs Inter

Displays the number of SIP Invite messages received by Unified CVP in the current interval. It includes the failed calls, and calls rejected due to the SIP service being out of service.

Call Server Stats SIP Avg LAT Second Inter

Displays the period of time between the CONNECT from ICM and when the call is answered. The metric includes the average latency computation for the calls that have been answered in the last statistics aggregation interval.

Call Server Stats SIP Int Post Call Answered

Displays the number of service calls answered during the interval.

Call Server Stats SIP Fail XFR Post Inter

Displays the number of failed re-invite requests on either the inbound or outbound legs of the call during the interval. After a SIP dialog is established, re-INVITE messages perform transfers. Re-invite requests can originate from the endpoints or else be initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for both kinds of re-invite requests.

Call Server Stats SIP Fail XFR Pre Inter

Displays the number of failed SIP transfers since system start time. When Unified CVP attempts to make a transfer to the first destination of the call, it sends the initial INVITE request to set up the caller with the ICM routed destination label. The metric does not include rejections due to the SIP Service not running. The metric includes failed transfers that were made after a label was returned from the ICM Server in a CONNECT message.

Call Server SIP Real Time Statistics

Displays number of greeting calls, active calls, whisper calls, total calls.

Call Server Stats SIP Greeting Calls

Displays the total number of greeting calls handled by the SIP service.

Call Server Stats SIP Active Calls

Displays a real time snapshot metric indicating the count of the number of current calls being handled by the SIP service.

Call Server Stats SIP Whisper Calls

Displays the total number of whisper calls handled by the SIP service.

Call Server Stats SIP Total Calls

Displays the total number of calls being handled by the SIP service. The metric includes incoming, outgoing, and ringtone type calls. For each active call in the SIP service, there will be an incoming call, and an outgoing call to the destination of the transfer label.

Call Server SIP Whisper Announcement Interval Statistics

Displays interval whisper answered and interval whisper failed statistics.

Call Server Stats SIP Int Whisper Failed

Displays the number of calls for which whisper announcement was failed during the interval.

Call Server Stats SIP Int Whisper Answered

Displays the number of calls for which whisper announcement was successful during the interval.

Call Server SIP Whisper Announcement Statistics

Displays total whisper answered and total whisper failed.

Call Server Stats SIP Total Whisper Answered

Displays the total number of call for which whisper announce was successful since the system start time.

Call Server Stats SIP Total Whisper Failed

Displays the total number of calls for which whisper announce failed since the system start time.

VXML Infrastructure JVM Memory Real Time Statistics

Displays information about real time JVM available memory, total memory, current memory usage, uptime, and peak memory usage.

VXML Server Stats RT JVM Avail Mem

Displays the amount of available memory in the Java Virtual Machine. The number reported is in megabytes and indicates how much of the current system memory claimed by the Java Virtual Machine is not currently being used.

VXML Server Stats RT JVM Total Mem

Displays the amount of memory in megabytes available to the Java Virtual Machine. The number indicates how much system memory is available for the Java Virtual Machine.

VXML Server Stats RT JVM Current Mem Usage

Displays the current number of megabytes of memory used by the Java Virtual Machine.

VXML Server Stats RT JVM Uptime

Displays the time that the Java Virtual Machine has been running. This time is measured in hh:mm:ss and shows the amount of elapsed time since the Java Virtual Machine process began.

VXML Server Stats RT JVM Peak Mem Usage

Displays the greatest amount of memory used by the Java Virtual machine since startup. The number reported is in megabytes and indicates the peak amount of memory ever used simultaneously by this Java Virtual Machine.

VXML Infrastructure JVM Thread Real Time Statistics

Displays the number of threads currently in use and the peak number of threads used simultaneously in the Java Virtual Machine.

VXML Server Stats RT JVM Threads in Use

Displays the number of threads currently in use in the Java Virtual Machine. This number includes all of the Unified CVP standalone and thread pool threads, and those threads created by the Web Application Server running within the same JVM.

VXML Server Stats RT JVM Peak Threads

Displays the greatest amount of threads used simultaneously in the Java Virtual Machine since startup. The peak number of threads used by the Java Virtual Machine includes all Unified CVP standalone and thread pool threads, and threads created by the Web Application Server running within the same JVM.

VXML Infrastructure Thread Pool Real Time Statistics

Displays real time idle pool threads, core pool threads, maximum threads used, running pool threads, and maximum threads statistics.

VXML Server Stats RT Idle Pool Threads

Displays the number of idle threads waiting for some work.

VXML Server Stats RT Core Pool Threads

Displays the number of thread pool threads that will never be destroyed no matter how long they remain idle.

VXML Server Stats RT Max Threads Used

Displays the maximum number of thread pool threads ever simultaneously tasked with some work to process.

VXML Server Stats RT Running Pool Threads

Displays the number of running thread pool threads currently processing some work.

VXML Server Stats RT Max Threads

Displays the maximum number of thread pool threads that will ever exist simultaneously.

VXML Server Aggregate Statistics

Displays total sessions aggregate, lookup successes aggregate, lookup responses aggregate, lookup failures aggregate, lookup requests aggregate, and reporting events aggregate statistics.

VXML Server Stats Total Sessions Agg

Displays the number of sessions in the Unified CVP VXML server since startup.

VXML Server Stats ICM Lookup Successes Agg

Displays the number of requests from the Unified CVP VXML server to the ICM Service since startup. For each ICM lookup request that succeeded, this metric increases one.

VXML Server Stats ICM Lookup Responses Agg

Displays the number of responses the ICM Service has sent to the Unified CVP VXML server since startup. For each ICM lookup request (successful or failed), this metric increases by one. When multiple response messages are sent back to the Unified CVP VXML server to a single request, this metric increases per response message from the ICM Service.

VXML Server Stats ICM Lookup Failures Agg

Displays the number of requests from the Unified CVP VXML server to the ICM Service since startup. For each ICM lookup request that failed, this metric increases by one. This metric will increase when an ICM failed message was received or in the case the Unified CVP VXML server generates a failed message.

VXML Server Stats ICM Lookup Requests Agg

Displays the number of requests from the Unified CVP VXML server to the ICM Service. For each ICM lookup request (successful or failed), this metric increases by one.

VXML Server Stats Reporting Events Agg

Displays the number of reporting events sent from the Unified CVP VXML server since startup.

VXML Server Interval Statistics

Displays reporting events interval, lookup success interval, lookup request interval, lookup responses interval, lookup failure interval, and session interval statistics.

VXML Server Stats Reporting Events Inter

Displays the number of events sent to the Reporting Server from the Unified CVP VXML server.

VXML Server Stats ICM Lookup Success Inter

Displays the number of successful requests from the Unified CVP VXML server to the ICM Service in the current interval.

VXML Server Stats ICM Lookup Request Inter

Displays the number of requests from the Unified CVP VXML server to the ICM Service.

VXML Server Stats ICM Lookup Responses Inter

Displays the number of responses to failed and successful ICM Lookup Requests that the ICM Service sends to the Unified CVP VXML server. In the case that multiple response messages are sent back to the Unified CVP VXML server to a single request, this metric increases per response message from the ICM Service.

VXML Server Stats ICM Lookup Failure Inter

Displays the number of requests from the Unified CVP VXML server to the ICM Service in the current interval. This metric increases when an ICM failed message is received or when the Unified CVP VXML server generates the failed message.

VXML Server Stats Session Inter

Displays the number of sessions in the Unified CVP VXML server.

VXML Server Real Time Statistics

Displays the number of active ICM lookup requests and active sessions statistics.

VXML Server Stats Active ICM Lookup Requests

Displays the number of current ICM requests being handled by the Unified CVP VXML server.

VXML Server Stats VXML Active Sessions

Displays the number of current sessions being handled by the Unified CVP VXML server.

Unified Contact Center Enterprise (Unified CCE)

Cisco Prime Collaboration Assurance provides you the Unified CCE dashboards, which are system defined and available when you add the Unified CCE. It also allows you to create custom dashboards based on your monitoring needs. For details on the performance counters, see the [Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise](#).

To view the dashboards, go to **Monitor > System View > Performance**, select Unified CCE and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list. Information related to the selected dashboard is displayed in different dashlets, and each dashlet displays the Server details, Current Usage and Maximum value received in the last three minutes.



Note

The Unified Contact Center Enterprise should be functioning, for the data to be displayed for Unified CCE dashboards in Cisco Prime Collaboration Assurance.

System Summary

Displays information about total memory, page faults per second, handle count, Cisco ICM router calls, and services.

Total Memory

Displays the total amount of virtual memory utilization on the system.

Page Faults Per Second

Displays the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation; hence this is also equal to the number of page fault operations.

Handle Count

Displays the total count of handles currently open by this process. This number is equal to the sum of the handles currently open by each thread in this process.

Cisco ICM Router Calls

Displays the (calculated) inbound call rate measured in the number of calls received per second.

Services

Displays the name of the service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable).

CTI SVR Agent Status

Displays the ready agent count & not ready agent count, logged in & logged out agent count, talking agent count, and work not ready agent count.

Ready Agent Count

Displays the number of Agents that are logged in and are ready to accept calls.

Work Not Ready Agent Count

Agents occupied with work associated with the last call. This implies that agent is no longer connected to the call. These agents are not ready to receive additional calls when they exit this state.

Not Ready Agent Count

Displays the number of Agents that are logged in, but occupied with tasks other than accepting incoming calls.

Logged In Agent Count

Displays the Agents that have logged in. This does not necessarily indicate that they are ready to accept calls.

Talking Agent Count

Displays the number of Agents currently talking on Inbound or Outbound calls.

Logged Out Agent count

Displays the number of Agents that are logged out of the system. This count helps in validating the statistics if there are any state mismatches.

CTI SVR Session Status

Displays sessions closed, sessions failed, sessions unknown, sessions open, total sessions, and sessions opening.

Sessions Closed

Displays the total number of sessions that are terminated by the CTI Server.

Sessions Failed

Displays the number of sessions that failed due to various reasons like missing heartbeat, open request timeout, session inactivity, and so on. These timers are configurable parameters in CTI Server.

Sessions Unknown

Displays the number of sessions for which there is no socket connection made yet.

Sessions Open

Displays the number of sessions that were successfully setup.

Total Sessions

Displays the total number of sessions maintained by CTI Server.

Sessions Opening

Displays the number of sessions that are in the process of setting up a connection.

CTI SVR Call Count

Displays active call count, private call count, cleared call count and deactivated call count.

Active Call Count

Displays the number of calls that are currently in progress.

Private Call Count

Displays the number of calls that are privately tracked by CTI Server and which are not reported to OPC.

Cleared Call Count

Displays the number of calls that no longer exist in the system.

Deactivated Call Count

Displays the number of calls that are not currently active and eventually cleared.

EAPIM Calls And Messages Count

Displays calls per second, messages per second, invalid call count, agent count, call count, and messages sent.

Calls Per Sec

Displays the number of incoming calls per second.

Messages Per Sec

Displays the number of call events, agent events exchanged per second between the JTAPI Gateway and CM PIM.

Invalid Call Count

Displays the number of calls that are not in any of the valid call states.

Agent Count

Displays the number of agents that are currently configured in system.

Call Count

Displays the number of calls that are in progress.

Messages Sent

Displays the number of call events, agent events, and CSTA messages sent today.

OPC SideA Agent Count

Displays sideA agent count, work ready & work not ready sideA agent count, ready & not ready sideA agent count, and talking sideA agent count.

Work Not Ready SideA Agent Count

Displays the agents occupied with work associated with the last call. This implies that agent is no longer connected to the call. These Agents are not ready to receive additional calls when they exit this state.

Ready SideA Agent Count

Displays the number of Agents that are logged in and are ready to accept calls.

Not Ready SideA Agent Count

Displays the number of Agents that are logged in, but occupied with task other than accepting incoming calls.

Talking SideA Agent Count

Displays the number of Agents currently talking on Inbound or Outbound calls.

SideA Agent Count

Displays the number of Agents that are configured in the system.

Work Ready SideA Agent Count

Displays the agents occupied with work associated with the last call. This implies that agent is no longer connected to the call and is ready to receive additional calls when they exit this state.

OPC Call Count

Displays alerting call count, failed call count, call count, queued call count, connected call count, and initiated call counts.

OPC Alerting Call Count

Displays the number of calls for which the device is in alerting (ringing) state. This indicates that a call wishes to become connected to a device.

OPC Failed Call Count

Displays the number of calls for which the normal state progression has been aborted. This state generally refers to the condition when a device tries to become connected to a call or a call tries to become connected to a device and the attempt fails. Failed can result because of failure to connect the calling device and call, failure to connect the called device and call, failure to create the call, and other reasons.

OPC Call Count

Displays the number of Calls that are currently active.

OPC Queued Call Count

Displays the number of calls for which the normal state progression has been stalled. This state generally refers to two conditions but can apply to others as well. One condition is when a device is trying to establish a connection with a call, and the process is stalled. The second condition is when a call tries to establish a connection with a device and that process is stalled.

OPC Connected Call Count

Displays the number of calls for which the device is actively participating in the call.

OPC Initiated Call Count

Displays the number of calls for which the device has requested for a service. Often this is the dialing state.

OPC SideA Skill Group And Service Count

Displays skill group count and services count.

OPC Skill Group Count

Displays a group of agents who share a common set of skills and who can, therefore, all handle specific types of calls. Each skill group contains one or more agents. If supported by the peripheral, each agent can be a member of more than one skill group. This counter gives the number of various skill groups available for the agents to sign in.

OPC Service Count

Displays the number of services that are configured to process the calls. A service is a type of processing the caller requires. A peripheral might have services defined for sales, technical support, or opening new accounts. Each service has one or more skill groups whose members can provide the service. Each skill group can be associated with more than one service.

VRUPIM Call and Messages Count

Displays VRUPIM new calls, pre routed calls, calls at VRU, messages to VRU, messages from VRU, and connection resets count.

VRUPIM New Calls

Displays the rate at which new calls arrive at the Voice Response Unit (VRU). New calls are calls not under ICM script control when arriving at a Service Control VRU.

VRUPIM Pre Routed Calls

Displays the rate at which Pre-Routed calls arrive at VRU. Pre-Routed calls are calls under ICM script control when arriving at a Service Control VRU.

VRUPIM Calls at VRU

Displays the number of calls that are currently at VRU. For a VRU that only uses a Call Routing Interface, this value is zero.

VRUPIM Messages To VRU

Displays the rate at which messages are sent to VRU. This counter is active only when enabled in ICM registry.

VRUPIM Messages From VRU

Displays the rate at which messages are received from VRU. This counter is active only when enabled in ICM registry.

VRUPIM Connection Resets

Displays the number of times the TCP connection between ICM and the Voice Response Unit changed from an established state to a closed state since the application started.

ICM Router Call Status

Displays number of calls in the router, router calls, calls in queue, and calls in progress.

ICM Router Calls in Router

Displays the number of active calls in the Router, including the calls sent to VRU for treatment or queuing and the calls the Router is waiting for response from the routing client.

ICM Router Calls

Displays the (calculated) inbound call rate measured in the number of calls received per second.

ICM Router Calls In Queue

Displays the number of calls queued in all network Voice Response Units (VRUs), from the Router's perspective, including those calls that are in the process of transferring to the VRU for queuing.

ICM Router Calls In Progress

Displays the number of calls currently in progress (being controlled by the CCE application).

ICM Router Status

Displays router rejection percentage, router size in KB, messages processed, maximum & average process time, and congestion level.

ICM Router Rejection Percentage

Displays the number of calls rejected due to high call rates.

ICM Router State Size in KB

Displays the current Router state size - the total size of all of the state transfer objects in Router memory; this size is measured in kilobytes. After one Router side goes out of service, when it returns in-service, the Router state is transferred from the surviving Router side to the returning Router side.

ICM Router Messages Processed

Displays the number of MDS messages Router processed. By default, this counter is disabled.

ICM Router Max Process Time in ms

Displays the maximum time (in milliseconds) the Router spends processing a MDS message.

ICM Router Avg Process Time

Displays the average time the Router spends processing a MDS message.

ICM Router Congestion Level

Displays the number of calls queued or blocked due to high call rates.

ICM Logger DB Write

Displays write average time, write records processed, and number of DB writes.

ICM Logger Number of DB Write

Displays the number of database writes (records/rows) in the historical logger process that is written to the database at the time the counter is polled.

ICM Logger DB Write Average Time

Displays the average amount of time, in 100 nanosecond units, required to write data to a table in the central controller database. This value represents the average time per write of the write operations that occurred in the past second. This object is a good indicator of contention for database access.

ICM Logger DB Write Records Processed

Displays the number of records processed – written to the database – in the Historical Logger Process in the past second.

ICM Distributor Real Time Agent Queue

Displays agent queue depth, skill group queue depth, agent DB write average time & write records processed, and agent skill group DB write records processed & write average time.

ICM Distributor Real Time Agent Queue Depth

Displays the queue depth – number of pending write transactions – for the Agent table in the Real-time Client process.

ICM Distributor Real Time Agent Skill Group Queue Depth

Displays the queue depth – number of pending write transactions – for the Agent Skill Group table in the Real-time Client process.

ICM Distributor Real Time Agent DB Write Records Processed

Displays the number of Agent table records written by the Real-time Client process in the past 1 second interval.

ICM Distributor Real Time Agent DB Write Average Time

Displays the average time - in units of 100 ns - for the Real-time Client process to write an Agent table transaction within the past 1 second interval.

ICM Distributor Real Time Agent Skill Group DB Write Average Time

Displays the average time - in units of 100 ns - for the Real-time Client process to write an Agent Skill Group table transaction within the past 1 second interval.

ICM Distributor Real Time Agent Skill Group DB Write Records Processed

Displays the number of Agent Skill Group table records written by the Real-time Client process in the past 1 second interval.

Distributor Real Time Route DB Write

Displays the number of write records processed, queue depth, and average time taken to write an route table transaction.

ICM Distributor Real Time Route DB Write Average Time

Displays the average time – in units of 100 ns – for the Real-time Client process to write an Route table transaction within the past 1 second interval.

ICM Distributor Real Time Route DB Write Records Processed

Displays the number of Route table records written by the Real-time Client process in the past 1 second interval.

ICM Distributor Real Time Route Queue Depth

Displays the queue depth – number of pending write transactions – for the Route table in the Real-time Client process.

Distributor Real Time Service DB Write

Displays service DB write records processed, queue depth, and average time.

ICM Distributor Real Time Service DB Write Records Processed

Displays the number of Service table records written by the Real-time Client process in the past 1 second interval.

ICM Distributor Real Time Service Queue Depth

Displays the queue depth – number of pending write transactions – for the Service table in the Real-time Client process.

ICM Distributor Real Time Service DB Write Average Time

Displays the average time – in units of 100 ns – for the Real-time Client process to write an Service table transaction within the past 1 second interval.

Distributor Real Time Skill Group DB Write

Displays skill group write records processed, average time, and queue depth.

ICM Distributor Real Time Skill Group DB Write Records Processed

Displays the number of Skill Group table records written by the Real-time Client process in the past 1 second interval.

ICM Distributor Real Time Skill Group Queue Depth

Displays the queue depth – number of pending write transactions – for the Skill Group table in the Real-time Client process.

ICM Distributor Real Time Skill Group DB Write Average Time

Displays the average time – in units of 100 ns – for the Real-time Client process to write an Skill Group table transaction within the past 1 second interval.

Distributor Real Time CallType DB Write

Displays call type DB write average time, records processed, and queue depth.

ICM Distributor Real Time Call Type DB Write Average Time

Displays the average time – in units of 100 ns – for the Real-time Client process to write an CallType table transaction within the past 1 second interval.

ICM Distributor Real Time Call Type DB Records Processed

Displays the number of CallType table records written by the Real-time Client process in the past 1 second interval.

ICM Distributor Real Time Call Type Queue Depth

Displays the queue depth – number of pending write transactions – for the CallType table in the Real-time Client process.

Distributor Replication DB Write

Displays distributor replication DB average time and records processed.

ICM Distributor Replication DB Write Average Time

Displays the average time – in units of 100 nanoseconds – for database write operations in the HDS Replication process during the past 1 second interval.

ICM Distributor Replication DB Records Processed

Displays the number of records written by the HDS Replication process in the past 1 second interval.

Cisco Unified Intelligence Center

Cisco Prime Collaboration Assurance provides you the Cisco Unified Intelligence Center dashboards, which are system defined and available when you add Cisco Unified Intelligence Center. Cisco Prime Collaboration Assurance also allows you to create custom dashboards based on your monitoring needs. For details on the performance counters, see the [Administration Console User Guide for Cisco Unified Intelligence Center](#).

To view the dashboards, go to **Monitor > System View > Performance**, select Intelligence Center and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list. Information related to the selected dashboard is displayed in different dashlets, and each dashlet displays the Server details, Current Usage and Maximum value received in the last three minutes.

Prerequisites:

- Cisco Unified Intelligence Center must be managed in Cisco Prime Collaboration Assurance.
- Cisco Unified Intelligence Center of version 9.x and later must be reachable for the data to be displayed for Cisco Unified Intelligence Center dashboards in Cisco Prime Collaboration Assurance.

The following are the newly supported Cisco Unified Intelligence Center dashboards:

System Summary

Displays information about CPU usage, Virtual Memory usage, Common Partition Usage, and the Critical Services status. As a system administrator you can monitor the System Summary dashlets to analyze the slow response of the system.

CPU Usage

Displays the real time CPU usage and the maximum value in the past 3 minutes.

Limitation: You have to use other reports also to monitor the system at the per-process level to determine which process or processes are causing CPU issues.

Virtual Memory Usage

Displays the real-time Virtual Memory usage and the maximum value in the past 3 minutes.

Common Partition Usage

Displays the real-time Common Partition Usage and the maximum value in the past 3 minutes.

Services

Displays the name of the service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable).



Note If the service status is displayed as Unknown State, the system cannot determine the state of the service.

CPU and Memory

Displays information about CPU usage, virtual memory usage, memory usage, and processors for the server.

CPU Usage

Displays the total CPU that is consumed, and the maximum CPU that is consumed in the last 3 minutes.

Virtual Memory Usage

Displays the total virtual memory that is consumed, and the maximum virtual memory that is consumed in last 3 minutes.

Memory Usage

Displays the following information:

- % VM Used: Represents the percentage of system virtual memory utilization on the system. The value of the % VM Used counter is equal to the value that is derived from either of the following two equations:

$$\frac{(\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} + \text{Used Swap KBytes})}{(\text{Total KBytes} + \text{Total Swap KBytes})}$$

$$\text{Used VM KBytes} / \text{Total VM KBytes}$$

- Total: Represents the total amount of memory in the system in kilobytes.

Used

Represents the amount of system physical memory that is in use, in kilobytes, in the system. The value of the Used KBytes counter is equal to the value that is derived from the following equation:

$$\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes}$$

The Used KBytes value is different from the Linux Used value that is shown in top or free command output. The used value that is shown in Linux top or free command output is equal to $\text{Total KBytes} - \text{Free KBytes}$, and it also includes the sum of Buffers KBytes and Cached KBytes.

Free

Represents the total amount of memory that is available in the system, in kilobytes.

Shared

Represents the amount of shared memory in the system, in kilobytes.

Buffers

Represents the capacity of buffers in the system, in kilobytes.

Cached

Represents the amount of cached memory, in kilobytes.

Total Swap

Represents the total amount of swap space, in kilobytes, in the system.

Used Swap

Represents the amount of swap space, in kilobytes, that is in use on the system.

Free Swap

Represents the amount of free swap space, in kilobytes, that is available in the system.

Processors

Displays the following information:

- **Processor:** Instance of the processor. For example, a quad-core CPU has four processors: 0, 1, 2, and 3.
- **% CPU:** The processor's share of the elapsed CPU time excluding the idle time since last update, expressed as a percentage of CPU time.
- **User:** Displays the percentage of CPU utilization that the CPU spent executing at the user level (application).
- **Nice:** Displays the percentage of CPU utilization that the CPU spent executing at the user level with nice priority.
- **System:** Displays the percentage of CPU utilization that the CPU spent executing at the system level (kernel).
- **Idle:** Displays the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.
- **IRQ:** Displays the percentage of time that the processor spent executing the interrupt request, which is assigned to devices for interrupt, or sending a signal to the computer when it finished processing.
- **Soft IRQ:** Displays the percentage of time that the processor spent executing the software interrupt (softirq), which means that task switching is deferred until later to achieve better performance.
- **IO Wait:** Displays the percentage of time that the CPU or CPUs were idle, during which the system had an outstanding disk I/O request.

Disk Usage

Displays information about disk usage on the node. It has the following dashlets: Common Partition Usage, Swap Partition Usage, Spare Partition Usage, Shared Memory Partition Usage, Active Partition Usage, Boot Partition Usage.

Each of the dashlets displays the following information:

Used

Represents the percentage of disk space that is in use on this file system.

Max Past 3 min

Represents the percentage of disk space that is in use on this file system in the past 3 minutes.

Used Space

Represents the amount of disk space, in megabytes, that is in use on this file system.

Total Space

Represents the amount of total disk space, in megabytes, that is on this file system. The number in this counter may differ from other total size values for disk space that you may see on the system, because the value of the Total Mbytes counter is the sum of Used Mbytes performance counter and the Free value that is shown in the CLI (show status) output. The Total Mbytes value is less than this CLI output for Total, which includes the minfree percentage of reserved file system disk blocks. Keep a minfree reserved to ensure a sufficient amount of disk space for the file system to operate at high efficiency.

Process

Displays information about the processes that are running on the node.

Process

Name of the process.

PID

The task's unique process ID, which periodically wraps, although it never restarts at zero.

& CPU

The task's share of the elapsed CPU time since the last update and is expressed as a percentage of total CPU time.

Status

The task's process status:

- 0: Running
- 1: Sleeping
- 2: Uninterruptible disk sleep
- 3: Zombie
- 4: Traced or stopped (on a signal)
- 5: Paging
- 6: Unknown

Shared Memory

The amount of shared memory, in kilobytes, that a task is using. Other processes could potentially share the same memory.

Nice

The nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining whether to run the task.

VmRSS

The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes, including Code, Data, and Stack.

VmSize

The total amount of virtual memory, in kilobytes, that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

VmData

The virtual memory usage of the heap for the task in kilobytes.

Thread Count

The number of threads that are currently grouped with the task. The negative value -1 indicates that this counter is currently not available because thread statistics (including all performance counters in the Thread object as well as the Thread Count counter in the Process object) have been turned off because the system's total processes and threads have exceeded the default threshold value.

Datastack Size

The stack size for task memory status.

Page Fault Count

The number of major page faults that a task encountered that required the data to be loaded into memory.

Historical Data Aggregated

Displays information about the reporting engine info report historical runtime total.

Reporting Engine Info Report Historical Runtime Total

Displays the total amount of seconds spent running reports.

Tomcat

The Tomcat provides information about Tomcat non-secure and secure Hypertext Transport Protocol (HTTP) connectors. A Tomcat Connector represents an endpoint that receives requests and sends responses.

The Connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Intelligence Center web pages are accessed.

It displays information about MBytes received, MBytes sent, threads busy, threads maximum, connector errors, and connector requests.

Cisco Tomcat Connector MBytes Received

Displays the total number of data received by the Tomcat connector.

Cisco Tomcat Connector MBytes Sent

Displays the total number of data that the Tomcat connector has sent.

Cisco Tomcat Connector Threads Busy

Displays the Tomcat connector's current number of busy/in-use request processing threads.

Cisco Tomcat Connector Threads Max

Displays the Tomcat connector's maximum number of request processing threads.

Cisco Tomcat Connector Errors

Displays the total number of HTTP errors (for example, 401 Unauthorized) encountered by the Tomcat connector.

Cisco Tomcat Connector Requests

Displays the total number of requests that have been handled by the Tomcat connector.

Live Data

Displays information about live messages processed, live messages processed size, live messages processing latency, live messages received size, live messages received, and live messages transmitted.

Reporting Engine Info Live Messages Processed

Displays the total number of Live Data messages processed to OpenFire.

Reporting Engine Info Live Messages Processed Size

Displays the total size of Live Data messages processing (bytes) to OpenFire.

Reporting Engine Info Live Messages Processing Latency

Displays the total amount of time spent in processing the Live Data milliseconds(ms) to OpenFire.

Reporting Engine Info Live Messages Received Size

Displays the total size of Live Data messages received (bytes) from the streaming data sources.

Reporting Engine Info Live Messages Received

Displays the total number of Live Data messages received from the streaming data sources.

Reporting Engine Info Live Messages Transmitted

Displays the total number of Live Data messages transmitted from the streaming data sources.

Tomcat JVM

The Tomcat Java Virtual Machine (JVM) object provides information about the Tomcat JVM, which represents, among other things, a pool of common resource memory used by Unified Intelligence Center.

Displays information about the KBytes memory free, KBytes memory maximum, and KBytes memory total.

Cisco Tomcat JVM KBytes Memory Free

Displays the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects created by Tomcat and its web applications such as Unified Intelligence Center. When the amount of free dynamic memory is low, more memory is automatically allocated and total memory size (represented by the KbytesMemoryTotal counter) increases up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.

Cisco Tomcat JVM KBytes Memory Max

Displays the maximum dynamic memory block size for the Unified Intelligence Center Tomcat Java Virtual Machine.

Cisco Tomcat JVM KBytes Memory Total

Displays the current total dynamic memory block size - including free and in-use memory - for the Tomcat Java Virtual Machine.

Realtime Data

Displays the report realtime cells retrieved, report realtime completed, report realtime running, report realtime runtime, report realtime waiting, and report realtime rows retrieved.

Reporting Engine Info Report Realtime Cells Retrieved

Displays the total number of cells (rows times columns) that have been retrieved from all data sources.

Reporting Engine Info Report Realtime Completed

Displays the total number of reports that have been successfully executed.

Reporting Engine Info Report Realtime Running

Displays the number of reports that are currently running. A report is currently running when the Runnable object has been assigned a thread from the pool. It does not include those that are waiting in a queue for a thread to become available.

Reporting Engine Info Report Realtime Runtime

Displays the total amount of seconds spent running reports.

Reporting Engine Info Report Realtime Waiting

Displays the total number of reports that are currently queued for execution.

Reporting Engine Info Report Realtime Rows Retrieved

Displays the total number of rows that have been retrieved by Unified Intelligence Center from data sources.

Realtime Interval

Displays information about report realtime cells retrieved interval, report realtime completed interval, report realtime running interval, report realtime runtime interval, report realtime waiting interval, and report realtime rows retrieved interval.

Reporting Engine Info Report Realtime Cells Retrieved Interval

Displays the total number of cells (rows times columns) that have been retrieved from all data sources over the last interval.

Reporting Engine Info Report Realtime Completed Interval

Displays the change of counter Report (H/RT) Completed over the last interval.

Reporting Engine Info Report Realtime Running Interval

Displays the interval measurement of the Report (H/RT) Running counter.

Reporting Engine Info Report Realtime Runtime Interval

Displays the change of counter Report (H/RT) Runtime over the last interval.

Reporting Engine Info Report Realtime Waiting Interval

Displays the change of counter ReportRealtimeWaiting over the last interval.

Reporting Engine Info Report Realtime Rows Retrieved Interval

Displays the interval measurement of the Report (H/RT) RowsRetrievedTotal counter.

Historical Data

Displays the report historical cells retrieved, report historical completed, report historical rows retrieved, report historical running, report historical runtime, and report historical waiting.

Reporting Engine Info Report Historical Cells Retrieved

Displays the total number of cells (rows times columns) that have been retrieved from all data sources.

Reporting Engine Info Report Historical Completed

Displays the total number of reports that have been successfully executed.

Reporting Engine Info Report Historical Rows Retrieved

Displays the total number of rows that have been retrieved by Unified Intelligence Center from data sources.

Reporting Engine Info Report Historical Running

Displays the number of (H/RT) reports that are currently running. A report is currently running when the Runnable object has been assigned a thread from the pool. It does not include those that are waiting in a queue for a thread to become available.

Reporting Engine Info Report Historical Runtime

Displays the total amount of seconds spent running reports.

Reporting Engine Info Report Historical Waiting

Displays the total number of reports that are currently queued for execution.

Historical Data Interval

Displays information about the report historical cells retrieved interval, report historical completed interval, report historical rows retrieved interval, report historical running interval, report historical runtime interval, and report historical waiting interval.

Reporting Engine Info Report Historical Cells Retrieved Interval

Displays the total number of cells (rows times columns) that have been retrieved from all data sources over the last interval.

Reporting Engine Info Report Historical Completed Interval

Displays the change of counter Report (H/RT) Completed over the last interval.

Reporting Engine Info Report Historical Rows Retrieved Interval

Displays the interval measurement of the Report (H/RT) RowsRetrievedTotal counter.

Reporting Engine Info Report Historical Running Interval

Displays the interval measurement of the Report (H/RT) Running counter.

Reporting Engine Info Report Historical Runtime Interval

Displays the change of counter Report (H/RT) Runtime over the last interval.

Reporting Engine Info Report Historical Waiting Interval

Displays the change of counter ReportRealtimeWaiting over the last interval.

Cisco MediaSense

Cisco Prime Collaboration Assurance provides you the MediaSense dashboards, which are system defined and available when you add Cisco MediaSense. Cisco Prime Collaboration Assurance also allows you to create custom dashboards based on your monitoring needs. For details on the performance counters, see the [Cisco MediaSense User Guide](#).

To view the dashboards, go to **Monitor > System View > Performance**, select MediaSense and cluster from the Cluster drop-down list and then select the required dashboard from the Dashboard drop-down list. Information related to the selected dashboard is displayed in different dashlets, and each dashlet displays the Server details, Current Usage and Maximum value received in the last three minutes.

Prerequisites:

- Cisco MediaSense must be managed in Cisco Prime Collaboration Assurance.
- Cisco MediaSense must be reachable, for the data to be displayed on MediaSense dashboards in Cisco Prime Collaboration Assurance.

The following are the newly supported Cisco MediaSense dashboards:

System Summary

Displays information about CPU usage, Virtual Memory usage, Common Partition Usage, and the Critical Services status. As a system administrator you can monitor the System Summary dashlets to analyze the slow response of the system.

CPU Usage

Displays the real time CPU usage and the maximum value in the past 3 minutes.

Limitation: You have to use other reports also to monitor the system at the per-process level to determine which process or processes are causing CPU issues.

Virtual Memory Usage

Displays the real-time Virtual Memory usage and the maximum value in the past 3 minutes.

Common Partition Usage

Displays the real-time Common Partition Usage and the maximum value in the past 3 minutes.

Services

Displays the name of the service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable).



Note If the service status is displayed as Unknown State, the system cannot determine the state of the service.

CPU and Memory

Displays information about CPU usage, virtual memory usage, memory usage, and processors for the server.

CPU Usage

Displays the total CPU that is consumed, and the maximum CPU that is consumed in the last 3 minutes.

Virtual Memory Usage

Displays the total virtual memory that is consumed, and the maximum virtual memory that is consumed in last 3 minutes.

Memory Usage

Displays the following information:

- % VM Used: Represents the percentage of system virtual memory utilization on the system. The value of the % VM Used counter is equal to the value that is derived from either of the following two equations:

$$\frac{(\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} + \text{Used Swap KBytes})}{(\text{Total KBytes} + \text{Total Swap KBytes})}$$
$$\text{Used VM KBytes} / \text{Total VM KBytes}$$

- Total: Represents the total amount of memory in the system in kilobytes.

Used

Represents the amount of system physical memory that is in use, in kilobytes, in the system. The value of the Used KBytes counter is equal to the value that is derived from the following equation:

$$\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes}$$

The Used KBytes value is different from the Linux Used value that is shown in top or free command output. The used value that is shown in Linux top or free command output is equal to $\text{Total KBytes} - \text{Free KBytes}$, and it also includes the sum of Buffers KBytes and Cached KBytes.

Free

Represents the total amount of memory that is available in the system, in kilobytes.

Shared

Represents the amount of shared memory in the system, in kilobytes.

Buffers

Represents the capacity of buffers in the system, in kilobytes.

Cached

Represents the amount of cached memory, in kilobytes.

Total Swap

Represents the total amount of swap space, in kilobytes, in the system.

Used Swap

Represents the amount of swap space, in kilobytes, that is in use on the system.

Free Swap

Represents the amount of free swap space, in kilobytes, that is available in the system.

Processors

Displays the following information:

- **Processor:** Instance of the processor. For example, a quad-core CPU has four processors: 0, 1, 2, and 3.
- **% CPU:** The processor's share of the elapsed CPU time excluding the idle time since last update, expressed as a percentage of CPU time.
- **User:** Displays the percentage of CPU utilization that the CPU spent executing at the user level (application).
- **Nice:** Displays the percentage of CPU utilization that the CPU spent executing at the user level with nice priority.
- **System:** Displays the percentage of CPU utilization that the CPU spent executing at the system level (kernel).
- **Idle:** Displays the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.
- **IRQ:** Displays the percentage of time that the processor spent executing the interrupt request, which is assigned to devices for interrupt, or sending a signal to the computer when it finished processing.
- **Soft IRQ:** Displays the percentage of time that the processor spent executing the software interrupt (softirq), which means that task switching is deferred until later to achieve better performance.
- **IO Wait:** Displays the percentage of time that the CPU or CPUs were idle, during which the system had an outstanding disk I/O request.

Disk Usage

Displays information about disk usage on the node. It has the following dashlets: Common Partition Usage, Swap Partition Usage, Spare Partition Usage, Shared Memory Partition Usage, Active Partition Usage, Boot Partition Usage.

Each of the dashlets displays the following information:

Used

Represents the percentage of disk space that is in use on this file system.

Max Past 3 min

Represents the percentage of disk space that is in use on this file system in the past 3 minutes.

Used Space

Represents the amount of disk space, in megabytes, that is in use on this file system.

Total Space

Represents the amount of total disk space, in megabytes, that is on this file system. The number in this counter may differ from other total size values for disk space that you may see on the system, because the value of the Total Mbytes counter is the sum of Used Mbytes performance counter and the Free value that is shown in the CLI (show status) output. The Total Mbytes value is less than this CLI output for

Total, which includes the minfree percentage of reserved file system disk blocks. Keep a minfree reserved to ensure a sufficient amount of disk space for the file system to operate at high efficiency.

Process

Displays information about the processes that are running on the node.

Process

Name of the process.

PID

The task's unique process ID, which periodically wraps, although it never restarts at zero.

& CPU

The task's share of the elapsed CPU time since the last update and is expressed as a percentage of total CPU time.

Status

The task's process status:

- 0: Running
- 1: Sleeping
- 2: Uninterruptible disk sleep
- 3: Zombie
- 4: Traced or stopped (on a signal)
- 5: Paging
- 6: Unknown

Shared Memory

The amount of shared memory, in kilobytes, that a task is using. Other processes could potentially share the same memory.

Nice

The nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining whether to run the task.

VmRSS

The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes, including Code, Data, and Stack.

VmSize

The total amount of virtual memory, in kilobytes, that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

VmData

The virtual memory usage of the heap for the task in kilobytes.

Thread Count

The number of threads that are currently grouped with the task. The negative value -1 indicates that this counter is currently not available because thread statistics (including all performance counters in the Thread object as well as the Thread Count counter in the Process object) have been turned off because the system's total processes and threads have exceeded the default threshold value.

Datastack Size

The stack size for task memory status.

Page Fault Count

The number of major page faults that a task encountered that required the data to be loaded into memory.

Incoming Call Breakdown

Displays information about the service classified for recording, service classified for playback, service classified for reject, and service classified as anything else.

Cisco MediaSense Call Control Service Classified for Recording

Displays the number of calls handled as recording requests.

Cisco MediaSense Call Control Service Classified for Playback

Displays the number of calls handled as playback requests.

Cisco MediaSense Call Control Service Classified for Reject

Displays the number of calls rejected based on the configuration.

Cisco MediaSense Call Control Service Classified as Anything Else

Displays the number of calls accepted but not handled as playback or recording requests.

Error Analysis

Displays information about the service number of recorded sessions with errors, agent rejected convert requests, agent rejected RTSP monitoring requests, agent rejected RTSP playback requests, and agent rejected raw download requests.

Cisco MediaSense Call Control Service Number of Recorded Sessions with Errors

Displays the number of recorded sessions completed with errors.

Cisco MediaSense Storage Management Agent Rejected Convert Requests

Displays the number of rejected convert requests.

Cisco MediaSense Storage Management Agent Rejected RTSP Monitoring Requests

Displays the number of rejected RTSP monitoring requests.

Cisco MediaSense Storage Management Agent Rejected RTSP Playback Requests

Displays the number of rejected RTSP playback requests.

Cisco MediaSense Storage Management Agent Rejected Raw Download Requests

Displays the number of rejected raw download requests.

Performance Summary

Displays information about the service mean setup delay, service max setup delay, service mean query response time, and service max query response time.

Cisco MediaSense Call Control Service Mean Setup Delay

Displays the average delay (in milliseconds) between the initial receipt of the SIP Invite from Unified CM and the SIP response to the Unified CM rolling window time.

Cisco MediaSense Call Control Service Max Setup Delay

Displays the maximum delay (in milliseconds) between the initial receipt of the SIP Invite from Unified CM and the SIP response to the Unified CM rolling window time.

Cisco MediaSense API Service Mean Query Response Time

Displays the average query response time in the last hour.

Cisco MediaSense API Service Max Query Response Time

Displays the maximum query response time in the last hour.

Cisco Unified Contact Center Express

Cisco Prime Collaboration Assurance provides you the Cisco Unified Contact Center Express (Unified CCX) dashboards, which are system defined and available when you add Unified CCX. Cisco Prime Collaboration Assurance also allows you to create custom dashboards based on your monitoring needs. For details on the performance counters, see the [Unified Contact Center Express Operations Guide](#).

To view the dashboards, go to **Monitor > System View > Performance**, select Contact Center Express and cluster from the Cluster or Device drop-down list and then select the required dashboard from the Dashboard drop-down list. Information related to the selected dashboard is displayed in different dashlets, and each dashlet displays the Server details, Current Usage and Maximum value received in the last three minutes.

Prerequisites:

- Unified CCX must be managed in Cisco Prime Collaboration Assurance.
- Unified CCX must be reachable, for the data to be displayed on Contact Center Express dashboards in Cisco Prime Collaboration Assurance.

The following are the newly supported Unified CCX dashboards:

System Summary

Displays information about CPU usage, Virtual Memory usage, Common Partition Usage, and the Critical Services status. As a system administrator you can monitor the System Summary dashlets to analyze the slow response of the system.

CPU Usage

Displays the real time CPU usage and the maximum value in the past 3 minutes.

Limitation: You have to use other reports also to monitor the system at the per-process level to determine which process or processes are causing CPU issues.

Virtual Memory Usage

Displays the real-time Virtual Memory usage and the maximum value in the past 3 minutes.

Common Partition Usage

Displays the real-time Common Partition Usage and the maximum value in the past 3 minutes.

Services

Displays the name of the service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable).



Note If the service status is displayed as Unknown State, the system cannot determine the state of the service.

CPU and Memory

Displays information about CPU usage, virtual memory usage, memory usage, and processors for the server.

CPU Usage

Displays the total CPU that is consumed, and the maximum CPU that is consumed in the last 3 minutes.

Virtual Memory Usage

Displays the total virtual memory that is consumed, and the maximum virtual memory that is consumed in last 3 minutes.

Memory Usage

Displays the following information:

- % VM Used: Represents the percentage of system virtual memory utilization on the system. The value of the % VM Used counter is equal to the value that is derived from either of the following two equations:

$$\frac{(\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} + \text{Used Swap KBytes})}{(\text{Total KBytes} + \text{Total Swap KBytes})}$$

$$\frac{\text{Used VM KBytes}}{\text{Total VM KBytes}}$$

- Total: Represents the total amount of memory in the system in kilobytes.

Used

Represents the amount of system physical memory that is in use, in kilobytes, in the system. The value of the Used KBytes counter is equal to the value that is derived from the following equation:

$$\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes}$$

The Used KBytes value is different from the Linux Used value that is shown in top or free command output. The used value that is shown in Linux top or free command output is equal to $\text{Total KBytes} - \text{Free KBytes}$, and it also includes the sum of Buffers KBytes and Cached KBytes.

Free

Represents the total amount of memory that is available in the system, in kilobytes.

Shared

Represents the amount of shared memory in the system, in kilobytes.

Buffers

Represents the capacity of buffers in the system, in kilobytes.

Cached

Represents the amount of cached memory, in kilobytes.

Total Swap

Represents the total amount of swap space, in kilobytes, in the system.

Used Swap

Represents the amount of swap space, in kilobytes, that is in use on the system.

Free Swap

Represents the amount of free swap space, in kilobytes, that is available in the system.

Processors

Displays the following information:

- **Processor:** Instance of the processor. For example, a quad-core CPU has four processors: 0, 1, 2, and 3.
- **% CPU:** The processor's share of the elapsed CPU time excluding the idle time since last update, expressed as a percentage of CPU time.
- **User:** Displays the percentage of CPU utilization that the CPU spent executing at the user level (application).
- **Nice:** Displays the percentage of CPU utilization that the CPU spent executing at the user level with nice priority.
- **System:** Displays the percentage of CPU utilization that the CPU spent executing at the system level (kernel).
- **Idle:** Displays the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.
- **IRQ:** Displays the percentage of time that the processor spent executing the interrupt request, which is assigned to devices for interrupt, or sending a signal to the computer when it finished processing.
- **Soft IRQ:** Displays the percentage of time that the processor spent executing the software interrupt (softirq), which means that task switching is deferred until later to achieve better performance.
- **IO Wait:** Displays the percentage of time that the CPU or CPUs were idle, during which the system had an outstanding disk I/O request.

Disk Usage

Displays information about disk usage on the node. It has the following dashlets: Common Partition Usage, Swap Partition Usage, Spare Partition Usage, Shared Memory Partition Usage, Active Partition Usage, Boot Partition Usage.

Each of the dashlets displays the following information:

Used

Represents the percentage of disk space that is in use on this file system.

Max Past 3 min

Represents the percentage of disk space that is in use on this file system in the past 3 minutes.

Used Space

Represents the amount of disk space, in megabytes, that is in use on this file system.

Total Space

Represents the amount of total disk space, in megabytes, that is on this file system. The number in this counter may differ from other total size values for disk space that you may see on the system, because the value of the Total Mbytes counter is the sum of Used Mbytes performance counter and the Free value that is shown in the CLI (show status) output. The Total Mbytes value is less than this CLI output for Total, which includes the minfree percentage of reserved file system disk blocks. Keep a minfree reserved to ensure a sufficient amount of disk space for the file system to operate at high efficiency.

Process

Displays information about the processes that are running on the node.

Process

Name of the process.

PID

The task's unique process ID, which periodically wraps, although it never restarts at zero.

& CPU

The task's share of the elapsed CPU time since the last update and is expressed as a percentage of total CPU time.

Status

The task's process status:

- 0: Running
- 1: Sleeping
- 2: Uninterruptible disk sleep
- 3: Zombie
- 4: Traced or stopped (on a signal)
- 5: Paging
- 6: Unknown

Shared Memory

The amount of shared memory, in kilobytes, that a task is using. Other processes could potentially share the same memory.

Nice

The nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining whether to run the task.

VmRSS

The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes, including Code, Data, and Stack.

VmSize

The total amount of virtual memory, in kilobytes, that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

VmData

The virtual memory usage of the heap for the task in kilobytes.

Thread Count

The number of threads that are currently grouped with the task. The negative value -1 indicates that this counter is currently not available because thread statistics (including all performance counters in the Thread object as well as the Thread Count counter in the Process object) have been turned off because the system's total processes and threads have exceeded the default threshold value.

Datastack Size

The stack size for task memory status.

Page Fault Count

The number of major page faults that a task encountered that required the data to be loaded into memory.

Virtualized Voice Browser

Cisco Prime Collaboration Assurance provides you the Virtualized Voice Browser dashboards, which are system defined and available when you add Virtualized Voice Browser. Cisco Prime Collaboration Assurance also allows you to create custom dashboards based on your monitoring needs.

To view the dashboards, go to **Monitor > System View > Performance**, select Virtualized Voice Browser and device IP address/host name from the Cluster or Device drop-down list and then select the required dashboard from the Dashboard drop-down list. Information related to the selected dashboard is displayed in different dashlets, and each dashlet displays the Server details, Current Usage and Maximum value received in the last three minutes.

Prerequisites:

- Virtualized Voice Browser must be managed in Cisco Prime Collaboration Assurance.
- Virtualized Voice Browser must be reachable, for the data to be displayed on Virtualized Voice Browser dashboards in Cisco Prime Collaboration Assurance.

The following are the newly supported Virtualized Voice Browser dashboards:

System Summary

Displays information about CPU usage, Virtual Memory usage, Common Partition Usage, and the Critical Services status. As a system administrator you can monitor the System Summary dashlets to analyze the slow response of the system.

CPU Usage

Displays the real time CPU usage and the maximum value in the past 3 minutes.

Limitation: You have to use other reports also to monitor the system at the per-process level to determine which process or processes are causing CPU issues.

Virtual Memory Usage

Displays the real-time Virtual Memory usage and the maximum value in the past 3 minutes.

Common Partition Usage

Displays the real-time Common Partition Usage and the maximum value in the past 3 minutes.

Services

Displays the name of the service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable).



Note If the service status is displayed as Unknown State, the system cannot determine the state of the service.

CPU and Memory

Displays information about CPU usage, virtual memory usage, memory usage, and processors for the server.

CPU Usage

Displays the total CPU that is consumed, and the maximum CPU that is consumed in the last 3 minutes.

Virtual Memory Usage

Displays the total virtual memory that is consumed, and the maximum virtual memory that is consumed in last 3 minutes.

Memory Usage

Displays the following information:

- % VM Used: Represents the percentage of system virtual memory utilization on the system. The value of the % VM Used counter is equal to the value that is derived from either of the following two equations:

$$\frac{(\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} + \text{Used Swap KBytes})}{(\text{Total KBytes} + \text{Total Swap KBytes})}$$

$$\text{Used VM KBytes} / \text{Total VM KBytes}$$

- Total: Represents the total amount of memory in the system in kilobytes.

Used

Represents the amount of system physical memory that is in use, in kilobytes, in the system. The value of the Used KBytes counter is equal to the value that is derived from the following equation:

$$\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes}$$

The Used KBytes value is different from the Linux Used value that is shown in top or free command output. The used value that is shown in Linux top or free command output is equal to $\text{Total KBytes} - \text{Free KBytes}$, and it also includes the sum of Buffers KBytes and Cached KBytes.

Free

Represents the total amount of memory that is available in the system, in kilobytes.

Shared

Represents the amount of shared memory in the system, in kilobytes.

Buffers

Represents the capacity of buffers in the system, in kilobytes.

Cached

Represents the amount of cached memory, in kilobytes.

Total Swap

Represents the total amount of swap space, in kilobytes, in the system.

Used Swap

Represents the amount of swap space, in kilobytes, that is in use on the system.

Free Swap

Represents the amount of free swap space, in kilobytes, that is available in the system.

Processors

Displays the following information:

- **Processor:** Instance of the processor. For example, a quad-core CPU has four processors: 0, 1, 2, and 3.
- **% CPU:** The processor's share of the elapsed CPU time excluding the idle time since last update, expressed as a percentage of CPU time.
- **User:** Displays the percentage of CPU utilization that the CPU spent executing at the user level (application).
- **Nice:** Displays the percentage of CPU utilization that the CPU spent executing at the user level with nice priority.
- **System:** Displays the percentage of CPU utilization that the CPU spent executing at the system level (kernel).
- **Idle:** Displays the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.

- **IRQ:** Displays the percentage of time that the processor spent executing the interrupt request, which is assigned to devices for interrupt, or sending a signal to the computer when it finished processing.
- **Soft IRQ:** Displays the percentage of time that the processor spent executing the software interrupt (softirq), which means that task switching is deferred until later to achieve better performance.
- **IO Wait:** Displays the percentage of time that the CPU or CPUs were idle, during which the system had an outstanding disk I/O request.

Disk Usage

Displays information about disk usage on the node. It has the following dashlets: Common Partition Usage, Swap Partition Usage, Spare Partition Usage, Shared Memory Partition Usage, Active Partition Usage, Boot Partition Usage.

Each of the dashlets displays the following information:

Used

Represents the percentage of disk space that is in use on this file system.

Max Past 3 min

Represents the percentage of disk space that is in use on this file system in the past 3 minutes.

Used Space

Represents the amount of disk space, in megabytes, that is in use on this file system.

Total Space

Represents the amount of total disk space, in megabytes, that is on this file system. The number in this counter may differ from other total size values for disk space that you may see on the system, because the value of the Total Mbytes counter is the sum of Used Mbytes performance counter and the Free value that is shown in the CLI (show status) output. The Total Mbytes value is less than this CLI output for Total, which includes the minfree percentage of reserved file system disk blocks. Keep a minfree reserved to ensure a sufficient amount of disk space for the file system to operate at high efficiency.

Process

Displays information about the processes that are running on the node.

Process

Name of the process.

PID

The task's unique process ID, which periodically wraps, although it never restarts at zero.

& CPU

The task's share of the elapsed CPU time since the last update and is expressed as a percentage of total CPU time.

Status

The task's process status:

- 0: Running
- 1: Sleeping

- 2: Uninterruptible disk sleep
- 3: Zombie
- 4: Traced or stopped (on a signal)
- 5: Paging
- 6: Unknown

Shared Memory

The amount of shared memory, in kilobytes, that a task is using. Other processes could potentially share the same memory.

Nice

The nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining whether to run the task.

VmRSS

The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes, including Code, Data, and Stack.

VmSize

The total amount of virtual memory, in kilobytes, that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

VmData

The virtual memory usage of the heap for the task in kilobytes.

Thread Count

The number of threads that are currently grouped with the task. The negative value -1 indicates that this counter is currently not available because thread statistics (including all performance counters in the Thread object as well as the Thread Count counter in the Process object) have been turned off because the system's total processes and threads have exceeded the default threshold value.

Datastack Size

The stack size for task memory status.

Page Fault Count

The number of major page faults that a task encountered that required the data to be loaded into memory.

Performance Dashboards

Performance page displays system-defined dashboards based on the performance counters.

**Note**

- If both cluster name and host name are same in Unified Communications Manager, you must rename the cluster name and rediscover Unified Communications Manager in Cisco Prime Collaboration Assurance, to view performance dashboards for the selected cluster.
- If you have already created custom dashboard for performance counters, you must reconfigure the same in Cisco Prime Collaboration Assurance 12.1 for the following device types:

Device Type	Version
Finesse	10 or higher
Socialminer	10 or higher

To view the dashboards, select the product and cluster from the Cluster or Device drop-down list and then select the required dashboard from the Dashboard drop-down list.

Along with the system-defined dashboards for every cluster or device, you can also view trends for the device related metrics using the Trend dashboard. For more information on how to view trends, see [Trend Dashboard](#).

For Cisco Prime Collaboration Release 11.1 and later

Unified CM and Unity Connection

The following system-defined dashboards are available for Unified CM:

**Note**

For Unity Connection, you can see these dashlets only- System Summary, CPU and Memory, Disk Usage, Process, and Port Monitor.

System Summary

Displays information about CPU usage, Virtual Memory usage, Common Partition Usage, and the Critical Services status. As a system administrator you can monitor the System Summary dashlets to analyze the slow response of the system.

CPU Usage

Displays the real time CPU usage and the maximum value in the past 3 minutes.

Limitation: You have to use other reports also to monitor the system at the per-process level to determine which process or processes are causing CPU issues.

Virtual Memory Usage

Displays the real-time Virtual Memory usage and the maximum value in the past 3 minutes.

Common Partition Usage

Displays the real-time Common Partition Usage and the maximum value in the past 3 minutes.

Services

Displays the name of the service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable).



Note If the service status is displayed as Unknown State, the system cannot determine the state of the service.

Communications Manager Summary

Displays registered phones, calls in progress, and active gateway ports and channels.

Registered Phones

Displays the total number of phones that are registered and the delta of phones that are registered in the last minute. A negative value indicates that phones were unregistered; a positive value indicates new phones were registered.

Calls in Progress

Displays the total number of calls in progress and the delta calls in progress in the last minute. A negative value indicates that calls were completed or dropped; a positive value indicates new calls were established.

Active MGCP Ports and Channels

Displays the total number of active MGCP ports and channels and the delta of active MGCP ports and channels in the past minute. A negative value indicates that active MGCP ports and channels decreased; a positive value indicates that active MGCP ports and channels increased.

Call Activity

Call Activity

Displays the call activity on Cisco Unified Communications Manager, including calls completed, calls attempted, calls in progress, and logical partition total failures. This includes all servers in the cluster, if applicable.

Calls Completed

Displays the number of calls that were actually connected (when a voice path or video stream is established) through Cisco Unified Communications Manager. This number increases when the call terminates.

Calls Attempted

Displays the total number of calls attempted. An attempted call occurs any time when a phone goes off hook and back on hook, regardless of whether any digits dialed, or connected to a destination. The system considers few call attempts during feature operations like transfer and conference as calls attempted.

Calls in Progress

Displays the total number of calls in progress and the delta calls in progress in the past 1 minute. A negative value indicates that calls were completed or dropped; a positive value indicates that new calls were established.

Logical Partition Failures

Displays the total Logical Partition Failures. Also displays the delta of Logical Partition Failures in the past 1 minute.

Gateway Activity

Displays gateway activity on Cisco Unified Communications Manager, including active ports, ports in service, and calls completed. Gateway Activity includes all nodes in the cluster, if applicable.

MGCP FXS

- Ports in Service: Displays the number of FXS ports that are currently available for use in the system.
- Ports Active: Displays the number of FXS ports that are currently in use (active) on this Unified CM.
- Calls Completed: Displays the total number of successful calls that were made from all the FXS port instances on the MGCP FXS device.

MGCP FXO

- Ports in Service: Displays the number of FXO ports that are currently available for use in the system.
- Ports Active: Displays the number of FXO ports that are currently in use (active) on this Unified CM.
- Calls Completed: Displays the total number of successful calls that were made from all the FXO port instances on the MGCP FXO device.

MGCP T1

- Spans in Service: Displays the number of T1 CAS spans that are currently available for use.
- Channel Active: Displays the number of T1 CAS voice channels that are in an active call on this Unified CM.
- Calls Completed: Displays the total number of successful calls that were made from all the instances of MGCP T1 CAS device.

MGCP PRI

- Spans In Service: Displays the number of PRI spans that are currently available for use.
- Channel Active: This represents the number of PRI voice channels that are in an active call on this Unified CM.
- Calls Completed: Displays the total number of successful calls that were made from all the instances of MGCP PRI device.

Displays the trunk activity on Cisco Unified Communications Manager, including calls in progress and calls completed. This counter includes all nodes in the cluster, if applicable.

H323

Calls In Progress: Displays the total number of calls currently in progress on all the instances of Cisco H323 device.

Calls Completed: Displays the total number of successful calls made from all the instances of Cisco H323 device.

SIP Trunk

Calls In Progress: Displays the total number of calls that are currently in progress on all the instances of SIP device, including all active calls. When all calls that are in progress are connected, the number of calls in progress and the number of active calls are the same.

Calls Completed: Displays the total number of calls that were actually connected (a voice path was established) from all the instances of SIP device. This number increments when the call is terminated.

SDL Queue

Displays SDL queue information, including the number of signals in queue and number of processed signals.

Signals in SDL Queue

High: Indicates the number of high-priority signals in the Unified CM queue. High-priority signals include timeout events, internal Unified Communications Manager KeepAlives, certain gatekeeper events, and internal process creation, among other events. A large number of high-priority events will cause degraded performance on Unified CM, resulting in slow call connection or loss of dial tone. Use this counter in conjunction with the Queue Signals Processed High counter to determine the processing delay on Unified CM.

Normal: Indicates the number of normal-priority signals in the Unified CM queue. Normal priority signals include call processing functions, key presses, and on-hook and off-hook notifications, among other events. A large number of normal-priority events will cause degraded performance on Unified CM, sometimes resulting in delayed dial tone, slow call connection, or loss of dial tone. Use this counter in conjunction with the Queue Signals Processed Normal counter to determine the call processing delay on Unified CM. Remember that high-priority signals must complete before normal-priority signals begin to process, so check the high-priority counters as well to get an accurate picture of the potential delay.

Low: Indicates the number of low-priority signals in the Unified CM queue. Low-priority signals include station device registration (except the initial station registration request message), among other events. A large number of signals in this queue could result in delayed device registration.

Lowest: Indicates the number of lowest-priority signals in the Unified CM queue. Lowest priority signals include the initial station registration request message during device registration. A large number of signals in this queue could result in delayed device registration.

Processed SDL Signals

High: Indicates the number of high-priority signals that are processed by Unified CM for each 1-second interval. Use this counter in conjunction with the Queue Signals Present High counter to determine the processing delay on this queue.

Normal: Indicates the number of normal-priority signals that are processed by Unified CM for each 1-second interval. Use this counter in conjunction with the Queue Signals Present Normal counter to determine the processing delay on this queue. Remember that high-priority signals are processed before normal-priority signals.

Low: Indicates the number of low-priority signals that are processed by Unified CM for each 1-second interval. Use this counter in conjunction with the Queue Signals Present Low counter to determine the processing delay on this queue. The number of signals that are processed gives an indication of how much device registration activity is being processed in this time interval.

Lowest: Indicates the number of lowest-priority signals processed by Unified CM for each 1-second interval. Use this counter in conjunction with the Queue Signals Present Lowest counter to determine the processing delay on this queue. The number of signals that are processed gives an indication of how many devices began the Unified CM registration process in this time interval.

Cisco TFTP

Displays Cisco trivial file transfer protocol (TFTP) status on the Cisco Unified Communications Manager node, including total TFTP requests, total TFTP requests found, and total TFTP requests aborted.

TFTP Requests

This counter includes all nodes in the cluster, if applicable. This counter represents the total number of file requests (such as requests for XML configuration files, phone firmware files, and audio files) that the TFTP server handles. This counter represents the sum total of the following counters after the TFTP service has started: RequestsProcessed, RequestsNotFound, RequestsOverflow, RequestsAborted, RequestsInProgress.

CPU and Memory

Displays information about CPU usage, virtual memory usage, memory usage, and processors for the server.

CPU Usage

Displays the total CPU that is consumed, and the maximum CPU that is consumed in the last 3 minutes.

Virtual Memory Usage

Displays the total virtual memory that is consumed, and the maximum virtual memory that is consumed in last 3 minutes.

Memory Usage

Displays the following information:

- % VM Used: Represents the percentage of system virtual memory utilization on the system. The value of the % VM Used counter is equal to the value that is derived from either of the following two equations:

$$\frac{(\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} + \text{Used Swap KBytes})}{(\text{Total KBytes} + \text{Total Swap KBytes})}$$

$$\frac{\text{Used VM KBytes}}{\text{Total VM KBytes}}$$

- Total: Represents the total amount of memory in the system in kilobytes.

Used

Represents the amount of system physical memory that is in use, in kilobytes, in the system. The value of the Used KBytes counter is equal to the value that is derived from the following equation:

$$\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes}$$

The Used KBytes value is different from the Linux Used value that is shown in top or free command output. The used value that is shown in Linux top or free command output is equal to $\text{Total KBytes} - \text{Free KBytes}$, and it also includes the sum of Buffers KBytes and Cached KBytes.

Free

Represents the total amount of memory that is available in the system, in kilobytes.

Shared

Represents the amount of shared memory in the system, in kilobytes.

Buffers

Represents the capacity of buffers in the system, in kilobytes.

Cached

Represents the amount of cached memory, in kilobytes.

Total Swap

Represents the total amount of swap space, in kilobytes, in the system.

Used Swap

Represents the amount of swap space, in kilobytes, that is in use on the system.

Free Swap

Represents the amount of free swap space, in kilobytes, that is available in the system.

Processors

Displays the following information:

- **Processor:** Instance of the processor. For example, a quad-core CPU has four processors: 0, 1, 2, and 3.
- **% CPU:** The processor's share of the elapsed CPU time excluding the idle time since last update, expressed as a percentage of CPU time.
- **User:** Displays the percentage of CPU utilization that the CPU spent executing at the user level (application).
- **Nice:** Displays the percentage of CPU utilization that the CPU spent executing at the user level with nice priority.
- **System:** Displays the percentage of CPU utilization that the CPU spent executing at the system level (kernel).
- **Idle:** Displays the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.
- **IRQ:** Displays the percentage of time that the processor spent executing the interrupt request, which is assigned to devices for interrupt, or sending a signal to the computer when it finished processing.
- **Soft IRQ:** Displays the percentage of time that the processor spent executing the software interrupt (softirq), which means that task switching is deferred until later to achieve better performance.
- **IO Wait:** Displays the percentage of time that the CPU or CPUs were idle, during which the system had an outstanding disk I/O request.

Disk Usage

Displays information about disk usage on the node. It has the following dashlets: Common Partition Usage, Swap Partition Usage, Spare Partition Usage, Shared Memory Partition Usage, Active Partition Usage, Boot Partition Usage.

Each of the dashlets displays the following information:

Used

Represents the percentage of disk space that is in use on this file system.

Max Past 3 min

Represents the percentage of disk space that is in use on this file system in the past 3 minutes.

Used Space

Represents the amount of disk space, in megabytes, that is in use on this file system.

Total Space

Represents the amount of total disk space, in megabytes, that is on this file system. The number in this counter may differ from other total size values for disk space that you may see on the system, because the value of the Total Mbytes counter is the sum of Used Mbytes performance counter and the Free value that is shown in the CLI (show status) output. The Total Mbytes value is less than this CLI output for Total, which includes the minfree percentage of reserved file system disk blocks. Keep a minfree reserved to ensure a sufficient amount of disk space for the file system to operate at high efficiency.

CTI Manager

Displays information about the devices and applications that interfaces with the CTI Manager. Its displays the following information

Open Devices

The number of devices open by all applications that are connected to CTI Manager.

Open Lines

The number of lines open by all applications that are connected to CTI Manager.

CTI Connection

The number of applications that are connected to CTI Manager.

CM Links

The active Unified Communication Manager link to CTI Manager.

Heartbeat

Displays heartbeat information for the Cisco Unified Communications Manager and Cisco TFTP service.

CMs Heartbeat

Current Value represents the heartbeat of Unified CM. This is an incremental count that indicates that Unified CM is running. If the count does not increment, then Unified CM is down. Past 1 min displays the delta; a value of 0 indicates that Unified Communications Manager is down.

TFTP Heartbeat

Current Value represents the heartbeat of the TFTP server. This is an incremental count that indicates that the TFTP server is running. If the count does not increment, then the TFTP server is down. Past 1 min displays the delta; a value of 0 indicates the TFTP server is down.

SIP Activity

Displays SIP activity on Cisco Unified Communications Manager, including summary requests, summary responses, summary of failure responses in, summary of failure responses out, retry requests out, and retry responses out. SIP Activity includes all nodes in the cluster, if applicable.

Summary Requests

Displays the summation of total number of SIP request messages received by the SIP device, including retransmissions + the total number of SIP request messages sent out (originated and relayed) by the device. Where a particular message is sent more than once, for example as a retransmission or as a result forking, each transmission is counted separately.

Summary Responses

Displays the summation of total number of SIP response messages received by the SIP device, including retransmissions + the total number of SIP response messages sent (originated and relayed) by the SIP device, including retransmissions.

Summary Failure Responses In

Displays the summation of total number of 4xx class SIP responses received by the SIP device, including retransmissions. This class of responses indicates request failure by a SIP device that provides a client function + the total number of 5xx class SIP responses received by the SIP device, including retransmissions. This class of responses indicates failure responses received by a SIP device that provides a client function + the total number of 6xx class SIP responses received by the SIP device, including retransmissions. This class of responses indicates failure responses received by a SIP device that provides a client function. The responses generally indicate that a node has definitive information about a particular called party, not just the particular instance indicated in the Request-URI.

Summary Failure Responses Out

Displays the summation total number of 4xx class SIP responses sent by the SIP device, including retransmissions. This class of responses indicates request failure by a SIP device that provides a node function + the total number of 5xx class SIP responses sent by the SIP device, including retransmissions. This class of responses indicates failure responses sent by a SIP device that provides a node function + the total number of 6xx class SIP responses sent by the SIP device, including retransmissions. This class of responses indicates failure responses sent by a SIP device that provides a node function. The responses generally indicate that a node has definitive information about a particular called party, not just the particular instance indicated in the Request-URI.

Retry Requests Out

Displays the total number of Request retries that have been sent by the SIP device.

Retry Responses Out

Displays the summation of the total number of Final Response retries that have been sent by the SIP device + the total number of non-Final Response retries that have been sent by the SIP device.

Process

Displays information about the processes that are running on the node.

Process

Name of the process.

PID

The task's unique process ID, which periodically wraps, although it never restarts at zero.

& CPU

The task's share of the elapsed CPU time since the last update and is expressed as a percentage of total CPU time.

Status

The task's process status:

- 0: Running
- 1: Sleeping
- 2: Uninterruptible disk sleep
- 3: Zombie
- 4: Traced or stopped (on a signal)
- 5: Paging
- 6: Unknown

Shared Memory

The amount of shared memory, in kilobytes, that a task is using. Other processes could potentially share the same memory.

Nice

The nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining whether to run the task.

VmRSS

The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes, including Code, Data, and Stack.

VmSize

The total amount of virtual memory, in kilobytes, that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

VmData

The virtual memory usage of the heap for the task in kilobytes.

Thread Count

The number of threads that are currently grouped with the task. The negative value -1 indicates that this counter is currently not available because thread statistics (including all performance counters in the Thread object as well as the Thread Count counter in the Process object) have been turned off because the system's total processes and threads have exceeded the default threshold value.

Datastack Size

The stack size for task memory status.

Page Fault Count

The number of major page faults that a task encountered that required the data to be loaded into memory.

Database Summary

Provides connection information for the server, such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, the number of devices that are queued for a device reset, the number of replicates that have been created, and the status of the replication.

Change Notification Requests Queued in DB

Displays the number of records from the DBCNQueue table.

Change Notification Requests Queued in Memory

Displays the number of change notification requests that are queued in memory.

Total Number of Connection Clients

Displays the number of change notification requests that are queued in memory.

Replicates Created

Displays the number of replicates that were created by Informix for the DB tables. Every table contains at least one replicate. This counter displays information during Replication Setup.

Replication Status

Displays the state of replication:

- 0 = Initializing ReplTask thread
- 1 = Replication setup script fired from this node
- 2 = Replication is good; replication is set up correctly and most of the tables in the database should be in sync for all nodes of the cluster



Note Run the CLI command **utils dbreplication status** to see if any tables are out of sync

- 3 = Replication data transfer is bad in the cluster



Note When the counter shows a value of 3, replication is bad in the cluster. This value does not mean that replication is bad on that particular node. Run the CLI command **utils dbreplication status** find out where and what exactly is broken.

- 4 = Replication Setup did not succeed

Phone Summary

Displays information about the Cisco Unified Communications Manager node, including the number of registered phones, registered SIP phones, registered SCCP phones, partially registered phones, and the number of failed registration attempts. This includes all nodes in the cluster, if applicable.

Registered Devices

Displays the number of SIP phones, SCCP phones and total phones that are registered in Unified CM. The Past 1 Minute column displays the delta of phones that were registered or unregistered in the past 1 minute.

Registration Issues

Displays the registration issues of all the phones in Unified CM. The Failed Attempts tab displays the number of attempts that are failed to register phones; the Partial Registration tab displays the number of partial registrations of phones. The Past 1 Minute column displays the delta of values in the past 1 minute.

Device Summary

Displays information about the Unified CM node, including the number of registered phone devices, registered gateway devices, and registered media resource devices. Device Summary includes all nodes in the cluster, if applicable.

Registered Phones

Displays the total phones registered in Unified CM cluster; Past 1 Minute displays the delta of total registered phones in the past 1 minute.

Registered Gateways

Displays the total gateways (FXS, FXO, T1CAS and PRI) registered in Unified CM cluster; Past 1 Minute displays the delta of total registered gateways in the past 1 minute.

Registered Media Resources

Displays the total media resources (MOH, MTP, XCODE and CFB) that are registered in Unified CM cluster; Past 1 Minute displays the delta of total registered media resources in the past 1 minute.

Registered Other Station Devices

Displays the total other station devices registered in Unified CM cluster; Past 1 Minute displays the delta of total other station devices in the past 1 minute.

Registered Services

Displays the details of all different types of devices: Phones, Gateways, Media Resources, and Other Station devices. Details for each type are displayed separately.

IM and Presence Summary

PE Active JSM Conferences

The Number of Active JSM Conferences performance counter contains the number of client emulation conferences between the Cisco Presence Engine and Cisco XCP Router. The value of this counter should always equal the number of licensed users on the box.

Past 1 Minute displays the delta of counter value in the past 60 seconds.

Active Calendar Subscriptions

The Number of Active Calendar Subscriptions performance counter contains the number of calendar subscriptions that are currently active on the box.

Past 1 Minute displays the delta of counter value in the past 60 seconds.

Incoming SIP Subscriptions

The Number of Active Inbound SIP Subscriptions performance counter contains the current number of active inbound SIP subscriptions that are maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence Service node. Monitor this counter if the IM and Presence Service node is configured for SIP Interdomain Federation or SIP Intradomain Federation.

Past 1 Minute displays the delta of counter value in the past 60 seconds.

Outgoing SIP Subscriptions

The Number of Active Outbound SIP Subscriptions performance counter contains the current number of active outgoing SIP subscriptions being maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence Service node. Monitor this counter if IM and Presence Service node is configured for SIP Interdomain Federation or SIP Intradomain Federation.

The total combined count of SubscriptionsOut and SubscriptionsIn must not rise above 260,000 on any single IM and Presence Service node.

Past 1 Minute displays the delta of counter value in the past 60 seconds.

Total Ad Hoc Chat Rooms

The Total Ad Hoc Group Chat Rooms performance counter contains the total number of ad hoc chat rooms that are currently hosted on the node.



Note Ad hoc chat rooms are automatically destroyed when all users leave the room, so this counter rises and falls in value regularly.

Past 1 Minute displays the delta of counter value in the past 60 seconds.

Total Persistent Chat Rooms

The Total Persistent Chat Rooms performance counter contains the total number of persistent chat rooms that are hosted on the node. The room owner must explicitly destroy persistent chat rooms. This counter can be monitored to identify whether the total number of persistent chat rooms is very large and also to help identify whether some persistent chat rooms are not being used regularly anymore.

Past 1 Minute displays the delta of counter value in the past 60 seconds.

Cisco Jabber Summary

Jabber Login Failures

Represents the number of failed login requests that were received by the Cisco Simple Object Access Protocol (SOAP) interface. After 1 minute, the counter displays the delta of counter value in the last 60 seconds.

Current Connected Jabber or XMPP Clients

Contains the current number of XMPP clients that are connected to the Cisco XCP Connection Manager on an individual IM and Presence Service server. This number rises and falls based on the usage patterns of your deployment. Further investigation may be required if this number is higher than expected for your user base. After 1 minute, the counter displays the delta of counter value in the last 60 seconds.

IM Packets Since Last Restart

Provides the total number of IM packets that are handled by the IM and Presence Service node across all users. After 1 minute, the counter displays the delta of counter value in the last 60 seconds.

IM Packets in Last 60 Seconds

The total number of IM packets that are handled by the IM and Presence Service node across all users in the past 60 seconds. This counter is reset to zero every 60 seconds. The same rules for counting IM packets apply as for TotalMessagePackets. Monitor this counter to help identify the busy IM hours in your organization. After one minute, the counter displays the delta of counter value in the last 60 seconds.

Learned Patterns

Learned Pattern reports and Service Advertisement Framework (SAF) forwarder reports support the Call Control Discovery feature. When you configure the Call Control Discovery feature, Cisco Unified Communications Manager advertises itself and its hosted DN patterns to other remote call-control entities that use the SAF network. Likewise, these remote call-control entities advertise their hosted DN patterns, which Unified CM can learn and insert in digit analysis.

Column	Description
Pattern	Displays the name of the learned pattern from the remote call-control entity.
TimeStamp	Displays the date and time that the local Unified CM marked the pattern as a learned pattern.
Status	Indicates whether the learned pattern was reachable or unreachable.
Protocol	Displays the protocol for the SAF-enabled trunk that was used for the outgoing call to the learned pattern. If the remote call-control entity has QSIG tunneling configured for the SAF-enabled trunk, the data indicates that QSIG tunneling was used; for example, EMCA is listed along with H.323 in this column.
AgentID	Displays the name of the remote call-control entity that advertised the learned pattern.
IP Address	Displays the IP address for the call-control entity that advertised the learned pattern; Displays the port number that the call-control entity uses to listen for the call.
ToDID	Displays the PSTN failover configuration for the learned pattern.
CUCMNodeId	Displays the ID from the local Unified CM node.

Port Monitor

The Port Monitor lets you monitor the activity of each Cisco Unity Connection voice messaging port in real-time. This information can help you determine whether the system has too many or too few ports.

The Port Monitor displays the information for each port as described in the following table.

Field	Description
Port Name	The display name of the port in Cisco Unity Connection Administration.
Caller	For incoming calls, the phone number of the caller.
Called	For incoming calls, the phone number that was dialed.
Reason	If applicable, the reason why the call was redirected.
Redir	The extension that redirected the call. If the call was redirected by more than one extension, this field shows the extension prior to the last extension.
Last Redir	The last extension that redirected the call.
Application Status	The name of the conversation that Cisco Unity Connection is playing for the caller. When the port is not handling a call, the status appears as Idle.
Display Status	The action that the conversation is currently performing. When the port is not handling a call, the status appears as Idle.
Conversation Status	Specific details about the action that the conversation is performing. When the port is not handling a call, the status appears as Idle.
Port Ext	The extension of the port.
Connected To	For Cisco Unified Communications Manager SCCP integrations, the IP address and port of the Cisco Unified Communications Manager node to which the ports are registered.

View Historical Trends

Historical trending is enabled by default for the dashlets (CPU Usage, Virtual Memory Usage, and Common Partition Usage) under the System Summary dashboard. Click **Zoom** at the bottom-right corner of the dashlet to view the Trend View graph.

Prerequisites

All devices should be in managed state in Cisco Prime Collaboration Assurance. In case of clusters, all the nodes should be in managed state.

For voice devices (Cisco Unified CM, Cisco Packaged Contact Center Enterprise, Cisco Unified Presence, Cisco Unity Connection, Cisco Media Sense, Cisco Finesse, Cisco Unified IC, and Cisco Unified Contact

Center Express), along with the system-defined dashboards, you can also view trends for the device related metrics.

For Cisco Prime Collaboration Release 11.5 and later

For voice devices (Cisco Unified CM, Cisco Packaged Contact Center Enterprise, Cisco Unified Presence, Cisco Unity Connection, Cisco Media Sense, Cisco Finesse, Cisco Unified IC, Cisco Unified Contact Center Express, and Cisco Virtualized Voice Browser), along with the system-defined dashboards, you can also view trends for the device related metrics.



Note

- The device related metrics vary based on the device type you select.
- Historical trending is not supported for non-voice devices such as Cisco Unified CCE, Cisco Voice Portal, MCU/TPS, Cisco Unified Border Element, Cisco Voice Gateways, Cisco Unified Communications Manager Express, and ISDN Gateway.

Trend Dashboard

To view trends for metrics, select **Trend** from the Dashboard drop-down list and then from the Metrics Selection dialog box, select the metrics for which you want to enable trend, and click **Add**. You can select any number of metrics that you want, but we recommend that you select only a maximum of six metrics for every device type.

You can also perform the following:

- View data either as a chart or in a tabular format.
- Compare the trends for two or more performance metrics by clicking the **Merge** option.
- Click **Zoom** to view the trend graph in a detailed view. This option also helps you view the history, hourly average, maximum, and minimum data. Using the zoom selector graph displayed in the detailed view, you can adjust the pointer in the time window (x axis) of the graph to view the trend for the selected time period.
- Add more trends using the Add Graph (+) button at the top-right corner of the user interface.
- Change the chart type.

Create Custom Performance Dashboards

For Cisco Prime Collaboration Release 11.5 and later

You can add customized dashboards in the home page (**Network Health Overview > Performance**); either in the graphical view (limited to 6 counters) or tabular view (up to 50 counters). By default, the graphical view is enabled. The Min., Max., and Avg. values for the counters are also displayed.



Note All the custom dashboard metadata are stored in the database. However, the counter values are obtained live from the devices and are saved in the cache memory. If a performance dashboard is not open for more than 30 minutes, the polling stops and the cache memory is cleared until the next time the custom dashboard is launched. If the historical trend is enabled for custom dashboard counter(s), the polled data is stored in the database for seven days. For information on the purge policies, see [Cisco Prime Collaboration Assurance Guide- Advanced](#).

In graphical view, the graph depicts the current values of a counter for every few seconds or minutes, as specified in the polling interval. You can also mouse over the various red points in the line to view the value of the counter as a tool tip.



Note Click **See Average** to view the Min., Max., and Avg. values for the counter in the graphical view.

You can also:

- Add events to the custom dashboard.
- Switch between the graphical and tabular views.



Note When you create customized dashboards in the graphical view or when you switch from tabular view to graphical view using the edit option, ensure that the number of counters you select is less than or equal to 6. If the number of counters is more than 6, you need to remove the excess counters to view the dashboard in the graphical view.

To create custom dashboards:

- Step 1** Choose the product and the cluster from the Cluster or Device drop-down list.
- Step 2** Click the + button adjacent to the Dashboard drop-down list.
- Step 3** On the Custom Dashboard page, enter the dashboardname (**//dashboardname//**), select the polling interval, view, and server.

You can collect historical data for custom graph from the Custom Performance Dashboard.

For Cisco Prime Collaboration Release 11.6 and earlier

Note When two different login users create custom dashboards using the same dashboard name, cluster and counter details or with different dashboard name with same cluster and counter group details, the application displays incorrect dashboard details for the respective users.

For Cisco Prime Collaboration Release 12.1 and later

Note The custom dashboard name is changed from **Custom-//dashboardname//** to **Custom-//dashboardname_loggedInUser//** so that different users can view their respective dashboard details with correct data though the dashboard name, cluster name, and counter group details remains the same.

You can enable the historical trend for the performance counters that you select, while creating custom dashboards in the graphical view. This option is disabled when you create custom dashboards in tabular view or switch from graphical to tabular view. A warning message appears stating that the historical trend data is lost, when you switch from graphical to tabular view.

- Note**
- For the Historical Trend option to be enabled, the polling interval must be greater than or equal to 60 seconds.
 - The polling interval must be greater than or equal to 30 seconds, if you have a mega-cluster with more than 10 communications manager nodes configured.

Step 4 Select the desired performance counters from the Select Performance Counters pane. Expand the counter group and select the counter. The instances corresponding to the counter is displayed in the Select Instances pane.

Step 5 Select the instances of your choice and click **Add**.

- Note** You can also perform a search that is case sensitive, for a counter group, counter, or instance using the search option available in the Select Performance Counters or Select Instances pane.

Step 6 Click **Create**.

You can also edit or delete a custom dashboard you created, using the **Edit** and **Delete** buttons. For information about creating a new performance counter event, see . When you create custom events from the custom dashboards, you need not provide the cluster details.

- Note** Only the dashboard name appears on the Edit or Delete Custom Dashboard dialog box.

Click the **Zoom** link at the bottom-right of the dashlet, to view the Trend View graph for the performance counter. You can export the historical trend data in either CSV or PDF format using the Export option available in the Trend View graph.

You can also click **Merge** to view the Merge View graph for one or more dashlets that you have created. The collected trend data is stored for seven days, and then purged.

- Note** The Zoom and Merge options are available only if you have enabled the historical trend option for that custom dashboard.

Add a Customized Dashboard

You can add customized dashboards in the home page.

You can also do the following:

- Add the existing dashlets to a different dashboard.
- Move the dashlets around under a dashboard by dragging and dropping them.

To add a new dashboard:

Step 1 Click the “Settings” icon on the top-right corner of the home page, and then click **Add New Dashboard**.

Step 2 Enter a name in the box provided, and click **Apply**.

Step 3 Click **Add Dashlet(s)**.

Step 4 Click **Add** adjacent to the dashlets you want to add.



CHAPTER 24

Cisco Prime Collaboration Assurance Reports

This section explains the following:

- [Cisco Prime Collaboration Assurance Reports, on page 377](#)
- [Prerequisites to Generate the Cisco Prime Collaboration Assurance Reports, on page 377](#)
- [Update Call Detail Records NAM Credentials, on page 378](#)
- [Call Classification, on page 383](#)
- [Configure SFTP Settings, on page 393](#)
- [Administrative Reports, on page 396](#)
- [CDR & CMR Call Report, on page 397](#)
- [NAM & Sensor Report, on page 408](#)
- [Session Reports/Conference Reports, on page 416](#)
- [TelePresence Endpoint Reports, on page 418](#)
- [Launch CUCM Reports, on page 419](#)
- [Miscellaneous Reports, on page 419](#)
- [Scheduled Reports, on page 424](#)
- [Access Data for Reports that Contain More than 2,000 Records, on page 427](#)
- [Troubleshoot File Download Issues, on page 427](#)

Cisco Prime Collaboration Assurance Reports

This chapter provides information on various reports in Cisco Prime Collaboration Assurance Reports.

Prerequisites to Generate the Cisco Prime Collaboration Assurance Reports

You can use the Cisco Prime Collaboration Assurance reports to identify problem areas, locate most commonly used and least used endpoints, and determine ideal locations and required endpoint types for future deployment.

Prerequisites:

- Update data source credentials. See [Update Call Detail Records NAM Credentials](#).
- (For voice call reports) Categorize calls, add Dial Plan, configure Gateway Codes. See [Call Classification](#).

- Configure SFTP. See [Configure SFTP Settings](#).
- Unified CM devices must be in managed state.
- Cisco Prime Collaboration Assurance must be added as billing server in Unified CM.

Update Call Detail Records NAM Credentials

Cisco Prime Collaboration Assurance collects SCS (number of seconds where loss is greater than 5%) from Cisco Unified CM clusters or Cisco Prime Virtual Network Analysis Module (Prime vNAM). It sends SNMP traps when the voice quality of a call fails to meet a user-defined quality threshold.

Cisco Unified CM calculates the MOS value for an entire call using the Cisco Voice Transmission Quality (CVTQ) algorithm. At the termination of a call, Cisco Unified CM stores the data in Call Detail Records (CDRs) and Call Management Records (CMRs) (for more information on CDR and CMR, see the [Cisco Unified Communications Manager Call Detail Records Administration Guide](#)).

To provide the credentials for Unified Communications Manager publisher servers, you must:

- Provide Cisco Prime Collaboration Assurance with credentials.
- Keep the credentials up-to-date. (Any time you update credentials on a Unified Communications Manager publisher server, you must also update the corresponding credentials in Cisco Prime Collaboration Assurance.)

To update the credentials, choose **CDR Source Settings > Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 11.5 and later

To update the credentials, choose **Alarm & Report Administration > CDR Source Settings > Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

To update the credentials, choose **Inventory > Inventory Management > Configure NAM**.

Add Credential for Prime NAM

To add a credential for Prime NAM server:

-
- Step 1** Choose **Assurance Administration > CDR Source Settings > Manage Call Quality Data Sources**.
- For Cisco Prime Collaboration Release 11.5 and later**
- Choose **Alarm & Report Administration > CDR Source Settings > Manage Call Quality Data Sources**.
- For Cisco Prime Collaboration Release 12.1 SP3 and later**
- Choose **Inventory > Inventory Management > Configure NAM**.
- Step 2** Click **Add**, and enter the required data. Here, every field is mandatory.
- Step 3** Click **OK**.
- For Cisco Prime Collaboration Release 12.1 SP3 and later**

Click **Save**.

Note You can enter either the Hostname or the IP Address in the specified format. Make sure the Hostname is resolvable with the IP address. If it is not resolvable, an error message pops up. The Configure NAM wizard also displays the **Status** of the NAM configurations along with the **Status Reasons**. The various statuses are Success, Verifying, and Failure.

Step 4 Click the **Refresh** button for the credential details to reflect on the user interface.

To edit or delete a credential, check the checkbox of the credential of your choice, and then click **Edit** or **Delete**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Click **Refresh** icon to view the latest NAM credential status.

To edit a credential, check the checkbox of the credential of your choice, and then make the required changes.

Note **Selected count/<total number of rows>** - Displays the number of rows selected by the total number of rows in the table.

Delete Credentials for Multiple Prime NAMs

Step 1 Choose **Inventory > Inventory Management > Configure NAM**.

Step 2 Check the checkbox of the credential of your choice.

Step 3 Click **Delete**.

A message pops up indicating that Are you sure you want to delete the selected NAM(s)?

Note If an error occurs, while deleting NAM(s), check the logs.

Verify Credentials for Multiple Prime NAMs

Step 1 Choose **Inventory > Inventory Management > Configure NAM**.

Step 2 Select the NAM for which you want to verify credentials.

Step 3 Click **Verify**.

Note While the NAM is in “Verifying” state, you can either Verify or Delete a NAM. If you try to verify or delete a NAM, a message appears indicating that NAM Credential(s) cannot be deleted or verified while NAM is in “Verifying” state.

Add Multiple NAM Credentials

You can add multiple NAM credentials, by importing a csv file with Prime NAMs details.

CSV (Comma Separated Values) format is the most common import and export format for spreadsheets and databases.

Preparing the CSV File

The CSV file is based on a default Microsoft Excel-styled CSV file. A CSV file contains a number of rows, each containing a number of columns. Fields are separated by commas and any content that must be treated literally, such as commas and new lines/'carriage returns' themselves are enclosed in quotes.

CSV File Requirements

In addition to being 'well-formed', CSV files have the following requirements.

Each CSV file must possess a heading row.

The CSV file import uses a CSV file's header row to determine how to map data from the CSV file's 2nd row and beyond to fields in the database.

The header row should avoid containing any punctuation (apart from the commas separating each column) or the importer may not work correctly.

CSV supports two types of header file formats: 6 header and 7 header.

- In 12.1 and earlier, it was a 7 header format because HostName and IP Address were two different fields.
- In 12.1 Service Pack 3, it is a 6 header format because it supports both HostName and IP Address in a single field.

The CSV file must contain the following details for each Prime NAM Server:

CSV 6 header file format with HostName

DisplayName	HostName	Protocol	Port	UserName	Password
nam	nam.atlas.local	HTTP	80	admin	Atlas!123

CSV 6 header file format with IPAddress

DisplayName	IPAddress	Protocol	Port	UserName	Password
NAM	10.104.243.11	HTTP	80	admin1	Nam!123

From 12.1 Service Pack 3 and later, it is recommended to use a 6 header file format only for NAM import. If there is an import file prepared in 11.6 and earlier, the same header file can be reused in 12.1 Service Pack 3 and later releases.



Note

- Ensure that the rows are not left blank and each record is one line.
- Leading and trailing whitespace is ignored.
- Embedded line-breaks.
- Hostname must be resolvable to IP address.

Import Credentials for Prime NAMs

-
- Step 1** Choose **Inventory** > **Inventory Management** > **Configure NAM**.
- Step 2** In the **Import NAM** section, click **Choose File** button to browse to the local csv file, and click **Import** to import the NAM in CSV format.
- Step 3** Click **Import**.
- Step 4** Click **Refresh** icon to view the latest NAM credential status".
- Step 5** Click **Save**.
-

Credential Verification - Error Messages

Various credential verification error messages are tabulated below. These messages are introduced as part of NAM Import.

Success/Error Message	Condition	Possible Solutions
IMPORT_PROCESS_SUCCESS_MESSAGE	All the NAM records are successfully imported.	Success message
IMPORT_PROCESS_SKIPPED_FEW_RECORDS	Failed for one of the following reasons:	
	1. "All the NAM records are not successfully imported. Could not resolve the Hostname for record. Please check the import file. If the problem persists, check the logs."	
	2. "All the NAM records are not successfully imported. Could not resolve the IP Address for record. Please check the import file. If the problem persists, check the logs."	
	3. "All the NAM records are not successfully imported. Could not resolve the Hostname or IP Address for record. Please check the import file. If the problem persists, check the logs."	
IMPORT_PROCESS_FAILURE	"All the NAM records are not successfully imported. Please check the import file. If the problem persists, check the logs."	Check for duplicates and enter correct data, for example, IP Address.

Success/Error Message	Condition	Possible Solutions
INCORRECT_FILE_FORMAT	“Imported file format is incorrect. Please check the user guide for the exact format and import the file in CSV format only.”	Import the file in CSV format only.
IMPORT_FILE_HEADERS_EMPTY	“File headers are incorrect. Please check the user guide for the exact format.”	Choose a file with correct header.
IMPORT_FILE_CONTENT_EMPTY	“Imported file contents are empty or not proper. Please check the user guide for the exact format.”	Enter NAM data.

Use NAM Credentials to Troubleshoot Problems and Verify Credentials

Any problem that prevents Cisco Prime Collaboration Assurance from contacting and connecting to NAM can interrupt the collection and analysis of call data and configuration data. You can perform the following:

- Verify that credentials are valid and that Cisco Prime Collaboration Assurance is actively obtaining data.
- Troubleshoot if you notice potential problems with NAM credential status or with reports (such as an unusual time gap).

Step 1 Perform the following troubleshooting:

For a Cisco Unified CM—Do the following:

- Verify that credentials for the cluster on Cisco Unified CM match those in Cisco Prime Collaboration Assurance, and correct, if necessary.
- Verify that DNS parameters are specified correctly on the Cisco Prime Collaboration Assurance server and the Cisco Unified CM hostname has been added to DNS. (Cisco Prime Collaboration Assurance must be able to resolve the IP address for Cisco Unified CM to obtain the correct name.)
- Check whether any known problems exist that prevent successful data exchange between a cluster and Cisco Prime Collaboration Assurance.
- This can happen after the connection between Cisco Prime Collaboration Assurance and Cisco Unified CM is reestablished after a break. Cisco Unified CM first sends old files to Cisco Prime Collaboration Assurance.
- Credentials that Cisco Prime Collaboration Assurance relies upon might change on a Cisco Unified CM platform. If this happens, check with your Unified CM administrator to obtain the correct credentials. If necessary, update the credentials in Cisco Prime Collaboration Assurance.

Step 2 Verify the credentials:

- Choose **Assurance Administration > CDR Source Settings > Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration > CDR Source Settings > Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Choose **Inventory > Inventory Management > Configure NAM**.

- b) Select the NAM for which you want to verify credentials.
- c) Click **Verify**.

Call Classification

Cisco Prime Collaboration Assurance uses call classification to categorize calls in Call Detail Record (CDR) reports.

Cisco Prime Collaboration Assurance determines whether a call fits in system-defined call categories by analyzing the following data:

- Details from CDRs
- Device types of the source and target endpoints
- Direction of the call (incoming or outgoing)
- Protocol (H.323, MGCP, or SIP)



Note CDR reports older than seven days are purged.

The following table lists system-defined call category types and names, and describes the calls included in the category type.

Category Type	Description	Category Name
Voicemail	Calls to or from voicemail.	Unity Voicemail—Calls that meet system-defined criteria for a voicemail call, such as calls to and from Cisco Unity and Cisco Unity Connection. Note You can add user-defined category names to this category type.
Conference	Calls to or from a conferencing system.	Conference Bridge—Calls that meet system-defined criteria for a call involving a conference bridge. Note You can add user-defined category names to this category type.

ICT	Calls to or from an intercluster trunk (ICT).	<ul style="list-style-type: none"> • ICT GK Controlled—ICT calls that are gatekeeper controlled. • ICT Non-GK Controlled—ICT calls that are not gatekeeper controlled.
VG/Trunk-Outgoing	<p>Calls to a voice gateway or a trunk; only OffNet calls are included.</p> <p>Note User-defined dial plans are applied to calls in the VG/Trunk-Outgoing call category.</p>	<ul style="list-style-type: none"> • MGCP Gateway Outgoing—Calls to an MGCP voice gateway. • H.323 Gateway Outgoing—Calls to an H.323 voice gateway. • H.323 Trunk Outgoing—Calls to an H.323 trunk. SIP Trunk Outgoing—Calls to a SIP trunk.
VG/Trunk-Incoming	Includes calls from a voice gateway or a trunk; only OffNet calls are included.	<ul style="list-style-type: none"> • MGCP Gateway Incoming—Calls from an MGCP voice gateway. • H.323 Gateway Incoming—Calls from an H.323 voice gateway. • H.323 Trunk Incoming—Calls from an H.323 trunk. SIP Trunk Incoming—Calls from a SIP trunk.
Tandem	A tandem call occurs when both endpoints are voice gateways or trunks.	Tandem.
OnNet Trunk	<p>Calls where one endpoint is a trunk and the call is not an OffNet call.</p> <p>For example, the trunk could be used to connect to WebEx or to a PBX.</p>	<ul style="list-style-type: none"> • OnNet H.323 Trunk. • OnNet SIP Trunk.
Internal	Calls that do not fall into any of the above categories. For example, calls where one endpoint is an IP phone and the other endpoint is a voice gateway and the call is not an OffNet call.	Internal.

Unknown	For system-related reasons, Prime Collaboration could not determine the device type of the endpoints.	Unknown.
---------	---	----------

Cisco Prime Collaboration Assurance places a call in the user-defined call category if:

- The call has already been categorized as an Internal, VG/Trunk-Outgoing, or OnNet Trunk call.
- A user-defined dial plan is assigned to the cluster in which the call occurred.

Understand OffNet and OnNet Calls

A call is considered to be OffNet when at least one endpoint is a gateway or a trunk and when any of the following is also true of the endpoint:

- The Call Classification parameter is set to Offnet in the gateway configuration—or the trunk configuration—in Unified CM (Administration).
- In Unified CM, both of the following are true:
 - Call Classification parameter is set to System Default in the gateway or trunk configuration.
 - System Default service parameter is set to Offnet.
- The endpoint is an analog gateway.

Any call that does not meet the criteria for an OffNet call is considered to be an OnNet call.

Call Category Creation

You can create a call category when you add a dial pattern to a dial plan.

To add a call category, choose **CDR Analysis Settings > Set Call Category**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration > CDR Analysis Settings > Set Call Category**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

To add a call category, choose **Alarm & Report Administration > CDR Analysis Settings > Set Call Category**.

Cisco Prime Collaboration Assurance supports a few predefined set of call categories that determine how they are used within Cisco Prime Collaboration Assurance.

The following is a set of predefined call categories: Unity Voicemail, Local, Long Distance, International, Emergency, Service, and Toll Free.

Create Custom Call Category

Cisco Prime Collaboration Assurance also allows you to create custom call category.

Step 1 Click **Alarm & Report Administration > CDR Analysis Settings > Set Call Category**.

Step 2 Click **Add** button to create a custom call category. A new row is displayed at the end of the table.

Step 3 Choose **Call Category Type** from the drop-down.

Step 4 Click **Save**.

You can create a new call category, select the checkbox to modify the existing call category, or select multiple checkbox(s) to **Delete** the call category.

Dial Plan Addition

A dial plan must have a unique name, can include a set of toll-free numbers, and must include a set of dial patterns. A dial pattern identifies a call category name and type and specifies the rule or pattern that a directory number must match for the call to be included in the category.

Cisco Prime Collaboration Assurance provides a default dial plan as a starting point from which you can define your own dial plans. The default dial plan includes default dial patterns: call category names, types, and rules. As you configure a dial plan, you can add, modify, and delete the rules that are specified in the default dial plan.

You can create multiple dial plans. You can assign only one dial plan to each cluster, but you can assign the same dial plan to multiple clusters.

For Cisco Prime Collaboration Release 11.5 and earlier

To add a dial plan, choose .

For Cisco Prime Collaboration Release 11.5 and later

To add a dial plan, choose **Alarm & Report Administration > CDR Analysis Settings > Dial Plan Configuration**.

To assign a dial plan, choose **Alarm & Report Administration > CDR Analysis Settings > Dial Plan Assignment**.

Understand the Default Dial Plan

When you add a dial plan, a copy of the default dial plan is displayed for you to update. You can:

- Select from the existing Call Category names.
- Add, update, or delete dial patterns

For Cisco Prime Collaboration Release 12.1 SP3 and later

- Select from the existing Call Category names.
- Add, update, or delete dial patterns

Changes that you make while configuring a dial plan have no effect on the default dial plan, which is based on the North American Numbering Plan (NANP).

The following table provides the default dial plan values.

Condition	No. of Chars	Default Pattern	Call Category Name	Call Category Type	Explanation	Priority

>	3	011!	International	International	If the number of digits dialed is greater than 3 and starts with 011, the call is classified as International.	1
=	7	!	Local	Local	If the number of digits dialed is equal to 7 and the pattern is ! (more than one digit; in this case, 7 digits), the call is classified as Local.	2
=	10	T!	Toll Free	Toll Free	If the number of digits dialed is equal to 10 and the pattern is T! (more than one digit; in this case, a 10-digit number that starts with a toll-free number that is defined in the dial plan), the call is classified as Toll Free.	3

=	10	G!	Local	Local	If the number of digits dialed is equal to 10 and the pattern is G! (more than one digit; in this case, a 10-digit number that starts with a gateway code that has been defined in Cisco Prime Collaboration Assurance), the call is classified as Local.	4
=	10	!	Long Distance	Long Distance	If the number of digits dialed is equal to 10 and the pattern is ! (more than one digit; in this case, a 10-digit number), the call is classified as Long Distance.	5

=	11	T!	Toll Free	Toll Free	If the number of digits dialed is equal to 11 and the pattern is T! (more than one digit; in this case, an 11-digit number that starts with a toll-free number that is defined in the dial plan), the call is classified as Toll Free.	6
=	11	XG!	Local	Local	If the number of digits dialed is equal to 11 and the pattern is XG! (more than one digit; in this case, an 11-digit number that starts with any single digit followed by a gateway code that has been defined in Cisco Prime Collaboration Assurance), the call is classified as Local.	7

=	11	!	Long Distance	Long Distance	If the number of digits dialed is equal to 11 and the pattern is ! (more than one digit; in this case, an 11-digit number), the call is classified as Long Distance.	8
---	----	---	---------------	---------------	--	---



Note Cisco Prime Collaboration Assurance classifies the call as Toll Free if the toll-free code is defined in the dial plan that is assigned to the cluster.

Add a Dial Plan

You can add a dial plan .

For Cisco Prime Collaboration Release 11.5 and earlier

Step 1 Choose **CDR Analysis Settings > Dial Plan Configuration**. Click **Add**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration > CDR Analysis Settings > Dial Plan Configuration**. Click **Add**.

The **Add Dial Pattern** dialog box is displayed.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Choose **Alarm & Report Administration > CDR Analysis Settings > Dial Plan Configuration**.

Enter a name to add a new dial plan in **Dial Plan Name** field.

Click + (Add) at the end of the table to add a dial pattern.

A new row is created.

Step 2 Create a dial pattern by supplying data in these fields:

- **Condition** - Applies to the number of characters. Select one:
 - Left Arrow (<) - Less than
 - Right Arrow (>) - Greater than
 - Equals symbol (=) - Equal to

- **Number of Chars** - Enter the total number of digits and non-numeric characters, including plus (+), pound (#), asterisk (*), comma (,), and the at symbol (@). Expresses the number of characters in the directory number to which the dial pattern applies.
- **Pattern** - Enter the pattern to apply to the digits, where:
 - G indicates that the digits identify a gateway code.
 - T indicates that Cisco Prime Collaboration Assurance should compare the digits with the toll-free numbers configured in the dial plan.
 - ! signifies multiple digits (any number that is more than 1 digit in length, such as 1234 or 5551234).
 - X signifies a single-digit number (such as 0, 1, or 9).
- **For Cisco Prime Collaboration Release 12.1 SP2 and earlier**
Call Category Name - Select one of the following radio buttons and supply data as required:
 - **Existing** - Select an existing call category name.
 - **New** - Enter a unique name and select a call category type.
- **For Cisco Prime Collaboration Release 12.1 SP3 and later**
Call Category Name - Select an existing call category name from the drop-down list that are configured using the “Set Call Category” user interface.

Step 3 Click **OK**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Click **Save**.

The row is added to the table.

Apply Dial Patterns to VG/Trunk-Outgoing, Internal, and OnNet Trunk Calls

The following table shows how dial patterns are applied from a user-defined dial plan to a call in the Internal, VG/Trunk-Outgoing, or OnNet Trunk call category.

Cisco Prime Collaboration Applies Dial Patterns of This Category Type...	To the Directory Number that is the...	In a Call That Is in This System-Defined Category...
<ul style="list-style-type: none"> • Conference • Emergency • International • Local • Long Distance • Service • Toll Free • Voicemail 	Destination	VG/Trunk-Outgoing
<ul style="list-style-type: none"> • Conference • Voicemail 	Source	
<ul style="list-style-type: none"> • Conference • Voicemail 	<ul style="list-style-type: none"> • Source • Destination 	<ul style="list-style-type: none"> • Internal • OnNet Trunk

Edit a Dial Plan

You can edit a dial plan. While editing a dial plan, you can add, edit, or delete dial patterns.

-
- Step 1** Choose **Alarm & Report Administration > CDR Analysis Settings > Dial Plan Configuration**.
- Step 2** Click the icon (Edit) to modify a dial pattern.
- Step 3** Make the required changes.
- Step 4** Follow **Step 3** from “Add a Dial Plan” to modify the existing dial pattern.
- Step 5** Click the icon (Save). The row is updated to the table.
-

Delete a Dial Plan

You can remove a dial plan.

-
- Step 1** Choose the respective row and click the **Delete** button to remove the dial plan.
- Step 2** Click **Save** to keep all the changes on the dashlet.
- Click **Cancel** to exit.
-

Configure Gateway Codes

Cisco Prime Collaboration Assurance uses the gateway codes that you configure to determine the call classification for an external call.



Note To view the gateways for which gateway codes are already configured, select clusters and click **View**. The Gateway Code report displays only Media Gateway Control Protocol (MGCP), and H323 gateways. The analog Signaling Connection Control Part (SCCP) gateway is not displayed.

To configure gateway codes:

- Step 1** Choose **Assurance Administration > CDR Analysis Settings > Gateway Code Configuration**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Alarm & Report Administration > CDR Analysis Settings > Gateway Code Configuration**.
- Step 2** On the Gateway Code Summary page, select a cluster and click **Manage Gateway Code**.
- Step 3** Enter the gateway code, and then click **Apply**.

Configure SFTP Settings

If you are using Unified Communications Manager to monitor calls, you must configure SFTP settings.

To configure SFTP settings:

- Step 1** Choose **Assurance Administration > CDR Source Settings > CUCM SFTP Credentials**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Alarm & Report Administration > CDR Source Settings > CUCM SFTP Credentials**.
For Cisco Prime Collaboration Release 12.1 and later
Choose **Inventory > Inventory Management > CUCM/SFTP Credentials**.
For Cisco Prime Collaboration Release 12.1 SP3 and later
Choose **Inventory > Inventory Management**. Click on **CUCM SFTP Credentials** tab.
- Step 2** Enter the required information. For field descriptions, see the table for [SFTP Settings Page - Field Descriptions](#).
- Step 3** Click **Save**.
- A popup message window is displayed to confirm whether you want to update the SFTP credentials across all the managed Unified Communications Manager publishers.
- Note** Cisco Prime Collaboration Assurance is added as a billing server in the managed Unified Communications Manager publishers.

Step 4 Click Yes.

SFTP Settings Page - Field Descriptions

For Cisco Prime Collaboration Release 12.1 SP3 and later

The following table describes the fields in the SFTP Settings page.

Table 65: SFTP Settings Page - Field Descriptions

Fields	Description
Username	<p>You cannot change the username from smuser.</p> <p>This same username, smuser, must be configured in Cisco Unified Communications Manager.</p>
Password	<p>During fresh installation, ensure that the CUCM SFTP Credential is not set by default. You must set the CUCM SFTP password in Inventory Management -> CUCM SFTP Credentials tab.</p> <p>If credentials is not set, user will not be allowed to add PCA as a CDR Destination in CUCM during device discovery. The application must alert the user to set the CUCM SFTP password stating, "Please configure CUCM SFTP credentials to enable this feature. It can be configured under CUCM SFTP Credentials Tab".</p> <p>Note If you want to add PCA as a CDR destination in CUCM, while initiating device discovery, select the "Add the Prime Collaboration server as a CDR Destination in the Unified CM servers" check box in Discover Devices -> Device Discovery tab under Auto-Configuration option. For more information, see the section on "Discovery Methods".</p> <p>For Cisco Prime Collaboration Release 12.1 SP3 and earlier</p> <p>The default password is smuser. If you change the password here, you must also change the password for smuser in Cisco Unified Communications Manager.</p>
Re-enter Password	Enter Password to confirm.

For Cisco Prime Collaboration Release 12.1 SP3 and earlier

The following table describes the fields in the SFTP Settings page.

Table 66: SFTP Settings Page - Field Descriptions

Fields	Description
Low-Volume Schedule Hours	
<day> <timerange>	For each day of the week, timerange indicates the hours during which Cisco Prime Collaboration Assurance processes fewer records. During the low-volume schedule, Cisco Prime Collaboration Assurance performs database maintenance.
Miscellaneous	
Wait for Diagnostic Report (min)	Number of minutes that Cisco Prime Collaboration Assurance continues to search, when there is a large volume of data, before displaying the matching records found for a diagnostic report.
Report Data Retention Period (days)	Number of days that data is retained in the Cisco Prime Collaboration Assurance database before being purged.
SFTP	
Username	You cannot change the username from smuser. This same username, smuser, must be configured in Cisco Unified Communications Manager.

Fields	Description
Change password check box	<p>For Cisco Prime Collaboration Release 12.1 SP3 and later</p> <p>During fresh installation, ensure that the CUCM SFTP Credential is not set by default. You must set the CUCM SFTP password in Inventory Management -> CUCM SFTP Credentials tab.</p> <p>If credentials is not set, user will not be allowed to add PCA as a CDR Destination in CUCM during device discovery. The application must alert the user to set the CUCM SFTP password stating, "Please configure CUCM SFTP credentials to enable this feature. It can be configured under CUCM SFTP Credentials Tab".</p> <p>Note If you want to add PCA as a CDR destination in CUCM, while initiating device discovery, select the "Add the Prime Collaboration server as a CDR Destination in the Unified CM servers" check box in Discover Devices -> Device Discovery tab under Auto-Configuration option. For more information, see the section on "Discovery Methods".</p> <p>For Cisco Prime Collaboration Release 12.1 SP3 and earlier</p> <p>The default password is smuser. If you change the password here, you must also change the password for smuser in Cisco Unified Communications Manager.</p>

Administrative Reports

The following administrative reports are available:

Report	Description
System Status Report	<p>Provides information about Inventory, Data Purging, Notifications, Phone Licensing (comprises of Synthetic Tests, Phone Status Tests, and IP SLA Voice Tests), and System Limits.</p> <p>It also provides information about Synthetic Tests, Phone Status Tests, and IP SLA Voice Tests for the following test results only:</p> <ul style="list-style-type: none"> • Synthetic Tests: If the test failed to run because of High CPU Utilization in the Cisco Prime Collaboration Assurance server. • Phone Status Tests: If the SAA source device is not reachable. • IP SLA Voice Tests: <ul style="list-style-type: none"> • If the configuration is incorrect. • If the device has low memory. • If the source device is not responding. • If the device has rebooted. <p>It provides information about phone status test for the following test result:</p> <ul style="list-style-type: none"> • Phone Status test: If the SAA source device is not reachable. <p>For the following parameters of System Limits:</p> <ul style="list-style-type: none"> • Port - Ethernet ports are categorized under this parameter. • Interfaces - Voice interfaces are categorized under this parameter.
Who Is Logged On Report	Helps you to identify users who are currently logged into Cisco Prime Collaboration Assurance.
Process Status	Shows the status of processes that are currently running on Cisco Prime Collaboration Assurance.

CDR & CMR Call Report

Cisco Prime Collaboration Assurance can process only CDR and CMR data of last 24 hours. CDR reports displays call details such as call category type, call class, call duration, termination type, call release code, and so on. CMR reports can be cross launched from Top 5 Voice Call Quality Location and CDR reports can

be cross launched from Top 5 Call Failure Location. You can also cross launch CMR reports from ServiceQualityThresholdCrossed alarm . The report loads up to 40 records initially, you can scroll down to view more records.

You can select any grade from the generated report to view the details of CMR reports for that particular CDR Record in an inline CMR (popover).

**Note**

CDR reports work only when both Cisco Prime Collaboration Assurance and CUCM are in the same domain.

CMR report generate reports that include all call data from the clusters or reports that include a subset of call data.

The following table describes the fields of CDR call reports.

Field	Description
Grade	<p>Based on voice call grade settings. Select one of the following:</p> <ul style="list-style-type: none"> • Good—The call value is less than the threshold value of long call SCSR (%) or short call SCSR (%) . The value of this grade appears in green color. • Acceptable—The call value is greater than or equal to threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in orange color. • Poor—The call value is greater than the threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in red color. • N/A—The SCSR (%) value is not available or is negative. • All— Select all the grade.
Cluster ID	Unified Communications Manager cluster.

Caller/Called	<ul style="list-style-type: none"> • Directory Number—Directory number where the call was made. • Device Type—Type of device making the call. • Signaling IP—IP address of the device that originated the call signaling. For IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway. • B-Channel—B-channel number of the MGCP gateway, or NA, if not applicable. • Media IP—IP address where the call originated. • Codec—Codec name. • Media Port—Port through which the call originated. • Device Pool—Device pool where the call originated. • Device Location—Location where the call originated. When you select the Quick Filter from Show drop-down menu, search option is available for Caller/Called Device Location. • Device Name—Name of the device. • Termination Cause—String that describes why the call was terminated.
Caller Video/Called Video	<ul style="list-style-type: none"> • Video Codec— Video Codec name. • Video Bandwidth— Bandwidth of the video. • Video IP— IP address where the video originated. • Video Port— Port through which the video originated. • Video Resolution— Resolution of the video.
Call Class	<p>One of these:</p> <ul style="list-style-type: none"> • Offnet • Onnet <p>Note For more information, see Understand OffNet and OnNet Calls, on page 385.</p>

Time Period	Date and time that the call started with respect to the Cisco Prime Collaboration Assurance server local time zone (not the time zone in which Cisco Unified CM resides). The maximum time limit is 7 days. .
Call Duration(s)	Length of the call, in seconds.
Call Category Names	A comma-separated list of the categories to which the call belongs. For more information, see Call Classification, on page 383 and Call Category Creation, on page 385
Call Category Types	A comma-separated list of the category types to which the call categories belongs. For more information see Call Classification, on page 383 and Call Category Creation, on page 385

The following table describes the fields of CMR reports.

Field	Description
MOS	Average MOS value during the sample duration. The value might be N/A or not available if the sample duration is very short. MOS reflects the experience of the listener.
Minimum MOS	The minimum MOS score within the sample duration. The value might be N/A or not available if the sample duration is very short.
Grade	Based on voice call grade settings. Select one of the following: <ul style="list-style-type: none"> • Good—The call value is less than the threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in green color. • Acceptable—The call value is greater than or equal to threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in orange color. • Poor—The call value is greater than the threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in red color. • N/A—The SCSR (%) value is not available or is negative. • All— Select all the grade.

Caller/Called	<ul style="list-style-type: none"> • Directory Number—Directory number where the call was made. • Device Type—Type of device making the call. • Signaling IP—IP address of the device that originated the call signaling. For IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway. • B-Channel—B-channel number of the MGCP gateway, or NA, if not applicable. • Media IP—IP address where the call originated. • Codec—Codec name. • Media Port—Port through which the call originated. • Device Pool—Device pool where the call originated. • Device Location—Location where the call originated. When you select the Quick Filter from Show drop-down menu, search option is available for Caller/Called Device Location. • Device Name—Name of the device.
Listener DN/IP	<p>Identifies the endpoint-called or caller-for which MOS and impairment details are reported; one of these:</p> <ul style="list-style-type: none"> • IP address of the listener. • Directory number of the listener.
Jitter (ms)	Milliseconds of jitter during the sample duration.
Packet Loss	Number of packets lost due to network transmission during the sample duration. Computed based on observed RTP sequence number analysis.
Max Jitter (ms)	Maximum milliseconds of jitter during the sample duration.
Conceal Seconds	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely conceal seconds).
Severely Conceal Seconds	Number of seconds during which a significant amount of concealment (greater than fifty milliseconds) was observed.
Conceal Ratio	Ratio of concealment frames to total frames.

Latency	Delay
Cluster	Unified Communications Manager cluster.
Time Period	Date and time that the call started with respect to the Cisco Prime Collaboration Assurance server local time zone (not the time zone in which the Unified Communications Manager resides).
Call Duration(s)	Length of the call, in seconds.
Caller Termination Cause	String that describes why the call was terminated on the caller endpoint
Called Termination Cause	String that describes why the call was terminated on the called endpoint. See Call termination cause codes section in Cisco Unified Communications Manager Call Details Record Administration Guide for the cause codes for failed calls.
Video attributes	Endpoints Report contain video attributes (for video endpoints) such as: <ul style="list-style-type: none"> • Video duration • Video packets lost • Video jitter • Video round trip time • Video RX Resolution • Video RX Frames Lost
Severely Conceal Seconds Ratio (%)	A metric to measure the voice quality. It is the ratio of Severely Conceal seconds(SCS) and total call duration.
Conceal Seconds Ratio (%)	A metric to measure the network quality. It is the ratio of Conceal seconds(CS) and total call duration.

**Note**

- All the columns may not appear in CDR & CMR reports by default. To view other fields, click **settings** button and choose **columns**.
- CDR & CMR reports support Jabber.

For Cisco Prime Collaboration Release 11.5 and later

The Location field displays the location that is configured on a device pool instead of the location that is configured on the device, when you set the device location to one of the system locations (Hub_None, Phantom, or Shadow).

**Note**

- Cisco Prime Collaboration Assurance displays a user defined location instead of Hub_None in Unified Communications Manager for the following features and reports:
 - CDR & CMR Reports
 - Top 5 Poor Voice Call Quality Locations
 - Top 5 Call Failure Locations
 - Unregistered Phone Troubleshooting: Top 5 locations
 - Global Search by location
- If the device location is set to Hub_None and is not associated with any user defined device pool in Unified Communications Manager, Cisco Prime Collaboration Assurance displays the Device Location as Hub_None. Cisco Prime Collaboration Assurance also displays Hub_None as a valid location in Global Search by location option and in Unified Communications Manager troubleshooting view.

You can filter the fields of report using Quick Filter options. For more information, see the Quick Filter section in [Filters](#).

The CDR & CMR report can be exported in both CSV and PDF format. The maximum number of records that can be exported to a PDF file is 30,000. The maximum number of records that you can export to CSV is 200,000.

To export the report, click the **Export** tool button in the right-hand pane of the report window. If your client system seems unresponsive when you try to export files, see [Troubleshoot File Download Issues](#).

The supported video codecs in CDR & CMR report are listed in the following:

- AAC
- G711Alaw 56k
- G711Alaw 64k
- G711Ulaw 56k
- G711Ulaw 64k
- G722 48k
- G722 56k
- G722 64k
- G722.1 24k
- G722.1 32k
- G723.1
- G726 16K
- G726 24K
- G726 32K

- G728
- G729
- G729AnnexA
- G729AnnexAwAnnexB
- G729AnnexB
- GSM
- GSM Enhanced Full Rate
- GSM Full Rate
- GSM Half Rate
- iSAC
- H.264
- H.265

Generate CDR & CMR Reports

To generate CDR & CMR call report:



Note

Only an administrator can export CDR/CMR reports. A script must be created to automate the task of exporting on the server.

Step 1 Choose **Assurance Reports > CDR & CMR Reports**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > CDR & CMR Reports**.

The CDR & CMR Reports page is displayed.

Step 2 Enter the information in the fields described below:

Table 67:

Field	Description
Display	Select CDR/CMR from the Display
Cluster	Select the Clusters from Cluster. The default value is All.

Field	Description
Location/Devicepool	Select the Location or Devicepool from Location/DevicePool. The default value is Location. If you select Location from Location/DevicePool then select any location from Location. If you select Devicepool from Location/DevicePool then select any devicepool from Devicepool. You can also search Location/Devicepool from the search option available in Location or Devicepool. The default value for Location or Devicepool is Any.
Device Type	Select the devices from Device Type. The default value is Any.
Endpoint	Select Directory Number or IP Address from the Endpoint. The default value is Directory Number.
Caller	<p>Enter the Directory Number or Caller IP address. The default value of Directory Number is * and default value of IP address is *.*.*.</p> <p>Directory Number can include any combination of alphanumeric characters and special characters like +, *, @, -, .</p> <p>For Directory Number search, use uppercase X as a single-digit wildcard; use * as multiple-digit wildcard. For example 1100X or 11*.</p> <p>For IP address search, the * wildcard applies to the entire octet. For example: 172.30.*.* or 2005:0420:2e00:0094:*.*.*.</p>
Called	<p>Enter the Directory Number or Called IP address. The default value of Directory Number is * and default value of IP address is *.*.*.</p> <p>Directory Number can include any combination of alphanumeric characters and special characters like +, *, @, -, .</p> <p>For Directory Number search, use uppercase X as a single-digit wildcard; use * as multiple-digit wildcard. For example 1100X or 11*.</p> <p>For IP address search, the * wildcard applies to the entire octet. For example: 172.30.*.* or 2005:0420:2e00:0094:*.*.*.</p>
Call Category	Select the name or type from the Call Category. The default value is Name.
Category Name/Type	Select the Category name or Category Type. The default value is All.

Field	Description
Grade	Select Good, Acceptable, Poor, All or N/A. The default value is All.
Jitter	Select the range from Jitter and enter the value in milliseconds. The default range is greater than or equal to zero.
Packet Loss	Select the range from Packet Loss and enter the value in the field. The default range is greater than or equal to zero.
Conceal Seconds	Select the range and enter the value in seconds field. The default range is greater than or equal to zero.
Conceal Ratio	Select the range from Conceal ratio and enter the value in the field. The default range is greater than or equal to zero.
Call Type	Select Audio, Video or Any. The default value is Any.
Call Class	Select On-Net, Off-Net, or Any. The default value is Any.
Call Duration	Select the value of call duration from Call Duration and enter the time in secs field. The default value is Any.
Termination Type	Select Success, Failed, or Any. The default value is Any.
Termination Cause Code	Select the cause code from Termination Cause Code. The default value is All.
Time Period	<p>Select Call Connect Time or Call Disconnect Time. The default value is Call Connect Time. In case of cross launch from Top N dashlet, the default value is Call Disconnect Time.</p> <p>Call Connect Time—time when the call originates.</p> <p>Call Disconnect Time—time when the call ends.</p> <p>Select Past or Enter the Start Time and End Time. The default value is Past.</p> <p>The default value for the Start Time is one hour less than Current Time and End Time is Current Time.</p> <p>You can select Past in Minutes, Hour(s), or Days. The default value for Past is 1 Hour(s).</p> <p>For example, if you select Past as 8 Hour(s) at 10 p.m today then it displays the records from 2 p.m to 9.59 p.m today.</p> <p>If you select Past as 1 day at 10 a.m today then it displays the records from 12 a.m through 11.59 p.m of previous day.</p>

The Jitter, Packet Loss, Conceal Seconds, Conceal Ratio fields are applicable only for CMR Filter and Call Category, Call Type, Call Class, Call Duration, Termination Type, and Termination Cause Code fields are applicable only for CDR Filter.

Step 3 Click **Apply Filter**.

The CDR & CMR report is generated.

When records are not available for the selected filter, it displays no data available.

CDR & CMR report displays only the records of last 7 days.

Troubleshoot

1. Issue: CDR & CMR report displays Grade as N/A.

Recommended Action: Check if Severely Conceal Seconds Ratio value is not received from the endpoint or CMRs are not present.

2. Issue: Severely Conceal Seconds Ratio is x% and call is graded as Poor Call but in actual the call is not a poor call.

Recommended Action: You can configure threshold values for Severely Conceal Seconds Ratio from Voice Call Grade Page under CDR Analysis Settings.

3. Issue: Call grading is incorrect.

Recommended Action: Cross check the threshold values for Severely Conceal Seconds Ratio against Severely Conceal Seconds Ratio value in the CMR Report for the calls.

4. Issue: CDR/CMR Records are not received.

Recommended Action: Perform one of the following:

- Add PCA as billing server in the Unified CM, if it is not added.

When you add PCA as billing server, check the **resend on failure** option in the Unified CM to avoid any failure of CDR delivery.

- Verify if SFTP username/password is same in Cisco Prime Collaboration Assurance and billing server in Unified CM.
- Check if CDR repository manager or CDR agent services are up in Unified CM.
- Check if "CDR Enabled Flag" and "Call Diagnostics Enabled" options are set correctly in Unified CM.
- Check If any firewall settings blocks the file transfer, if it blocks then correct this at the network infrastructure level.
- If Data collection of a cluster is in Failed state in Call Quality Data source management page then run rediscovery for that publisher. For a list of Setting Up Devices and Configure Devices for Cisco Prime Collaboration Assurance, see the following:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
 - [Configure Devices for Cisco Prime Collaboration Assurance](#)

NAM & Sensor Report

NAM & Sensor report displays the name of the sensor that collected the data, MOS, jitter, and time stamp.

**Note**

This report is not applicable if you have installed Cisco Prime Collaboration Assurance in MSP mode.

To generate NAM & Sensor report, choose **Assurance Reports > NAM & Sensor Reports**. Enter the values in required fields and click **Generate Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > NAM & Sensor Reports**.

The following table describes the fields of NAM & Sensor reports.

Field	Description
Name	<p>Descriptive name for the sensor that collected the data and analyzed the MOS.</p> <p>Note The name Cisco 1040 + < <i>last 6 digits from MAC address</i> > identifies a Cisco 1040 that automatically registered with Cisco Prime Collaboration Assurance.</p>
ID	1040 MAC address or Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) IP address.

Speaker/Listener	<p>Directory Number—Displayed when the device is managed by a Unified Communications Manager that:</p> <ul style="list-style-type: none"> • Is added to Cisco Prime Collaboration Assurance with the proper credentials • Has not been suspended from monitoring. <p>Device Type—Can provide the device type or one of these:</p> <ul style="list-style-type: none"> • N/A—Some error prevents Cisco Prime Collaboration Assurance from obtaining the device type. • Unavailable-This is the first time Cisco Prime Collaboration Assurance has seen this phone and the device type is not yet known; or the corresponding Unified CM: <ul style="list-style-type: none"> • Has not been added to Cisco Prime Collaboration Assurance. • Did not provide a valid device type to Cisco Prime Collaboration Assurance. <p>IP Address—If an IP address is clickable, click it to launch the Detailed Device View page or Phone Detail window.</p> <p>UDP Port—Transport layer port that is the source of the media stream.</p> <p>Device Name.</p>
Time	Time at which the sensor calculated MOS.
TOS	Type of Service (TOS).
MOS	<p>Average MOS value during the sample duration. The value might be N/A or not available if the sample duration is very short.</p> <p>MOS reflects the experience of the listener. Click the value to open a Sensor Stream Correlation window.</p>
Minimum MOS	<p>The minimum MOS score within the sample duration.</p> <p>The value might be N/A or not available if the sample duration is very short.</p>

Primary Degradation Cause	<p>One of these:</p> <ul style="list-style-type: none"> • Jitter • Packet loss • None—Jitter and packet loss values are both 0 (zero). <p>The value might be N/A or not available if the sample duration is very short.</p>
Grade	<p>Based on voice call grade settings. Select one of the following:</p> <ul style="list-style-type: none"> • Good—The call value is less than the threshold value of long call SCSR(%) or short call SCSR(%). • Acceptable—The call value is greater than or equal to threshold value of long call SCSR(%) or short call SCSR(%). • Poor—The call value is greater than the threshold value of long call SCSR(%) or short call SCSR(%). • N/A—The SCSR(%) value is not available or is negative. • All— Select all the grade. <p>For more information see Overview of Voice Call Grade Settings, on page 219.</p>
Jitter (ms)	Milliseconds of jitter during the sample duration.
Packet Loss	Number of packets lost due to network transmission during the sample duration. Computed based on observed RTP sequence number analysis.
Sample Duration(s)	Number of seconds, between the first and last packet that is analyzed. The value is usually 60, but can be less for an initial or final stream.
Max Jitter (ms)	Maximum milliseconds of jitter during the sample duration.
Adjusted Packet Loss(%)	Percentage packet loss due to high jitter. Computed based on a reference jitter buffer with a fixed length delay. This value is not affected by network loss.
Packet Loss (%)	Percent of packet loss. (Packets lost divided by total packets expected expressed as a percent.)
SSRC	Synchronization source ID-Identifies the source of a stream of RTP packets.

Listener DN/IP	Identifies the endpoint-called or caller-for which MOS and impairment details are reported; one of these: <ul style="list-style-type: none"> • IP address of the listener. • Directory number of the listener.
Cluster	Unified Communications Manager cluster.
Caller/Called	<ul style="list-style-type: none"> • Directory Number—Directory number where the call was made. • Device Type—Type of device making the call. • Signaling IP—IP address of the device that originated the call signaling. For IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway. • B-Channel—B-channel number of the MGCP gateway, or NA, if not applicable. • Media IP—IP address where the call originated. • Media Port—Port through which the call originated. • Device Pool—Device pool where the call originated. • Location—Location where the call originated.
Select Time Range	Date and time that the call started with respect to the Cisco Prime Collaboration Assurance server local time zone (not the time zone in which the Unified CM resides). The maximum time limit is 7 days.
Call Duration(s)	Length of the call, in seconds.

Impairment Details	<ul style="list-style-type: none"> • Jitter (ms)—Milliseconds of jitter during the call. • Packet Loss—Number of packets lost during the call. • Concealment Seconds—Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds). • Severely Concealed Seconds—Number of seconds during which a significant amount of concealment (greater than fifty milliseconds) was observed. • Latency—Delay • Concealment Ratio—Ratio of concealment frames to total frames.
Call Release Code	<ul style="list-style-type: none"> • Caller Termination Cause -String that describes why the call was terminated on the caller endpoint. • Called Termination Cause -String that describes why the call was terminated on the called endpoint. See Call termination cause codes section in Cisco Unified Communications Manager Call Details Record Administration Guide for the cause codes for failed calls.
Call Category Names	A comma-separated list of the categories to which the call belongs. For more information, see Call Classification, on page 383 and Call Category Creation, on page 385
Call Category Types	A comma-separated list of the category types to which the call categories belongs. For more information, see Call Classification, on page 383 and Call Category Creation, on page 385
Call Class	<p>One of these:</p> <ul style="list-style-type: none"> • Offnet • Onnet <p>Note For more information, see Understand OffNet and OnNet Calls, on page 385 .</p>
Severely Conceal Seconds Ratio (%)	A metric to measure the voice quality. It is the ratio of Severely Conceal seconds(SCS) and the duration.

Conceal Seconds Ratio (%)	A metric to measure the network quality. It is the ratio of Conceal seconds(CS) and duration.
---------------------------	---

The NAM & Sensor report can be exported in CSV format.

To export the report, click the **Export** tool button in the right-hand pane of the report window. Select **ALL** or enter the value in **Range** radio button and click **OK**. If your client system seems unresponsive when you try to export files, see [Troubleshoot File Download Issues](#).

Understand Sensor Reports

Two RTP streams—incoming and outgoing—make up a single voice call. Sensors capture voice traffic in various ways:

- Cisco 1040s listen to RTP voice traffic on Switch Port Analyzer (SPAN) ports that have been configured to mirror voice traffic. Depending on the phone ports and the voice VLANs that a SPAN port mirrors, a Cisco 1040 might listen to only one or both RTP streams, calculating MOS and sending data to Cisco Prime Collaboration Assurance at 60-second intervals.
- Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) can also capture data from SPAN ports. Alternatively, you can configure Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) to use other means of data capture. For a Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) to provide the data that Cisco Prime Collaboration Assurance needs, RTP stream monitoring must be enabled on the Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM). Cisco Prime Collaboration Assurance obtains data from Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) at 60-second intervals.

Sensor reports display the MOS that a sensor calculated for RTP streams on a minute-by-minute basis. For each interval, a sensor report displays one or two rows of data, depending on whether data from only one or both RTP streams was captured. Each row identifies the sensor that collected the data, the endpoints involved, MOS, milliseconds of jitter, and the time stamp.

View Sensor Stream Correlation Data

To launch a Sensor Stream Correlation window, generate a sensor report and click the Grade value for the stream that interests you.



Note If a “Cannot find server” page appears instead of a Sensor Stream Correlation page, see [Enable the Sensor Stream Correlation Window to Display](#).

Cisco Prime Collaboration Assurance correlates data from sensors against one another and against Unified CM call records and displays tables with the following information:

- Stream summary—A subset of the data that was displayed on the sensor report. Additionally, the source synchronization ID (SSRC) for the stream is listed. An SSRC identifies the source of a stream of RTP packets and remains unique during an RTP conference.



Note Another SSRC is assigned to RTP streams sent when the listener endpoint and UDP port are the source of a stream of RTP packets. The Sensor Stream Correlation window correlates data for one SSRC only.

- Call record—Information from the Unified CM CDR that correlates to the stream.



Note If the call is not complete yet, No Call Detail Record found for these streams appears in the table heading.

- Stream details—Details from one or more sensors where the SSRC matches the one in the stream summary.

The following table lists the data that is displayed in the Stream Summary table.

Table 68: Stream Summary

Column	Description
Speaker/Listener	<ul style="list-style-type: none"> • Directory Number-Displayed when the device is managed by a Unified Communications Manager that: <ul style="list-style-type: none"> • Is added to Cisco Prime Collaboration Assurance with the proper credentials. • Has not been suspended from monitoring. • IP Address-Depending on the device type, an IP Phone Details page or a Detailed Device View opens. • UDP Port-Transport layer port that is the source of the media stream. • Device Type-Can provide the device type or one of these: <ul style="list-style-type: none"> • N/A-Some error prevents Cisco Prime Collaboration Assurance from obtaining the device type. • Unavailable-This is the first time that Cisco Prime Collaboration Assurance has seen this phone and the device type is not yet known; or the corresponding Unified CM: <ul style="list-style-type: none"> • Has not been added to Cisco Prime Collaboration Assurance. • Did not provide a valid device type to Cisco Prime Collaboration Assurance.

TOS	Type of service.
Codec	Codec name.
SSRC	Synchronization Source ID-Identifies the source of a stream of RTP packets.

The following table lists data from the CDR, if available. If the call has not completed yet, No Call Detail Record found for these streams appears in the table heading and the row is blank.

Table 69: Call Record

Column	Description
Call Disconnect	The time that the call disconnected. Zero (0) is displayed if the call never connected.
Cluster ID	Unified CM cluster ID.
Caller Signaling IP	IP address of the device that originated the call signaling. For Cisco Unified IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway.
Caller B-Channel	B-channel number of the MGCP gateway, or NA, if not applicable.
Called Signaling IP	IP address of the device that terminates the call signaling.
Called B-Channel	B-channel number of the MGCP gateway, or NA, if not applicable.
Call Duration (s)	Length of the call, in seconds.
Caller Termination Cause	Populated when the originating party releases the call. Note Termination causes might not be populated.
Called Termination Cause	Populated when the terminating party releases the call or the call is rejected. Note Termination causes might not be populated.

The following table lists data from streams with an SSRC that matches the one in Stream Summary table.

Table 70: Stream Details

Column	Description
Sensor Name	Display name of the Cisco 1040 or Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM).
Time	Time at which the sensor calculated the MOS.

MOS	Average MOS in the sample duration.
Minimum MOS	Minimum MOS in the sample duration.
Primary Degradation Cause	Jitter, Packet Loss, or None when jitter and packet loss values are zero (0).
Jitter (ms)	Milliseconds of jitter.
Packet Loss	Number of packets lost. (Actual packet loss for the sample duration.)
Sample Duration (s)	Number of seconds elapsed between the first and last packets that are analyzed.
Max Jitter (ms)	Maximum jitter, in milliseconds.
Adjusted Packet Loss (%)	Percentage packet loss due to high jitter. Computed based on a reference jitter buffer with a fixed length delay. This value is not affected by network loss.
Packet Loss (%)	Percentage packet loss. (Actual packets lost divided by total packets expected expressed as a percent.)

Enable the Sensor Stream Correlation Window to Display

When you try to open a Sensor Stream Correlation window, if a window opens displaying a message such as “The page cannot be found”, you can resolve the problem by disabling the proxy server setting in your browser. The setting is found in Internet Options on the Connection tab.

Session Reports/Conference Reports

You can use Conference reports to view All Conference Summary report and Conference Detail report.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Conference Reports

The following are required for conference reports:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the [Configure Devices for Cisco Prime Collaboration Assurance](#).
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 Service Pack 1.

The following reports can be generated for Conference reports:

All Session/Conference Summary Report

The Conference Summary report provides information about the in-progress and completed conferences. The reports are available for four weeks.

This report includes the following information: endpoint name, device ID, total utilization, average duration, and longest conference.

It displays the scheduled duration of the scheduled conference. For an Ad hoc conference this value is displayed as "NA". It also displays utilized scheduled time in % which denotes the scheduled time utilization in percentage.

You can view the following additionally:

- IP address - Displays the IP Address of the selected endpoint that participated in the conference.
- Protocol - Displays the protocol used for the conference. This is displayed in the Participated conferences of Endpoint pane.

Ensure that the visibility of the phones is set to Full, to view the preceding details.

You can view the following additionally

- Received Video DSCP - The last received DSCP value of the video device(s) in the conference. This is only applicable for Cisco Unified IP Phones 8941 and 8945, Cisco DX Series, and Cisco TelePresence TX Series.
- Received Audio DSCP - The last received DSCP value of the audio device in the conference. This is only applicable for Cisco Unified IP Phones 8941 and 8945, Cisco DX Series, and Cisco TelePresence TX Series.
- Peak Packet Loss - The highest value of packet loss (in percentage) that occurred in the conference.

To generate the Conference Summary report, choose **Assurance Reports > Session Reports > All Session Summary Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Conference Reports > Conference Summary Report**.

Session/Conference Detail Report

The Conference Detail report provides the following details: conference ID, duration, start/end time, conference type, status, and alarm severity.

To generate the Conference Detail report, choose **Assurance Reports > Session Reports > Session Detail Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Conference Reports > Conference Detail Report**.

TelePresence Endpoint Reports

You can use TelePresence reports to view endpoint utilization, and no show endpoints summary.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Telepresence Endpoint Reports

The following are required for Telepresence Endpoint Reports:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the [Configure Devices for Cisco Prime Collaboration Assurance](#).
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 Service Pack 1.

The following reports can be generated for TelePresence endpoints:

Endpoint Utilization Report

The Endpoint Utilization report enables you to identify the most utilized and least utilized endpoints.

Average utilization of an endpoint is calculated using the following formula:

- For system-defined (1 day, 1 week, 4 weeks) reports:
$$(\text{Total number of utilization in minutes} / [\text{maximum utilization} * 60]) * 100$$
- For custom reports:
$$(\text{Total number of utilization in minutes} / [\text{maximum utilization} * 60 * \text{number of days}]) * 100$$
 - 1 day: The maximum utilization is ten hours.
 - 1 week: The maximum utilization is 50 hours.
 - 4 weeks: The maximum utilization is 200 hours.
 - Custom report: The maximum utilization is 7.14 hours per day.

It displays the utilized scheduled time in % which denotes the scheduled time utilization in percentage.

You can customize the endpoint utilization settings. To do so, select an endpoint model (endpoint(s) of a particular model) and then click the **Change Utilization** button. You can select the number of working hours in a day and the number of working days in a week.

To generate the Endpoint Utilization report, choose **Assurance Reports > Telepresence Endpoint Reports > Endpoints Utilization Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Telepresence Endpoint Reports > Endpoints Utilization Report**.

No Show Endpoint Summary Report

The No Show Endpoints Summary report provides information about the endpoints that did not participate in the scheduled conferences. This report is generated based on the scheduled completed conferences data.

To generate the No Show Endpoints Summary report, choose **Assurance Reports > Telepresence Endpoint Reports > No Show Endpoint Summary Report**.

For Cisco Prime Collaboration Release 11.5 and later

To generate the No Show Endpoints Summary report, choose **Reports > Telepresence Endpoint Reports > No Show Endpoint Summary Report**.

Launch CUCM Reports

Launch CUCM Reports enables you to cross launch to the reporting pages for the Cisco Unified Communications Manager clusters.

Go to **Launch CUCM Reports**, and click a cluster name to open the Cisco Unified Reporting application.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Launch CUCM Reports**.

Miscellaneous Reports

You can use Miscellaneous reports to view Other Reports, UCM/CME Phone Activity Reports, and Voice Call Quality Event History Reports.

UCM/CME Phone Activity Reports

UCM/CME Phone Activity reports provide information about the audio and video phones that have undergone a status change during the last 30 days.

If you have deployed Cisco Prime Collaboration Assurance in Enterprise mode, the Phone Activity reports display the domain name, except the Export Audio Phones report.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the Phone Activity reports display the customer name, except the Export Audio Phones report.

The following Activity reports are available:

Endpoint Move Report

The **Endpoint Move** report displays the details of IP/Video endpoints that have been moved in the last 30 days. It also displays the Extension, Cisco Unified CM address, switch address, and switch ports used before and after the move.

The **Endpoint Move** report shows the time at which the IP/Video endpoint move was detected, and not the time at which the move occurred.

To generate the Endpoint Move report, choose **Reports > Miscellaneous Reports > Endpoint Move**.

**Note**

Endpoint Move report is not supported for the video endpoints that do not support CDP.

Endpoint Audit Report

The Endpoint Audit Report shows the change that have occurred in the managed IP/Video endpoint network.

For example, this report shows you the IP/Video endpoint that have been added or deleted from your network, IP/Video endpoint status, and so on. Endpoint status changes occur, for instance, when an endpoint becomes unregistered with the Cisco Unified CM.

To generate the Endpoint Audit Report, choose **Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Endpoint Audit**.

**Note**

Endpoints appear as "Removed" in the Audit Report when they are unregistered in CUCM for more than 24 hours. For the record, endpoints that are deleted from CUCM while they are registered will first be shown as "Unregistered" in the Audit Report for the next 24 hours, and will be shown as "Removed" beyond that. Note that these will be deleted from Cisco Prime Collaboration Assurance Inventory after the first CDT discovery that happens after the deletion.

Endpoint Remove Report

The Endpoint Remove report lists endpoints that have been removed during the last 30 days.

To generate the Endpoint Remove report, choose **Reports > Miscellaneous Reports > Endpoint Remove Report**.

Endpoint Extension Report

The Endpoint Extension Report lists the endpoints for which extension numbers were changed during the last 30 days.

To generate the Endpoint Extension Report, choose **Reports > Miscellaneous Reports > Endpoint Extension Report**.

**Note**

The Endpoint Extension Report is not supported for Cisco Wireless IP Phone 7920.

Understand the Time Period Covered by Audio IP Phone Activity Reports

For Cisco Prime Collaboration Release 11.1 and earlier

When you generate an Audio IP Phone or Video IP Phone Activity report, your results can be affected by the time zones in which each of the following resides:

- Your client system—Cisco Prime Collaboration Assurance calculates the time period (previous 24 hours through previous 7 to 30 days, depending on the report) for Phone Activity reports based on the date and time on your client system.
- Prime Collaboration system—Cisco Prime Collaboration Assurance records some audits, such as extension number changes, based on the time that the change is detected on the Cisco Prime Collaboration system.
- Cisco Unified Communications Manager—Cisco Prime Collaboration Assurance records some audits, such as phone moves, based on the time on Cisco Unified CM that changes were detected.

If any of these systems is not in the same time zone as your system, you must take the time zone difference into account when you generate and view Phone Activity reports.

**Note**

If the audit date and time on the Cisco Prime Collaboration Assurance system is inconsistent with those shown in the Audio IP Phone or Video IP Phone Audit report, make sure that all Cisco Unified CM in the network are set to synchronize.

Track Phone Status when Cisco Unified CM Is Down

For Cisco Prime Collaboration Release 11.1 and earlier

If a Cisco Unified CM that is configured with a backup goes down, audio and video IP phones fail over to the backup Cisco Unified CM.

Cisco Prime Collaboration Assurance stores audit records for the phones that register with the backup and these status changes are included in IP Phone and Video Phone Audit reports.

Cisco Prime Collaboration Assurance does not store audit records in the following cases:

- An entire Cisco Unified CM cluster goes down.

A Cisco Unified CM for which a backup is not configured goes down.

Therefore, status changes for the phones registered to Cisco Unified CM in these situations are not included in Audio IP Phone Status and Video IP Phone Activity reports.

Voice Call Quality Event History Reports

You can search the Event History database for Voice Call Quality events based on:

- MOS
- Destination
- Codec
- Phone model

- Sensor(not applicable if you have installed Cisco Prime Collaboration Assurance in the MSP mode)
- Date
- Export

To generate Call Quality Event History report, choose **Assurance Reports > Miscellaneous Reports > Voice Call Quality Event History Reports**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Miscellaneous Reports > Voice Call Quality Event History Reports**.

The Voice Call Quality Event History report is a scrollable table that lists up to 2,000 records, based on your search criteria.

To view database contents beyond 2,000 records, choose **Assurance Reports > Miscellaneous Reports > Voice Call Quality Event History Reports > Export**, click **Export**. If more than 1,000 records match your search criteria, a popup window reports the total number of matching records found.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Miscellaneous Reports > Voice Call Quality Event History Reports > Export**.

When you export Voice Call Quality Event History Reports In Internet Explorer browser, the **Windows Security** popup window may prompt for your credentials. The report is downloaded even if you cancel the **Windows Security** popup window.

For the Save at field, enter a location for storing the reports on the server where Cisco Prime Collaboration Assurance is installed; the default location is /opt/emms/cuom/ServiceQualityReports.



Note

If you configure export settings to save files outside of default location, be sure to log into the Cisco Prime Collaboration Assurance server, create the folder that you entered on the Export Settings page, and provide write permission to the folder for the user. If you do not perform these tasks, Cisco Prime Collaboration Assurance cannot create the export files.

For the E-mail to field, enter one or more complete e-mail addresses separated by commas.

To download the report, click **Download Report**.

If you have deployed Cisco Prime Collaboration Assurance in the Enterprise mode, the Call Quality Event History reports can be viewed for a specific domain selected from the global selector (drop-down). However, when you export the report, using the export option, the reports are not filtered based on the domain selected from the global selector.

If you have deployed Cisco Prime Collaboration Assurance in the MSP mode, the Call Quality Event History reports contain customer details such as, customer name. The reports can be viewed for a specific customer selected from the global selector (drop-down). However, when you export the report, using the export option, the reports are not filtered based on the customer selected from the global selector. Also, in this mode, you cannot search the Event History database for Voice Call Quality events based on Sensor.

Other Reports

Other reports provide information about CTI applications, Cisco Analog Telephone Adaptor (ATA) devices, and Cisco 1040 sensors if you have deployed Cisco Prime Collaboration Assurance in Enterprise mode.



Note If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you cannot generate reports for Cisco 1040 sensors.

To generate these reports, choose **Assurance Reports > Miscellaneous Reports > Other Reports** and select a report.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Miscellaneous Reports > Other Reports**.

CTI Applications Report

The CTI Applications report lists CTI applications that are registered with Cisco Unified CM.

The following applications are registered to Cisco Unified CM as CTI devices or CTI ports:

- Cisco Personal Assistant
- Cisco Customer Response Applications
- Cisco IP Contact Center
- Cisco Emergency Responder

ATA Devices Report

The ATA Devices report provides information about the ATA devices that are registered with Cisco Unified CM.

Cisco 1040 Sensors Report

The Cisco 1040 Sensors report provides information about Cisco 1040 sensors that are deployed in your network. Before you generate Cisco 1040 Sensors Report, see prerequisites in [Prerequisites to Generate the Cisco Prime Collaboration Assurance Reports](#).



Note This report is not applicable if you have installed Prime collaboration in MSP mode.

When a web interface is accessible for an IP phone, you can open it from Cisco 1040 sensor report by clicking the hyperlink for one of the following:

- Extension number
- MAC address
- IP address

Conferencing Device Video Port Utilization Report

This report is generated based on the hourly utilization of conferencing devices.

Average Utilization

- 1 day: Average utilization of hour 1 + hour 2 + ... + hour 24) / 24.
- 1 week: Average hourly utilization of each hour in the week is aggregated and divided by (7 x 24).
- 4 weeks: Average hourly utilization of each hour in the 4 weeks is aggregated and divided by (7 x 24 x 4).
- Custom period: Average hourly utilization of each hour in the custom period is aggregated and divided by (24 x number of days in custom period).



Note

The utilization is shown as 100% even if the utilization is more than 100%.

Peak Utilization

- 1 day: The peak utilization is analyzed from individual peak values of each of the 24 hours.
- 1 week: The peak utilization is analyzed from individual peak values of each of the 7*24 hours.
- 4 weeks: The peak utilization is analyzed from individual peak values of each of the 7*24*4 hours.
- Custom periods: The peak utilization is analyzed from individual peak values of each hour in the custom period.

To generate the Conferencing Device Utilization report, choose **Assurance Reports > Miscellaneous Reports > Other Reports > Conferencing Device Utilization Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports > Miscellaneous Reports > Other Reports > Conferencing Device Utilization Report**.

Click the value of the Average Utilization or Peak Utilization columns to launch the Detailed Video Port Utilization graph. You can choose to view Hourly Average Utilization, Peak Utilization, or actual data (click **All**). You can also use the slider and select a small time interval also (such as a minute) to view actual data for that interval.

Scheduled Reports

Scheduled reports are utilization and inventory reports that you can schedule from the Report Launch Pad. You can generate them according to your scheduling preferences, and download or send them to the configured e-mail ID. These reports can be exported in both CSV and PDF format (except the Conference Detail Report, which can be exported only in CSV format). The data for these reports will be available for 30 days only.

These reports are not enabled by default. You can generate the reports on the spot or enable scheduling to generate them on predefined days.

Choose **Reports -> Scheduled Reports -> Reports**

The following scheduled reports are available:

Report Title	Description
Utilization Reports (Under Reports selector, select Utilization > Endpoint, and Endpoint No Show to see the Monthly Utilization and Monthly No Show Reports.)	
Monthly Utilization Report	Provides aggregate monthly reports on the utilization of the endpoints. The aggregate value is calculated by <i>Total utilization for all months / 12</i> .
Monthly No Show Report	Provides aggregate monthly reports on the nonparticipation of endpoints in scheduled conferences. The average aggregate value is calculated by <i>Total no show for all months / 12</i> .
Conference Detail Report	Provides details on the conference statistics for all completed conferences.
Inventory Reports	
Managed Devices Report	Provides information about managed devices. If a device is unknown, only the IP address is displayed. Use this report to find devices for which credentials have been updated.
Unmanaged Devices Report	Provides information about unmanaged devices. Use this report to identify devices for which credentials need to be updated.
Endpoints	<p>Provides information on the endpoints as displayed in the Endpoints Diagnostic page. For more information, see the Endpoint Diagnostics Dashboard, on page 239 section.</p> <p>Note The description on Cisco Unified Communications Manager (Call Manager) is mapped with the Endpoint Name column in Endpoint Report.</p> <p>The association of Endpoint Name and User Name columns helps in identifying the unique Cisco Jabber or Client Services Framework (CSF) devices.</p>
For Cisco Prime Collaboration Release 12.1 SP3 and later Endpoint(s) Reports (Under Reports selector, select Inventory -> Endpoints to view the following schedule reports: Endpoints Audit, Endpoints Move, Endpoints Remove, and Endpoints Extension Audit.)	

Report Title	Description
	<p>For Cisco Prime Collaboration Release 12.1 SP3 and later</p> <p>You can schedule Endpoints Audit, Endpoints Move, Endpoints Remove, and Endpoints Extension Audit reports and send the generated reports through email notification to the specified email ID. The generated report must list the details of last 1 day.</p> <p>If you have deployed Cisco Prime Collaboration Assurance in MSP Mode, Customer name column should be listed.</p>
Event History Reports	
All Events	Provides history of all the events that occurred in last one day, one week, or one month.



Note Scheduled Utilization reports (Monthly Utilization, Monthly No Show, and Conference Detail reports) are applicable for both video phones and TelePresence endpoints. Endpoint details will be populated in these reports based on the license that you purchased.

Generate Scheduled Reports

You can define the reporting period, the report generation date, and the frequency according to your preferences.

To generate a scheduled report:

-
- Step 1** Select a report from the Reports pane.
 - Step 2** Click the Settings tab under the Report Details pane, and click Enable Scheduling.
 - Step 3** Schedule the report generation using options in the Scheduler and Settings pane.
 - Step 4** Do either of the following:
 - Click **Save**.
 - Generate the report on the spot:
 - Click **Run Now** (adjacent to the report you want to generate).
 - Click the Run History tab under the Report Details pane.
 - Download the report.
-

To create a customized scheduled report, select a report from the Reports quick display in the left corner only, and click New under the Reports pane. Enter the required information and click Submit. Instances of the run

report are queued as jobs under the Job Management page. You can manage and monitor these jobs from the Job Management page (**System Administration > Job Management**).

Access Data for Reports that Contain More than 2,000 Records

Cisco Prime Collaboration Assurance reports display up to 2,000 records. If more than 2,000 records are returned when you generate a report, Cisco Prime Collaboration Assurance displays an informational message before displaying the report.

In this case, you can:

- Enter more specific filters to generate a report with fewer records.
- Export the report data to a CSV file to access the additional records. To open the export window, click the Export icon in the top right of the report window. You can export up to 30,000 records to a CSV file.



Note If your client system seems unresponsive when you try to export files, see [Troubleshoot File Download Issues](#).

Troubleshoot File Download Issues

If you try to export a report or other data to a file from Cisco Prime Collaboration Assurance and either the export dialog box or the window that prompts you to save the export file does not appear, use these procedures to try to fix the problem.

Procedure

	Command or Action	Purpose
Step 1	If you set the custom levels of security in Internet Explorer to medium or greater, the option, Automatic prompt to file download, is disabled. If you try to download a PDF or CSV file to a client system where Adobe Acrobat Reader or Microsoft Excel not installed, nothing happens. The PDF file or the spreadsheet is not displayed nor is a window that prompts you to save the file. To enable file download windows to display, do this on your desktop:	
Step 2	If you are using Internet Explorer, Automatic prompt to file download is enabled, and the window that prompts you to save the file still does not appear, do this:	



PART **VII**

Analyzing the Network

- [Analytics Dashboards and Reports, on page 431](#)



CHAPTER 25

Analytics Dashboards and Reports

This section explains the following:

- [Cisco Prime Collaboration Analytics Dashboards and Reports, on page 431](#)
- [Troubleshooting Prime Collaboration Analytics Dashboard, on page 468](#)

Cisco Prime Collaboration Analytics Dashboards and Reports

Cisco Prime Collaboration Analytics dashboards have time-period dependency. A report cannot be generated until enough time has passed to process data for the time period, specific to that report (daily, weekly, or monthly).

For Cisco Prime Collaboration Release 11.0 and earlier

You can generate custom reports for any period within the last one year only. And all report data older than one year are purged.

Following must be complete to enable data display on the Cisco Prime Collaboration Analytics dashboards for the first time you launch Cisco Prime Collaboration Analytics:

- Device Discovery
- **For Cisco Prime Collaboration Release 11.1 and earlier**
 - Session Import
- Conference Import
- Device Polling

See [Cisco Prime Collaboration Assurance Guide - Advanced](#) for more information about these tasks.

Cisco Prime Collaboration Analytics User Roles

User roles are used to define the authorizations of tasks that the users can access.

The user can be assigned to one of the following roles:

- Helpdesk—Does not have access to Analytics menu.
- Operator—Can view all the dashboards, but do not have access to edit and delete scheduled reports. Also, operator users does not have any configuration capabilities.

- Report viewer—Have access to all the dashboards except Capacity Analysis, License Usage, and My Dashboard. Report viewer cannot schedule reports and do not have access to the Scheduled Reports menu.
- Network Administrator, System Administrator and Super Administrator—Can access all the dashboards and can perform all the configuration tasks.

If you have deployed Cisco Prime Collaboration Assurance in MSP Mode, you do not have access to Custom Report Generator menu.

For more information about Cisco Prime Collaboration Assurance roles and its capabilities refer Cisco Prime Collaboration Assurance-Advanced User Roles in [Cisco Prime Collaboration Assurance Advanced Guide](#).

[User Roles and Tasks](#) lists the Cisco Prime Collaboration Analytics user roles and tasks they are mapped to.

Global Customer Selection

For Cisco Prime Collaboration Release 11.5 and later

This section applies only if you have deployed Cisco Prime Collaboration Assurance in MSP mode.

On the Cisco Prime Collaboration Assurance home page, you can select customers. To select customers, click the settings icon at the top right, and choose **Customer**. From the **Customer** dialogbox select the required customer names and click **Ok**. Based on the customer selection, data is displayed in analytics dashboards.

For more information on global customer selection refer Global Customer Selection section in [Cisco Prime Collaboration Assurance Advanced Guide](#).

Global Domain Selection

For Cisco Prime Collaboration Release 11.5 and later

This section applies only if you have deployed Cisco Prime Collaboration Assurance in Enterprise mode.

On the Cisco Prime Collaboration Assurance home page, you can select domain. Based on the domain selection, data is displayed in analytics dashboards.

For more information on global domain selection refer Global Assurance Domain Selection section in [Cisco Prime Collaboration Assurance Advanced Guide](#).


User Interface

You can use the Prime Collaboration Analytics user interface (UI),

- To view the dashlet details in chart mode or grid mode
- To export data
- To change the chart types
- To view the detailed view or quick view - These also let you choose chart or grid display.
- To view data tips for the corresponding pie wedges or bar wedges
- To maximize the dashlet

You can filter the data displayed based on Cluster and Duration in the *Filters* pane.

You can maximize the dashlet by clicking the maximize icon at the top right corner of the dashlet. When you click the maximize icon, the dashlet opens in a new tab.

By default, the layout template for all Analytics dashlets is set as 50/50. In order to gain an optimum view, we do not recommend you to change this setting. However, if you wish to set a custom layout, click  icon at the top right, choose **Layout Template** and select your desired layout.

Quick View

You can click a pie wedge or a bar wedge on the chart to launch the quick view of the corresponding endpoint. The quick view displays graph only for the selected endpoint. Similar to the dashlet view, quick view also allows you:

- To view the dashlet details in chart mode or grid mode
- To change the chart types
- To export data
- To launch the detailed view

Global Filter Option

Filter option is available at the top left of the UI for each dashlet. You can filter the data displayed for all dashlets based on duration (for example, last one week, one month and so on) and other attributes based on the dashlet type; for example call types (audio or video) in Traffic Analysis dashboards.



Note For Cisco Prime Collaboration Release 11.1 and earlier

Global filters are not applicable for the Metrics in the Technology Adoption dashboard.

Detailed Analysis

Prime Collaboration Analytics provides a detailed analysis (click See Details at the bottom-right) of each dashlet (endpoints, devices, technology usage...).

The Detailed Analysis page consists of Metrics and Filter pane, and Graph pane:

Metrics and Filter pane- You can filter data based on time period, call direction, call type, call status, calculation (of absolute values or percentage), call count, call duration, endpoint type, endpoint model, deployment status, cluster, or location/device pool.



Note For all dashlets in Capacity Analysis, you can filter the results using custom group, utilization, individual graphs (display each entity one below the other and is limited to 20 graphs per page) or merged graphs (display all entities in a single graph). You can sync custom dates in all graphs by selecting 'Keep selected time span in sync across all graphs'.

The *Export* option, available after the Metrics and Filter pane, at the top-right, allows you to schedule the export. You can generate reports for a dashlet according to your scheduling preferences, and download or send them to the preferred e-mail ID (You can even send the failure notification if the report generation is

unsuccessful). You can also send the scheduled reports to the configured sFTP server. To configure sFTP server, see [Configure sFTP Server](#) . The data from charts can be exported in CSV format or PDF, and the data from tabular-based dashlet can be exported in CSV format.

Graph pane- The graph displayed is based on values set for each parameter in Filter pane. The slider below the graph displays the desired time range (set in the Filter pane), you can drag the slider to zoom into a particular time period (narrow the time period) or alter values in x-axis and y-axis, resulting in the data being filtered for that period.

Tabular view- Prime Collaboration Analytics also provides option to view data in a tabular format that provides in-depth/detailed analysis of the data, such as detailed call record, hourly network usages, endpoint information and so on. Tabular view, in the Detailed Analysis, pops-up when you click legends/series displayed below the slider, or when you double-click at any point on the graph. You can also filter the data in the table or export it.

**Note**

- In detailed view, dashlets with Cisco VCS registered endpoints display the device pool and location, whenever the sub-zones are not configured. The Cisco VCS cluster or sub-zone details are displayed in the following dashlets:
 - All dashlets in Traffic Analysis.
 - All dashlets in Service Experience.
 - —All dashlets except for Deployment Distribution by Endpoint Model Endpoints Deployment Summary in Technology Adoption.
 - Least Used Endpoint Types (Asset Usage).

If the sub-zones are not configured in Cisco VCS, location, codec, and device pool details are displayed as VCS_Unknown. Impairment details are not applicable for Cisco VCS registered calls and is displayed as zero in the detailed view.

- **For Cisco Prime Collaboration Release 11.1 and earlier**

The detailed view of the Call Detail Records (CDRs) based dashlets displays the CDR or Call Management Records (CMRs) data only for the last 30 days. The call details of the endpoints prior to 30 days are not displayed by the dashlets, however, the aggregation of CDR or CMR data for the endpoints is available for the time period of 13 months or 56 weeks.

—The detailed view of the Call Detail Records (CDRs) based dashlets displays the CDR or Call Management Records (CMRs) data only for the last 30 days. The call details of the endpoints prior to 30 days are not displayed by the dashlets, however, the aggregation of CDR or CMR data for the endpoints is available for the time period of 3 months or 12 weeks

- For dashlets with IP address and Directory Number filters, ensure that you enter the details in the following order:
 - The IP address must be in the format x.x.x.x, and the range can be between 0.0.0.0 and 255.255.255.255, excluding these two values. It must not contain any special characters.
 - For Directory Numbers, only the following special characters are allowed: +, @, and . (period).
- In some dashboards, such as Capacity Analysis, Asset Usage (except Least Used Endpoints), you can view maximum data of 100. If the filter results in more than 100 items, an error message is displayed. Also, if the filter option is supported for Endpoint Types and Locations, the maximum value of 100 is applicable for Locations and not endpoint.
- While exporting the data, all analytics data is exported. The filter parameters are applicable for the data displayed on UI only and not for the exported data.

The Quick Tips help you customize the graphical view for your convenience.

Schedule Report, Export and Import

The drop-down icon available in the bottom-left, of the each dashlet, provides you with an option to choose among print, export and scheduling the report. You can generate reports for a dashlet according to your scheduling preferences, and download or send them to the preferred e-mail ID (You can even send the failure

notification if the report generation is unsuccessful). You can also send the scheduled reports to the configured sFTP server. To configure sFTP server, see [Configure sFTP Server](#).

When you schedule a reporting job, you can only select the start date and not the start time. Prime Collaboration schedules the job through the Job Scheduler. A periodic job runs every 60 minutes to check and execute the reports created newly on the current day, irrespective of the recurrence interval. By default any new report created on the current day with recurrence interval only once is executed again at 10.59PM in the respective time zone.

All the scheduled recurrent reports(daily, weekly, and monthly) runs between 5Am-8Am in the respective time zone everyday based on the recurrence interval. These reports are prioritized as low and high based on the time taken to run the reports. The reports that take more time is categorized as low priority and those which take less time to run as high priority reports. The high priority reports are executed first in a serial fashion followed by the low priority reports. Low priority reports are run in batches of 4.

The data from charts can be exported in CSV format or PDF, and the data from tabular-based dashlet can be exported in CSV format. You can also specify the number of instances that can be saved per report. After the number of instances reach the specified limit, the first report that was saved in the chronological order will be purged.

1. **Data Purging in Bottom Table:** During purging, the Bottom Table (BT) data will be purged after 35 days but the history of execution will have the exact number of times the Scheduled Report has been generated.
2. **Custom Interval in Scheduled Reports:** For the custom interval, if the Scheduled Report is generated, a report will be generated for the same interval when it is scheduled.

**Note**

Hence, it is recommended not to schedule a report for the custom interval.

Managing Customer Logo

For Cisco Prime Collaboration Release 11.5 and later

If you have deployed Cisco Prime Collaboration Analytics in MSP mode, you can assign a logo to the customer. These logos are displayed in the reports generated from the dashlet(scheduled or exported). The generated report will contain the logo of the customer selected in the global customer selection.

**Note**

The customer logo will be available only in the PDF format of the report.

You can upload, delete, and reset the logo of the customer.

To upload customer logo:

Before you begin

You must have administrator privilege to perform this task.

Step 1 Choose **Analytics Administration > Upload Customer Logo**.

Step 2 Choose the appropriate customer name.

Step 3 Click **Browse** and select the appropriate image.

Note You can upload images only in the format .jpg, .jpeg, .bmp, or .gif.

Step 4 Click **Submit** to save the image as customer logo.

To delete the logo, click **Delete Logo**. You can click **Reset** to update the logo.

Configure sFTP Server

To configure sFTP server:

Before you begin

If you have deployed Cisco Prime Collaboration Analytics in MSP mode, ensure the following:

- The user `<userid>` is available in the sFTP server.
- The folder `/<path>/<userid>` is available in the sFTP server and accessible only by that specific user `<userid>` and the administrator.

Step 1 Choose **Analytics Administration > sFTP Settings**.

Step 2 Enter the required details on the **sFTP Settings** page. Refer [Table 71: sFTP Settings Fields, on page 437](#) for field description.

Step 3 Click **Test Connection** to check the connectivity to the sFTP server.

Note In MSP mode, using test connection you can verify whether the folder `/<path>/<userid>` is available in the sFTP server.

Step 4 Upon successful connection, click **Save**.

For Cisco Prime Collaboration Release 11.1 and earlier

In MSP mode, the operator users do not have access to **Analytics Administration** menu and cannot configure sFTP server.

Table 71: sFTP Settings Fields

Field	Description
sFTP Server(IP Address)	IP address of the sFTP server where the scheduled reports must be saved.
sFTP Port	Port number of the sFTP server.

Field	Description
Path(Directory)	Directory path in the sFTP server where the scheduled reports must be saved. If you have deployed Cisco Prime Collaboration Analytics in MSP mode, the reports are saved in the location <code>/<path>/<userid></code> and if you have deployed Cisco Prime Collaboration Analytics in enterprise mode, the reports are saved in the location <code>/<path></code> .
User Name	Username for accessing the sFTP server.
Password	Password for accessing the sFTP server.

Prerequisites for Data Population in the Cisco Prime Collaboration Analytics Dashlets

Ensure that the following prerequisites are met for data to be populated in the Cisco Prime Collaboration Analytics dashlets.

- Endpoints registered with Unified CM and Cisco VCS are discovered (**Inventory**).
- CDR records for Unified CM and Cisco VCS registered endpoints is available (**Reports > CDR & CMR Reports**).
- Confirm data collection for the registered Unified CM in **Alarms & Events Administration > CDR Source Settings > Manage Call Quality Data Sources**.
- Verify data population by setting the global filters empty in the respective dashboard.
- Analytics uses historical data collected for a selected period of time. While selecting the filters for days, weeks, and months, the data is displayed excluding the current day, week, and month.

Technology Adoption

Use the Technology Adoption dashboard to validate technology investments made so far. This dashboard also provides key decision-support metrics that you can use in future investment decisions.

Prerequisite : The endpoints registered to Unified CM and Cisco VCS should be discovered.

Data Source : The device details for this dashlet is collected from Prime Collaboration inventory and the call details are collected from Unified CM and Cisco VCS CDR.

All dashlets in this dashboard display data for endpoints registered with Unified CM and VCS.

The deployment details for the Unknown endpoints will not be displayed in the Technology Adoption dashlets.

The Technology Adoption dashboard displays metrics that provide a quick update and a snapshot view of audio endpoints and video endpoints deployed in your organization.

The Technology Adoption dashboard displays the following metrics:

Metrics	Provides a quick update on
---------	----------------------------

Video endpoints deployed	<ul style="list-style-type: none"> • Total video endpoints in use • Change in the number of endpoints in the last 1 month • Percentage of video endpoints deployed
Video call minutes	<ul style="list-style-type: none"> • Total duration of video calls • Change in the duration of video calls in the last 12 weeks • Trend of video call usage
Audio endpoints deployed	<ul style="list-style-type: none"> • Total number of audio endpoints • Change in the number of endpoints in the last 1 month • Percentage of audio endpoints deployed
Audio call minutes	<ul style="list-style-type: none"> • Total duration of audio calls • Change in the duration of audio calls in the last 12 weeks.

Use the drop-down list to choose a time period for which to view metrics.

The following dashlets are available in the Technology Adoption dashboard:

Deployment Distribution by Endpoint Model

For Cisco Prime Collaboration Release 11.1 and earlier

This dashlet shows the deployment trend of the configured and active endpoints.

- All endpoints that are managed in Cisco Prime Collaboration Assurance, irrespective of their registration status are categorized as configured endpoints.
- Endpoints in Cisco Prime Collaboration Assurance which are either in registered or partially registered status are active endpoints.

By default, this dashlet will display the graph for all endpoints that were deployed from the date Cisco Prime Collaboration Assurance was installed till the current date. You can filter data based on weeks. If you select the time period as 7 days ago, the graph will display all the endpoints that were deployed from the day you installed Prime Collaboration till the current date (7 days ago).

As an example, you would be able to determine the rate of increase in addition/deployment of a specific endpoint model, say CTS 1000 series, over a period of time.



Note The **Duration** global filter is not applicable for this dashlet.

The device details (such as model number, version, and so on) are collected from Prime Collaboration inventory and also by polling the endpoints using SNMP or HTTP. This device information is stored in the Analytics

database and is used to group endpoints based on the model. The details thus collected are represented as pie chart.

You can filter deployment data on the detailed view based on endpoint type, endpoint model, device pool, cluster or location. You can also view the cumulative count for active and configured devices for a specific endpoint model.

For Cisco Jabber phones that are registered with Cisco VCS, the count of active and configured endpoints are same irrespective of their registration status. This is because, if the status of Cisco Jabber is unregistered, inventory immediately moves it to Deleted state. For the other phones (like soft client CSF, CUPC and so on) the device is moved to Deleted state only when the status remains to be unregistered for more than 24 hours.

Endpoints Deployment Summary

For Cisco Prime Collaboration Release 11.5 and later

This dashlet shows the deployment trend of the configured and active endpoints.

- All endpoints that are managed in Cisco Prime Collaboration Assurance, irrespective of their registration status are categorized as configured endpoints.
- Endpoints in Cisco Prime Collaboration Assurance which are either in registered or partially registered status are active endpoints.

By default, this dashlet will display the graph for all endpoints that were deployed from the date Cisco Prime Collaboration Assurance was installed till the current date. You can filter data based on weeks. If you select the time period as 7 days ago, the graph will display all the endpoints that were deployed from the day you installed Cisco Prime Collaboration Assurance till the current date (7 days ago).

As an example, you would be able to determine the rate of increase in addition/deployment of a specific endpoint model, say CTS 1000 series, over a period of time.



Note

The **Duration** global filter is not applicable for this dashlet.

The device details (such as model number, version, and so on) are collected from Cisco Prime Collaboration Assurance inventory and also by polling the endpoints using SNMP or HTTP. This device information is stored in the Analytics database and is used to group endpoints based on the model. The details thus collected are represented as pie chart.

You can filter deployment data on the detailed view based on endpoint type, endpoint model, device pool, cluster or location. You can also view the cumulative count for active and configured devices for a specific endpoint model.

For Cisco Jabber phones that are registered with Cisco VCS, the count of active and configured endpoints are same irrespective of their registration status. This is because, if the status of Cisco Jabber is unregistered, inventory immediately moves it to Deleted state. For the other phones (like soft client CSF, CUPC and so on) the device is moved to Deleted state only when the status remains to be unregistered for more than 24 hours.

Call Distribution by Endpoint Model

For Cisco Prime Collaboration Release 11.1 and earlier

This dashlet displays the call distribution based on call volume per endpoint model. You can view the details for the calls that are,

- Attempted-All calls, including the completed and failed.

- Completed-All the successful calls made from that endpoint model.
- Dropped-Non zero duration failed calls.
- Failed-All calls that failed.

The device details for this dashlet is collected from Prime Collaboration inventory and the call details are collected from Unified CM and Cisco VCS CDR.

You can filter the call distribution details in the detailed view page based on device pool, IP address, endpoint type, endpoint model, call type, call status, call direction, call count, call duration, cluster, user ID, or location.

The Cluster filter does not support Cisco VCS.

Call direction, in the above sentence means Incoming or Outgoing. It is determined based on the perspective of the endpoint or location making a call. For example, if an endpoint A calls endpoint B, it is an outgoing call from the perspective of endpoint A and incoming call from the perspective of endpoint B.

Call Volume by Endpoint Model

For Cisco Prime Collaboration Release 11.5 and later

This dashlet displays the call distribution based on call volume per endpoint model. You can view the details for the calls that are,

- Attempted-All calls, including the completed and failed.
- Completed-All the successful calls made from that endpoint model.
- Dropped-Non zero duration failed calls.
- Failed-All calls that failed.

The device details for this dashlet is collected from Prime Collaboration inventory and the call details are collected from Unified CM and Cisco VCS CDR.

You can filter the call distribution details in the detailed view page based on device pool, IP address, endpoint type, endpoint model, call type, call status, call direction, call count, call duration, cluster, user ID, or location.

The Cluster filter does not support Cisco VCS.

Call direction, in the above sentence means Incoming or Outgoing. It is determined based on the perspective of the endpoint or location making a call. For example, if an endpoint A calls endpoint B, it is an outgoing call from the perspective of endpoint A and incoming call from the perspective of endpoint B.

Call Distribution by Endpoint Types

For Cisco Prime Collaboration Release 11.1 and earlier

This dashlet displays the call distribution based on endpoint types-Audio endpoints and Video endpoints.

Audio endpoints are devices from which you can make and receive audio calls. Audio IP Phones, wireless IP Phones, and personal communication endpoints are categorized under Audio endpoints.

Video endpoints are devices from which you can make and receive the video calls. Multipurpose TelePresence, immersive TelePresence, personal TelePresence, mobile video and desktop video devices are categorized as Video endpoints.

For a list of Supported Audio and Video Endpoints in Cisco Prime Collaboration Assurance, see [Supported Devices for Cisco Prime Collaboration Assurance](#).

The device details for this dashlet is gathered from Prime Collaboration inventory and call details for this dashlet is obtained from Unified CM and Cisco VCS CDR.

You can filter the call distribution details in the detailed view page based on device pool, URI, directory number, IP address, endpoint type, endpoint model, call type, call status, call direction, call count, call duration, cluster, user ID, or location.

Call Volume by Endpoint Types

For Cisco Prime Collaboration Release 11.5 and later

This dashlet displays the call distribution based on endpoint types-Audio endpoints and Video endpoints.

Audio endpoints are devices from which you can make and receive audio calls. Audio IP Phones, wireless IP Phones, and personal communication endpoints are categorized under Audio endpoints.

Video endpoints are devices from which you can make and receive the video calls. Multipurpose TelePresence, immersive TelePresence, personal TelePresence, mobile video and desktop video devices are categorized as Video endpoints.

For a list of Supported Audio and Video Endpoints in Cisco Prime Collaboration Assurance, see [Supported Devices for Cisco Prime Collaboration Assurance](#).

The device details for this dashlet is gathered from Prime Collaboration inventory and call details for this dashlet is obtained from Unified CM and Cisco VCS CDR.

You can filter the call distribution details in the detailed view page based on device pool, URI, directory number, IP address, endpoint type, endpoint model, call type, call status, call direction, call count, call duration, cluster, user ID, or location.

Technology Usage

This dashlet shows the trend of audio and video usage. It shows the endpoint with maximum number of calls. You can view the data for each week in a graphical or tabular format. By default, data is displayed for the last 1 month.

The endpoints details for this dashlet is collected from Prime Collaboration inventory and the call details are collected from Unified CM and Cisco VCS CDR.

In detailed view, the formula used for calculating the percentage of the audio and video usage is:

Endpoint Count \geq number of calls per week with the same call status (failed/dropped/completed/attempted) / Device Count \geq number of calls per week (with the same model and call type) * 100.

You can filter the details in the detailed view page based on call type, URI, directory number, endpoint model, call status, usage status, location, device pool, cluster, user ID, or IP address.

Asset Usage

This dashboard helps you to track the asset usage. For example, it helps you to determine if endpoints have been effectively allocated and used, and so on.

Prerequisite : The endpoints registered to Unified CM and Cisco VCS should be discovered.

Data Source : The device details for this dashlet is collected from Prime Collaboration inventory and the call details are collected from Unified CM and Cisco VCS CDR.

The following dashlets are available in the Asset Usage dashboard:.

Least Used Endpoint Types

This dashlet displays the endpoint types that are least used, based on the number of calls made per week. By default, the dashlet displays only the unused endpoints (endpoints with no calls). The 'No more than X calls per week' category in the dashlet view includes, the unused endpoints and the endpoints with x calls per week.

This dashlet displays data for endpoints registered with Unified CM and VCS. Device details for this dashlet is collected from Prime Collaboration inventory and the call details are collected from CDR.

The detailed view displays only the data that is aggregated weekly. You can filter the data in the detailed view page based on endpoint type, endpoint model, usage status, device pool or location, user ID, or cluster.



Note The data displayed for the unused endpoints per week in the detailed view graph is not in synchronization with the Least Used Endpoint Types Report table in the detailed view. This is because Least Used Endpoint Types Report table shows aggregated data for the selected time filter. This is same as the dashlet view on Asset Usage.

Video TelePresence Rooms Utilization

You can track the most utilized and least utilized endpoints. This dashlet displays a list of Endpoint Names, Session Count, Used Duration, and Utilization for a week. You can filter the data by time period, endpoint type, and utilization percentage.

You can customize the number of working hours per day (by default, 8 hours) and working days per week (by default, 5 days) for each of the managed endpoints using **Change Utilization (Assurance Reports > Telepresence Endpoint Reports > Endpoint Utilization Report)**. These values are used while analyzing the asset usage for TelePresence Rooms.

You can launch the quick view if you rest the mouse over an endpoint name or utilization, which launches the graph and grid view consisting of number of sessions, duration, and utilization percentage.

In detailed analysis, you can filter the results displayed by time period, All Endpoints or a specific endpoint type, percentage or absolute values, individual or merged graphs. If you choose All Endpoints, you can also filter by utilization percentage.

No Show Video TelePresence Endpoint

You can identify endpoints that did not participate in the scheduled sessions. This dashlet displays the data based on the scheduled completed sessions. In this dashlet, you can view total scheduled sessions, scheduled sessions that have occurred, and No Show sessions- scheduled sessions that did not start and scheduled sessions completed but endpoints that were part of the scheduled session did not join (you can also view the data for this column in terms of percentage and absolute value). The endpoints with the no show count greater than zero are listed. You can filter the data by time period, endpoint type, and no show.

In detailed analysis, you can filter the data by time period, endpoint name, endpoint type, endpoint model, no shows (absolute and percentage), cluster, location, device pool to see the No Shows and No Shows percentage trend of endpoints. When you click on an endpoint legend, you can view endpoint model and type, show and no show count along with total scheduled sessions.



Note This dashlet is not supported in Cisco Prime Collaboration Analytics in MSP mode.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for No Show Video Telepresence Endpoint



Note

Ensure to enable Conference Diagnostics to populate the data.

The following are required for No Show Video Telepresence Endpoint:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the [Configure Devices for Cisco Prime Collaboration Assurance](#).
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 Service Pack 1.

No Show Video TelePresence Endpoint

For Cisco Prime Collaboration Release 11.1 and later

You can identify endpoints that did not participate in the scheduled sessions. This dashlet displays the data based on the scheduled completed sessions. In this dashlet, you can view total scheduled sessions, scheduled sessions that have occurred, and No Show sessions- scheduled sessions that did not start and scheduled sessions completed but endpoints that were part of the scheduled session did not join (you can also view the data for this column in terms of percentage and absolute value). The endpoints with the no show count greater than zero are listed. You can filter the data by time period, endpoint type, and no show.

In detailed analysis, you can filter the data by time period, endpoint name, endpoint type, endpoint model, no shows (absolute and percentage), cluster, location, device pool to see the No Shows and No Shows percentage trend of endpoints. When you click on an endpoint legend, you can view endpoint model and type, show and no show count along with total scheduled sessions.



Note

This dashlet is not supported in Cisco Prime Collaboration Analytics in MSP mode.

Traffic Analysis

The Traffic Analysis dashboard displays the technology usage by various users, departments, or business units in the organization. It helps you to plan and allocate business costs across various organizational units or departments.

Data Source : Call details of the dashlets in Traffic Analysis dashboard are obtained from CDR that the Cisco Unified Communications Manager generates.



Note In Detail View, the filters are based on Top N. In Bottom Table all the records are displayed based on other filter conditions selected in Detail View page. However, the database only holds raw data for 35 days. The Bottom Table displays the data accordingly.

The following dashlets are available in the Traffic Analysis dashboard:

Top N Callers

This dashlet lists the top N numbers from which calls originated, based on the total number of calls made from the directory number to any other number within the Prime Collaboration managed deployment.

You can filter the data displayed in the detailed view page based on directory number, call type, call count, call duration, cluster, location, device pool or endpoint details (such as IP, caller number, or source URI and so on). The directory numbers of those endpoints that are managed in the Prime Collaboration are displayed, the external directory numbers are not displayed.

You can view the number of calls or the duration of calls either in absolute or percentage mode. You can also view the users or directory numbers when you filter by endpoint or users respectively.

The formula used for calculating the percentage of top N callers is:

Total number of calls or the duration of calls for a particular number in a week / Total number of calls or duration of calls for all callers in that week * 100.

This dashlet displays data for endpoints registered with Unified CM and VCS.

Using the zoom selector graph displayed in the detailed view, you can adjust the pointer in the time window (x axis) of the graph to view details of the calls that were placed from that particular number, for the selected time period.

You can also view the top N callers for each individual cluster by using the global cluster filter.

Top N Dialed Numbers

This dashlet lists the Top N dialed numbers based on destination, for a specified time period. You can view the Top N numbers that were:

- Called the most number of times (call count)
- Engaged for the longest duration (call duration)

This dashlet displays data for endpoints registered with Unified CM and VCS.

You can filter the details displayed in the detailed view based on directory number, call type, call count, call duration, cluster, or location. The directory numbers of those endpoints that are managed in the Prime Collaboration are displayed, the external directory numbers are not displayed.

Top N Off-Net Traffic Locations

This dashlet displays the OffNet versus OnNet traffic trend per location.

You can filter the data displayed in the detailed view page based on off net or onnet traffic, call type, call count, call duration, cluster, location, device pool, endpoint details (such as IP, directory number, or source URI and so on), call direction, or user ID.

**Note**

You can also filter the data in the detailed view based on the call direction, such as, incoming or outgoing calls. Incoming calls are the calls received by the gateway from the CUCM, whereas the outgoing calls are the calls made from the gateway to the CUCM. So when you filter incoming calls, you must enter the endpoint details of the source or the caller and when you filter outgoing calls, you must enter the endpoint details of the callee or the destination.

When you filter data based on the endpoints the directory numbers of those endpoints that are managed in the Cisco Prime Collaboration Assurance are displayed, the external directory numbers are not displayed.

In dashlet view, the formula used to calculate the percentage of OnNet calls is:

Total number of OnNet calls in the location/ Total number of OffNet calls and OnNet calls in that location * 100

The formula used to calculate the percentage of OffNet calls is:

Total number of OffNet calls in the location/ Total number of OffNet calls and OnNet calls in that location * 100

The dashlet does not include the calls processed on Video Communication Server (VCS).

OffNet and OnNet Calls

Calls within the Cisco Unified CM (private network) are termed as OnNet calls. For example, a call from an internal cisco IP phone to another internal IP phone is an OnNet call. OnNet calls can be routed over intercluster trunks (ICT) or Session Initiation Protocol (SIP) trunks to integrate with remote Cisco Unified CM clusters or third-party SIP vendor equipment.

OffNet calls are normally the calls that are routed outside the private telephony system to the PSTN. Most OffNet calls are routed across gateways to the PSTN. A call can also be categorized as OffNet when at least one endpoint is a trunk or a gateway, and when one of the following holds good of the endpoint.

- The Call Classification parameter is set to OffNet in the gateway configuration or the trunk configuration in Unified Communications Manager (Administration).
- Call Classification parameter is set to System default in the gateway or trunk configuration.
- System default service parameter is set to OffNet.
- The endpoint is an analog gateway.

Any call that does not meet the criteria for an OffNet call is considered to be an OnNet call.

**Note**

By default, all route patterns and all calls to or from a gateway are classified as OffNet.

Top N Call Traffic Locations

This dashlet helps you to identify the top N locations that have highest number of calls, based on the call count or call duration.

You can filter the details in the detailed view based on location (both Top N and Bottom N), device pool (both Top N and Bottom N), IP Address, directory number, URI, call type, call status, call count, call duration, call direction, user ID, or cluster.



Note The dashlet displays call locations based on attempted calls only. Filters for the other statuses like completed, dropped, and failed calls are enabled in the detailed view.

In dashlet view, the formula used for calculating the percentage of the locations with highest number of calls is:

Total number of calls or duration of calls in a location / Total number of calls or duration of calls in all locations * 100.

Call Traffic Analysis

This dashlet displays the distribution of calls that belong to the following predefined call categories:

- External
- Internal
- Conference
- Emergency
- Long distance
- Toll free
- H 323 (Incoming and outgoing gateways/trunks) or MGCP (Incoming and outgoing gateways) or SIP (Incoming and outgoing trunks)
- Voicemail
- Local
- International

To add a call category, see section [Call Category Creation](#).



Note A call can be included in more than one call category; for example, an internal call can also be a conference call. Therefore, the sum of all calls that belong to all categories might be greater than the reported total number of calls.

This dashlet includes only the details for the calls processed on Unified CM. Call category information is collected from CDR.

In dashlet view, the formula used to calculate the percentage of the distribution of calls is:

Total number of calls or the duration of calls that belong to a specific traffic category / Total number of calls or duration of calls of all categories * 100.

In detailed view, the formula used to calculate the percentage of the distribution of calls is:

Total number of calls of a traffic type which belongs to one call status (failed, dropped, completed, attempted) / Total number of calls of a traffic type which belong to Attempted call status * 100.

You can filter the details in the Detailed View based on location, call type, call status, call count, call duration, call direction, user ID, or cluster.

Capacity Analysis

This dashboard displays the usage trends and available capacity of the key network resources. This information helps you to effectively plan for future capacity addition or dilution where needed.

For all the dashlets in Capacity Analysis dashboard, the data for the current day will be processed only on the following day. Therefore, the dashlets display the data for the current day as zero.

Data Source : The utilization data for this dashboard is obtained from the voice utilization polled data.

The quick view, dashlet view and the detailed view of these dashlets provide data for the time period for which the filter has been applied.

You can see the details of SIP Trunk types supported in the capacity analysis dashboard in the following table:

SIP Trunk Type	% Utilization Report		Busy-hour Trunk Traffic Report	
	Data Source	Support	Data Source	Support
SIP Trunk terminated at Cisco CUBE	Polling the CUBE directly	Available	CDR	Available
UCM logical SIP trunk (ICT, Trunk to WebEx, etc)	RTMT UCM SIP Performance Counter	NA	CDR	Available
SIP Trunk terminated at non-Cisco border element (ACME, etc)	RTMT UCM SIP Performance Counter	NA	CDR	Available

You can view the following dashlets from the Capacity Analysis dashboard:

Analytics Group Management

Prime Collaboration Analytics allows you to create custom groups for Trunks, Route Groups, and CAC Locations, based on your business needs. Click **Analytics Administration > Group Management**. Choose a group from the **Group Type** drop-down on the top-right. You can create new groups, modify the members of existing group, or remove a group.

For instance, all trunks in your network are displayed in the Analytics Group Management page. Select a trunk, under **All Trunks**, and add it to an existing group (Click **Add to Group**) or a new group (Click **Add New Group**).

After you create a group, the list of available groups are displayed under Trunk Groups in the left pane. These groups are also listed under **All Trunks** drop-down (in Trunk Utilization dashlet) of the Capacity Analysis dashboard

You can follow a similar approach for creating custom Route Groups and CAC Locations, the corresponding utilization thresholds are listed in the dashlets. When you apply a threshold, the results will be filtered based on threshold filter.

Use the **Settings** icon on the top-right corner to add or remove the columns displayed.



Note

- In MSP mode, the operator users do not have access to **Analytics Administration** menu, hence cannot create custom group.
- Group names can only be added or deleted, but cannot be edited.
- The trunk/route groups for Analytics Group Management and other dashlets in Prime Collaboration Analytics are imported from Prime Collaboration Assurance database, but the custom groups created in Prime Collaboration Analytics are not visible/used in Prime Collaboration Assurance.
- If you want to display the aggregated data in the Trunk/Route Group Utilization dashlet, you need to define the custom groups using **Monitor > Utilization Monitor > Route Group Utilization > RouteGroup Aggregation Settings**.
- If you want create custom groups for DSP, use **Device Inventory > Inventory Management > Create Group** (under Device Group).

Location CAC Bandwidth Utilization

Call Admission Control (CAC) enables you to control the audio and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link.

Audio and video quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control operates by rejecting a call when there is inadequate bandwidth and makes it a failed call.

It displays the location name, the number of calls that failed (calls that failed to establish due to lack of bandwidth), and the bandwidth used per location, as a percentage. By default, the table is sorted based on the Bandwidth Used.

The dashlet can be filtered based on utilization type as Peak and audio, video or immersive. By default, it displays the locations where bandwidth utilization has been peak for the last 28 days.

You can filter the details displayed in the detailed analysis based on WAN location, bandwidth used, utilization type, failed calls, or cluster. You can also filter the calls based on locations. Use the Select option to choose a location.

This dashlet will not include the details for the calls processed on VCS.

Trunk Utilization

This dashlet helps you to identify which trunks are the most heavily or least utilized. The utilization data for this dashlet is obtained from voice utilization polled data. This dashlet displays the maximum concurrent calls (configured data), concurrent calls (data used), trunk type, and the utilization in percentage for each trunk. It also includes the details for the calls processed on VCS.

Prerequisite :

- If you want to view the data for the custom trunk groups, you must define these groups using **Analytics Administration > Group Management**.
- You must configure the maximum capacity for SIP trunks for the SIP data to be populated in this dashlet. You can configure the maximum SIP capacity, by clicking **Missing Trunk?** on the top-left corner of the dashlet below the filters.

For other trunks, such as MGCP, inter-cluster and so on, the data is collected through polled data.

Busy-Hour Trunk Capacity

This dashlet helps you identify the trunks experiencing high average bouncing busy hour (ABBH) traffic. ABBH is calculated by analyzing the traffic load on a switching system during the peak hour of each day, over a certain period (typically one week), and then calculating the average for the time period.

Prerequisite : The maximum capacity for the CDR utilization trunks must be configured to see the available capacity in this dashlets. To configure maximum capacity for the CDR utilization trunks click **Missing Busy-Hour Trunk?** at the top left corner of the dashlet, below the filters.

You can also view the following capacity details of the trunk groups or route groups:

- Available Capacity
- Average Bouncing Busy Hour Traffic
- Maximum Bouncing Busy Hour Traffic

The maximum capacity required for a resource is calculated from the maximum BBH value, represented in erlangs. Maximum BBH is the maximum Bouncing Busy Hour value of a particular trunk for the selected time period. BBH is the peak value of that day.

The average capacity required is calculated from the ABBH value. Average capacity, here, means the minimum capacity required for a resource to maintain good traffic flow. ABBH is the average of all BBH values of a particular trunk or a route group for the selected time period.

**Note**

ABBH value will be calculated only for the working days, for the selected time period. For example, if you have specified the time period as one week, Analytics will first calculate the ABBH for seven days. The days that have BBH value less than 25 percentage of ABBH are considered as non-working days. Analytics ignores the non-working days and calculates the ABBH value for all the other days of that week.

By default, Analytics uses the Grade of Service (GOS) value as 0.01 to calculate the average required capacity and maximum required capacity. To calculate the average and maximum required capacity for a different GOS (for example, 0.1, 0.001 and so on), you must edit the gos.properties file. See [Editing the GOS Properties File](#) for details .

BBH of the current day is calculated only at the end of the day and you can see it only on the next day. There is no Inbound or Outbound traffic for ABBH. It is applicable only for BBH.

You can filter the details displayed in the detailed view based on trunk , traffic type, direction, bandwidth used, or cluster (this drop-down list is enabled only if you choose the Select option in the detailed view). When you select a cluster, all the devices for that cluster gets listed, regardless of whether the devices are maximum or least utilized.

You need to configure the maximum capacity for the CDR utilization trunks in order to see the available capacity in the dashlets. If the maximum capacity for the CDR trunks is not configured or zero, the data for these trunks will not be shown in the dashlet.

This dashlet will not include the details for the calls processed on VCS.

Calculating Erlang

An erlang is used to describe the total traffic volume of one hour. For example, If a group of users made 30 calls in one hour, and each call had an average call duration of 5 minutes, then the number of erlangs this represents is worked out as follows:

Minutes of traffic in the hour = number of calls x duration (30*5) = 150

Hours of traffic in the hour = 150/60 = 2.5

Therefore, the total traffic = 2.5 Erlangs.

Erlang traffic measurements are made in order to understand traffic patterns within your voice networks. It can also be used to work out the number of lines that will be required between a telephone system and a central office (PSTN exchange lines), or between multiple network locations.

Editing the GOS Properties File

Analytics uses the Grade of Service (GOS) value as 0.01 to calculate the average required capacity and maximum required capacity. To calculate the average and maximum required capacity for a different GOS (for example, 0.1, 0.001 and so on), you must edit the GOS properties file:

Step 1 Log in to the Prime Collaboration Assurance server with the administrator privilege.

Step 2 Open a new tab in browser and enter the URL this link
<https://<pc-server-ip>/emsam/applications/emsam/PCDiagnostics/fileEditor.jsp>.

Where, pc-service-ip is the Prime Collaboration Assurance server IP address.

Step 3 Choose the following:

- a) In the Location drop-down list, /opt/emms/emsam/advance_reporting/conf/.
- b) In the File Type drop-down list, properties.
- c) In the Files drop-down list, gos.properties.

Step 4 Click **Edit**.

Step 5 Edit the gos value and click **Save**.

Configuring Maximum Capacity for a Trunk or Gateway

To configure the maximum capacity for a trunk or gateway:



Note In MSP mode, the operator users do not have access to **Analytics Administration** menu, so you cannot configure the maximum capacity for a trunk or gateway.

Step 1 Choose **Analytics Administration > Trunk Traffic Max Capacity Settings** .

- Step 2** From the drop-down list, select the Cisco Unified CM cluster that you want to configure.
- Step 3** Select a gateway or trunk type.
- Step 4** Click **Configure Maximum Capacity** and make the appropriate entries.
- Step 5** Click **Apply**, and then click **Close**.

Importing Trunk Utilization Data for All Clusters

To import the trunk utilization data for all Cisco Unified CM clusters:



Note

In MSP mode, the operator users do not have access to **Analytics Administration** menu, so you cannot import the trunk utilization.

- Step 1** Choose **Analytics Administration > Trunk Traffic Max Capacity Settings**.
- Step 2** Click **Bulk Export**.
- Step 3** In the Export Trunk Configuration window, click **Export** to accept the default named export CSV file.
- Step 4** Open the CSV file and edit the data as needed.
- All the gateways and trunks will be listed in the file. You just need to enter the values in the file.
- Step 5** Click **Bulk Import**.
- Step 6** Browse to the location of the CSV file, and then click **Import**.

Route Group/Trunk Group Utilization

This dashlet helps you track route group utilization.

Prerequisite :

- To view the aggregated data, you must associate the trunks to a route group, by clicking **Missing Route Group/Trunk Group?** on the top-left corner of the dashlet below the filters..
- To view data for user-defined trunk groups, you must create custom groups, by clicking **Missing Route Group/Trunk Group?** on the top-left corner of the dashlet below the filters.
- For the SIP trunk data to be populated, you must configure the maximum capacity for SIP trunks, by clicking **Missing Route Group/Trunk Group?** on the top-left corner of the dashlet below the filters.. For other trunks, such as MGCP, inter-cluster and so on, the data is collected through polled data.
- If you want to view data for the custom groups, you must define these groups using **Analytics Administration > Group Management**.

This dashlet displays the aggregated data for trunk/route group. The utilization data for this dashlet is obtained from the voice utilization polled data. You can view maximum concurrent calls (configured data), concurrent calls (data used) and the utilization in percentage. You can also view the pattern of peak route group utilization over a period of months.

Busy-Hour Route-Group Capacity

This dashlet helps you identify the route groups experiencing high, average bouncing busy hour (ABBH) traffic. ABBH is calculated by analyzing the traffic load on a switching system during the peak hour of each day, over a certain period (typically one week), and then calculating the average for the time period.

Prerequisite : The maximum capacity for the CDR utilization trunks must be configured to see the available capacity in this dashlets. To configure maximum capacity for the CDR utilization trunks click **Missing Busy-Hour Route Group?** at the top left corner of the dashlet, below the filters.

You can also view the following capacity details of the trunk groups or route groups:

- Available Capacity
- Average Bouncing Busy Hour Traffic
- Maximum Bouncing Busy Hour Traffic

The maximum capacity required for a resource is calculated from the maximum BBH value, represented in erlangs. Maximum BBH is the maximum Bouncing Busy Hour value of a particular route group for the selected time period. BBH is the peak value of that day.

The average capacity required is calculated from the ABBH value. Average capacity, here, means the minimum capacity required for a resource to maintain good traffic flow. ABBH is the average of all BBH values of a particular route group for the selected time period.

**Note**

ABBH value will be calculated only for the working days, for the selected time period. For example, if you have specified the time period as one week, Analytics will first calculate the ABBH for seven days. The days that have BBH value less than 25 percentage of ABBH are considered as non-working days. Analytics ignores the non-working days and calculates the ABBH value for all the other days of that week.

By default, Analytics uses the Grade of Service value as 0.01 to calculate the average required capacity and maximum required capacity. To calculate the average and maximum required capacity for a different GOS (for example, 0.1, 0.001 and so on) you must edit the gos.properties file. See [Editing the GOS Properties File](#) for details .

BBH of the current day is calculated only at the end of the day and you can see it only on the next day. There is no Inbound or Outbound traffic for ABBH. It is applicable only for BBH.

In the detailed analysis page, you can filter the details displayed based on route group, traffic type, direction, bandwidth used, or cluster (this drop-down list is enabled only if you choose the Select option in the detailed view). When you select a cluster, all the devices for that cluster gets listed, regardless of whether the devices are maximum or least utilized.

In addition, you can view the traffic type and direction of the associated trunks for a route group when you select **Show Trunks**. The tabular view (pops up when the legend is clicked) also displays associated trunks details for a route group.

You need to configure the maximum capacity for the CDR utilization trunks in order to see the available capacity in the dashlets. If the maximum capacity for the CDR trunks is not configured or zero, the data for these trunks will not be shown in the dashlet.

To configure maximum capacity for CDR trunks, see [Configuring Maximum Capacity for a Trunk or Gateway, on page 451](#).

This dashlet will not include the details for the calls processed on VCS.

DSP Utilization

You can track DSP resource utilization, so that you can optimize its usage. In this dashlet, you can view the average and minimum DSP utilization for a gateway.

Prerequisite : The gateways must be discovered to populate data in this dashlet.

You can view the details of utilization based on the time period, through the Quick view (launched when you rest your mouse pointer on a value in the Gateway column).

In detailed analysis page, you can filter by custom group or DSP utilization, time period, MTP, Transcoder, cluster, and gateway. The tabular view (pops up when you click the legend) displays the peak, average and minimum DSP usage, and total number of channels used on an hourly basis.

You can create a DSP custom group either using the **Device Inventory** or from the DSP Detailed Analysis page. In the Detailed Analysis page, click **Save Results** after applying the required filter parameters. While creating the custom groups, you must ensure that the number of gateways selected must not exceed 100. You can edit or delete the custom groups from the Device Work Center page only.



Note

For Cisco Prime Collaboration Release 11.1 and earlier

In MSP mode, the operator user do not have the privilege to create custom group, hence the **Save Result** button is grayed out.

Service Experience

This dashboard helps you to analyze the service quality distribution and traffic trends based on number of calls, location, or call duration.

Prerequisite : The Call Measure Records(CMR) must provide either Mean Opinion Score (MOS) or Severely Concealed Seconds Ratio (SCSR) values.

Data Source : The device details for this dashlet is collected from Prime Collaboration inventory and the call quality details for this dashlet is obtained from CDR.

In addition to other filters in the detailed analysis view, for each dashlet of the Service Experience dashboard, you can also filter the results based on a selected user (specify the userid in the User field). The tabular view (pops-up when you click legends/series displayed below the slider, or when you double-click at any point on the graph) also has the user field. The same results, containing details of a selected user, can be also be exported.

Issue found:

Detail view page for "Users with Call Quality Issues" shows 'No data'.

Work around provided:



Note

You can find the Detail view page from Quick view shows data.

1. Login to Prime Collaboration Assurance server address 10.197.94.104 with the username *globaladmin* and password *Ecmbu!23*.
2. Go to 'Analytics -> Service Experience'

3. Observe the data available in 'Users with Call Quality Issues' dashlet
4. Click on 'See Details'.
5. Detail view page shows 'No data'.

Service Experience Distribution

For Cisco Prime Collaboration Release 11.1 and earlier

This dashlet displays the percentage distribution of calls that belong to the following predefined service categories:

- Good—The Severely Concealed Seconds Ratio (SCSR) value falls below the long call and short call SCSR threshold.
- Acceptable—The SCSR value exceeds or equals the long call and short call SCSR threshold.
- Poor—The SCSR value exceeds the long call and short call SCSR threshold.
- Grade Not Available—Occurs when the corresponding SCSR value is not available.

To configure threshold, see the Overview of Voice Call Grade Settings section in [Cisco Prime Collaboration Assurance Guide - Advanced](#).

In the dashlet view, you can select the chart to be displayed for:

- Graded calls— Good, Acceptable, and Poor calls
- Graded and Ungraded calls—Good, Acceptable, Poor, and Grade Not Available calls

By default, the dashlet view displays the chart for Graded calls.

You can filter the call quality data in the Detailed View based on the call type, call quality, device pool, directory number, IP address, URI, cluster, or location.

The device details for this dashlet are collected from Prime Collaboration inventory and the call quality details for this dashlet are obtained from CDR.

This dashlet includes only the details for the calls processed on Cisco Unified Communications Manager.

Call Quality Analysis

For Cisco Prime Collaboration Release 11.5 and later

This dashlet displays the percentage distribution of calls that belong to the following predefined service categories:

- Good—The Severely Concealed Seconds Ratio (SCSR) value falls below the long call and short call SCSR threshold.
- Acceptable—The SCSR value exceeds or equals the long call and short call SCSR threshold.
- Poor—The SCSR value exceeds the long call and short call SCSR threshold.
- Grade Not Available—Occurs when the corresponding SCSR value is not available.

To configure Thresholds, see Configuring Global Thresholds section in [Cisco Prime Collaboration Assurance Guide - Advanced](#).

In the dashlet view, you can select the chart to be displayed for:

- Graded calls— Good, Acceptable, and Poor calls
- Graded and Ungraded calls—Good, Acceptable, Poor, and Grade Not Available calls

By default, the dashlet view displays the chart for Graded calls.

You can filter the call quality data in the Detailed View based on the call type, call quality, device pool, directory number, IP address, URI, cluster, or location.

The device details for this dashlet are collected from Prime Collaboration inventory and the call quality details for this dashlet are obtained from CDR.

This dashlet includes only the details for the calls processed on Cisco Unified Communications Manager.

Endpoints with Service Quality Issues

For Cisco Prime Collaboration Release 11.1 and earlier

This dashlet lists the top N endpoint types and endpoint models that experience service quality issues. It shows the trend of acceptable and poor quality calls for all IP Phones except Cisco DX650, DX70, DX80, 88xx, and 78xx.

The device information details for this dashlet are gathered from Prime Collaboration inventory and the call quality information for this dashlet is obtained from CMR.

In dashlet view, the formula used for calculating the percentage of the acceptable and poor quality calls is:

Total number of Poor and Acceptable calls of an endpoint model or endpoint type / Total number of calls of same endpoint model or endpoint type * 100.

In detailed view, the formula used for calculating the percentage of the acceptable and poor quality calls is:

One type of call grade of an endpoint model or endpoint type / Total number calls of the same endpoint model or endpoint type * 100.

You can filter the details in the Detailed View based on endpoint type, endpoint model, call type, call grade, calculation (absolute or percentage), call count, call duration, cluster, location, device pool, IP Address, directory number, or URI.

This dashlet includes only the details for the calls processed on Cisco Unified Communications Manager.



Note

The call count data displayed in the detailed view graph will not be in synchronization with the data displayed in the Call Records table. This is because, the detailed view graph aggregates the data at the endpoint level (using CMR) but the Call Records table displays data at call details level (using CDR).

Endpoints with Call Quality Issues

For Cisco Prime Collaboration Release 11.5 and later

This dashlet lists the top N endpoint types and endpoint models that experience service quality issues. It shows the trend of acceptable and poor quality calls for all IP Phones except Cisco DX650, DX70, DX80, 88xx, and 78xx.

The device information details for this dashlet are gathered from Prime Collaboration inventory and the call quality information for this dashlet is obtained from CMR.

In dashlet view, the formula used for calculating the percentage of the acceptable and poor quality calls is:

Total number of Poor and Acceptable calls of an endpoint model or endpoint type / Total number of calls of same endpoint model or endpoint type * 100.

In detailed view, the formula used for calculating the percentage of the acceptable and poor quality calls is:

One type of call grade of an endpoint model or endpoint type / Total number calls of the same endpoint model or endpoint type * 100.

You can filter the details in the Detailed View based on endpoint type, endpoint model, call type, call grade, calculation (absolute or percentage), call count, call duration, cluster, location, device pool, IP Address, directory number, or URI.

This dashlet includes only the details for the calls processed on Cisco Unified Communications Manager.


Note

The call count data displayed in the detailed view graph will not be in synchronization with the data displayed in the Call Records table. This is because, the detailed view graph aggregates the data at the endpoint level (using CMR) but the Call Records table displays data at call details level (using CDR).

Top N Call Failure Locations

For Cisco Prime Collaboration Release 11.1 and earlier

This dashlet displays the top N locations that have highest number of failed calls (calls that failed to establish due to lack of bandwidth).

This dashlet displays the locations that have highest number of failed calls (calls that failed to establish due to lack of bandwidth). A call is considered good when each endpoint clears the call successfully.

The location information for this dashlet is collected from CDR.

You can filter the details in the Detailed View based on location, call type, call status, call count, call duration, call direction, or cluster.

You can view the Cause Code Analysis report that summarizes user-selected cause codes in the detailed view. Each slice of the pie chart corresponds to a cause code. To see the number of occurrences of the cause code and its percentage in the graph, place the cursor over a slice of the pie chart.

In dashlet view, the formula used to calculate the percentage of failed calls is:

Total number of failed calls in a location / Total number of calls in the same location * 100

This dashlet includes only the details for the calls processed on Cisco Unified Communications Manager.

In detailed view, the formula used for calculating the percentage of failed calls is:

Total number of calls or duration of calls of a particular call status (failed, dropped, completed, attempted / Total number of attempted calls or duration of calls in the same location, call type and call direction * 100

See section **Call termination cause codes** in [Cisco Unified Communications Manager Call Details Record Administration Guide](#) for the cause codes for failed calls.

Call Status For Locations

For Cisco Prime Collaboration Release 11.5 and later

This dashlet displays the locations that have highest number of failed calls (calls that failed to establish due to lack of bandwidth). A call is considered good when each endpoint clears the call successfully.

The location information for this dashlet is collected from CDR.

You can filter the details in the Detailed View based on location, call type, call status, call count, call duration, call direction, or cluster.

You can view the Cause Code Analysis report that summarizes user-selected cause codes in the detailed view. Each slice of the pie chart corresponds to a cause code. To see the number of occurrences of the cause code and its percentage in the graph, place the cursor over a slice of the pie chart.

In dashlet view, the formula used to calculate the percentage of failed calls is:

Total number of failed calls in a location / Total number of calls in the same location * 100

This dashlet includes only the details for the calls processed on Cisco Unified Communications Manager.

In detailed view, the formula used for calculating the percentage of failed calls is:

Total number of calls or duration of calls of a particular call status (failed, dropped, completed, attempted) / Total number of attempted calls or duration of calls in the same location, call type and call direction * 100

See section **Call termination cause codes** in [Cisco Unified Communications Manager Call Details Record Administration Guide](#) for the cause codes for failed calls.

Users with Service Quality Issues

For Cisco Prime Collaboration Release 11.1 and earlier

This dashlet lists the users who have experienced most service quality issues. It displays the trend of acceptable and poor audio and video call quality for users.

In the Detailed View, you can filter based on call type (audio or video), call grade (good, acceptable, poor), calculation (absolute or percentage), call count, call duration, cluster, location, device pool, endpoint IP Address, and user.

Users with Call Quality Issues

For Cisco Prime Collaboration Release 11.5 and later

This dashlet lists the users who have experienced most service quality issues. It displays the trend of acceptable and poor audio and video call quality for users.

In the Detailed View, you can filter based on call type (audio or video), call grade (good, acceptable, poor), calculation (absolute or percentage), call count, call duration, cluster, location, device pool, endpoint IP Address, and user.

Call Grade for Locations

For Cisco Prime Collaboration Release 11.5 and later

This dashlet lists the total number of poor, acceptable and good calls based on the location. You can also view the overall call experience where the poor calls are represented in red, acceptable calls in orange, good calls in green, and grade not available in yellow.

The location information for this dashlet is collected from the CDR.

You can view the detailed information of the call grade by clicking the **See Details** at the bottom-right corner of the dashlet. In the **Detailed Analysis** page, you can filter the call grade data based on the call type, call quality, call count, call duration, calculation (absolute or percentage), device pool, cluster, or location, and individual or merged graphs.

In the detailed view, the formula used for calculating the percentage is:

Total number of calls in a particular call grade(good, acceptable, poor or grade not available) / Total number of calls (good + acceptable + poor + grade not available) * 100

For Cisco Prime Collaboration Release 11.1 and earlier

You can also configure the threshold range for poor, acceptable and good calls from the **Detailed Analysis** page. To configure call grade threshold, click **Configure** in the **Detailed Analysis** page. For details about configuring the call grade threshold, refer the Overview of Voice Call Grade Settings section in [Cisco Prime Collaboration Assurance Guide - Advanced](#).

Video Conferences

For Cisco Prime Collaboration Release 11.1 and earlier

This dashboard displays the usage trends of the conference resources. This information helps you to effectively plan for future capacity addition or dilution where needed.

Prerequisite : The dashboard data is populated only if there are at least two video endpoints (Multipurpose, Immersive, or Personal TelePresences) in a conference.

This dashboard provides information on locations with highest number of conferences, conference duration (in minutes) and number of participants. The quick view, dashlet view and the detailed view of these dashlets provide data for a selected time period.

You can view the following dashlets from the Conferences dashboard:

Video Conference Analysis

For Cisco Prime Collaboration Release 11.5 and later

This dashboard displays the usage trends of the conference resources. This information helps you to effectively plan for future capacity addition or dilution where needed.

Prerequisite : The dashboard data is populated only if there are at least two video endpoints (Multipurpose, Immersive, or Personal TelePresences) in a conference.

This dashboard provides information on locations with highest number of conferences, conference duration (in minutes) and number of participants. The quick view, dashlet view and the detailed view of these dashlets provide data for a selected time period.

You can view the following dashlets from the Conferences dashboard:

Video Conference Statistics

You can analyze the conference calls in your site based on call type and call category.

This dashlet displays number of participants, conference count and duration based on call type (adhoc, scheduled) and call category (p2p, multisite and multipoint).

In the detailed view, you can filter based on conference, participants, and duration for conference type and conference category. You can customize your display based on number of participants per conference and duration per conference.



Note In MSP mode, you cannot filter the dashlet details based on the call type such as adhoc, scheduled and all filters.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Video Conference Statistics



Note Ensure to enable Conference Diagnostics to populate the data.

The following are required for Video Conference Statistics:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the [Configure Devices for Cisco Prime Collaboration Assurance](#).
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 Service Pack 1.

Top N Video Conference Locations

You can analyze the number of participants in conference calls and overall conference duration for every location. You can filter these data on call type (adhoc and scheduled) and call category (p2p, multisite and multipoint).

In the detailed view, you can filter based on locations with maximum or minimum conferences. You can view details on conference type (adhoc, scheduled), session type (P2P, Multi-Point, Multi-Site), and clusters within a location.

The Cluster filter does not support Cisco VCS.



Note In MSP mode, you cannot filter the dashlet details based on the call type such as adhoc, scheduled and all filters.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Top N Video Conference Locations

**Note**

Ensure to enable Conference Diagnostics to populate the data.

The following are required for Top N video Conference Locations:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the [Configure Devices for Cisco Prime Collaboration Assurance](#).
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 Service Pack 1.

Conferencing Devices Video Utilization

This dashlet helps you to track the utilization of conferencing devices.

Prerequisite :Conference bridges must be deployed and discovered in device work center.

It also:

- Provides statistics of the peak and average usage of video ports in conferencing devices over a given period of time.
- Helps you see the usage trends of the video ports configured in your network, and manage them better. Provides information on the maximum number of a video ports that is configured on a device and number of ports used.

You can filter the details in the detailed analysis, based on conferencing device, utilization, peak or average ports, utilization percentage, and the device types such as Multipoint Control Unit (MCU), Cisco TelePresence Multipoint Switch (CTMS), or TelePresence Server (TPS). You can also select a Conductor and device information for each device type (these drop-down lists are enabled only if you choose the Select option in the detailed view).

Only the peak and average ports usage filters are applicable in the dashlet, detailed view, and quick view.

Conductor Bridge Pool Utilization

For Cisco Prime Collaboration Release 11.5 and later

This dashlet displays the cumulative utilization of the conference bridges for each conductor pool in your network.

The dashlet displays the following details:

- Pool Name—Name of the conference bridge pool

- Video Ports/Screen License Utilization—Number of video ports/screen licenses currently in use
- Max Video Ports/Screen License Utilization—Number of video ports/screen licenses available.
- Utilization—Percentage of video ports utilized from maximum available video ports.
- Conference Bridge Type
- Conductor Name—Name of the conductor that manages the conference bridge pool.

You can filter the data based on the utilization type(peak and average) and utilization percentage.

You can also view detailed information of the devices by clicking the **See Details** link. In the detailed view, you can filter the details of all the devices or selected device based on device type, device, time period, peak or average utilization, utilization percentage and individual or merged graphs.

UC System Performance

This dashboard helps you analyze system performance, based on CPU and Memory for the UC applications. You can use these trends to determine UC applications that are consuming high CPU/memory consistently over a period of time.

Prerequisite : The endpoints registered to Unified CM and Cisco VCS should be discovered.

Data Source : The performance utilization details for this dashboard is obtained from RTMT polled data

The quick view, dashlet view and the detailed view of these dashlets provide data for the time period for which the filter has been applied.

The following dashlets are available:

CPU Utilization - This dashlet displays the CPU utilization data (as a percentage) in terms of peak, average, and minimum utilization, for each device.

Memory Utilization - This dashlet displays the total memory and used memory (peak, average, and minimum) in terms of MB terms. Also, it displays the memory utilization as a percentage in terms of peak, average, and minimum utilization.



Note

- These dashlets display a maximum of 25 rows at an instant.
- Also, they display data (peak, average, and minimum) as a sparkline trend for last 2 days.

License Usage

This dashboard helps you to track the license usage of applications such as Unified Contact Center Enterprise (UCCE) and Cisco Voice Portal (CVP).

Prerequisite : Contact Center Assurance License is required to populate data in the license usage dashboard.

Data Source : The license usage details for this dashboard are obtained from voice utilization polled data.

The following dashlets are available in License Usage dashboard:

Contact Center Enterprise

This dashlet displays the license usage of Unified Contact Center Enterprise.

The dashlet displays the following details:

- Device—Device name
- Capability—Capability of the device such as router or peripheral gateway
- Instance Name—Name of the instance
- Agents logged on—Number of contact center agents currently logged on

You can filter the data based on the utilization type such as peak and average. By default, the dashlet displays the list of devices with peak utilization for the last 14 days.

To launch a quick view of the device, click the information icon available against the respective device name. The quick view shows the number of agents logged on for a particular time period, in the form of graph or grid view.

You can also view detailed information of the devices by clicking the *See Details* link. In the detailed view, you can filter the details of all the devices or selected device based on time period, cluster, capability, device, peak or average utilization, and individual or merged graphs.

Customer Voice Portal

This dashlet displays the license usage of CVP call servers.

The dashlet displays the following details :

- Device—Device name.
- **For Cisco Prime Collaboration Release 11.1 and earlier**
Type—Device Type. For aggregated device, the device type is Multidevice.
- **For Cisco Prime Collaboration Release 11.5 and later**
Type—Device Type. For aggregated device, the device type is Device Group.
- Port in use—Number of port licenses currently in use.
- Max ports—Number of port licenses available for the processing of new calls. If there is any change in the ports utilized in the selected period, then minimum- maximum available port range is displayed.
- Utilization (%)—Percentage of ports utilized from maximum available ports.
- Port request denied—Number of port license checkout requests that were denied since the start of the system.

For Cisco Prime Collaboration Release 11.5 and later

You can view the aggregated license usage of multiple devices. For aggregating devices, see [Aggregating Devices](#).

You can filter the data based on the utilization type such as peak and average. By default, the dashlet displays the list of devices with peak utilization for the last 14 days.

To launch a quick view of the device, click the information icon available against the respective device. The quick view shows the ports in use and its utilization for a particular time period, in graph or grid view.

You can also view the detailed information of the devices by clicking the **See Details** link. In the detailed view, you can filter the details of all the devices, selected or aggregated devices based on time period, utilization range, clusters, devices, peak or average utilization, percentage or absolute values, and individual or merged graphs.

Aggregating Devices

For Cisco Prime Collaboration Release 11.5 and later

You can select multiple CVP devices, and view the aggregated license usage of these devices.

**Note**

You must have administrator privilege to perform this task.

To select the devices for aggregation:

Step 1 Click **CVP Aggregation Configuration** on the top left corner of **Customer Voice Portal** dashlet.

Step 2 In the **CVP Aggregation Configuration** page, based on the mode of deployment, do the following:

- In Enterprise mode, select the devices for aggregation as required.
- In MSP mode, you can aggregate devices for individual customers as follows:
 - a. Click the customer name. The devices associated with the customer are displayed.
 - b. From the displayed devices, select the required devices for aggregation.
 - c. Enter a name for the aggregated devices.

Step 3 Click **Save**.

You can find the aggregated device values populated in the **Customer Voice Portal** dashlet with the device type as **Device Group**.

My Dashboard

You can customize dashboards on **My Dashboard** page and add existing dashlets to it.

You can also do the following:

- Create new dashboards.
- Add existing dashlets.
- Move dashlets around a dashboard by dragging and dropping them.
- Edit and delete dashlets.
- Add global filters.
- Change layout template. By default, the layout template for **My Dashboard** is set as 100.

To add a new dashboard:

-
- Step 1** Click the Settings icon on the top-right corner of the **My Dashboard** page, and then click **Add New Dashboard**.
 - Step 2** Enter a name in the text box provided, and click **Apply**.
 - Step 3** Click **Add Dashlet(s)**.
 - Step 4** Click **Add** next to the dashlet you want to add.
-

Custom Report

The Prime Collaboration Analytics custom reports are based on the OLAP cube technique. When you select a report, you have the flexibility of choosing the required attributes and values to generate an analytics report.

The attributes include elements such as DialedNumber, Date, Time, Cluster, MeetingCategory, and so on; the values, which represents the numeric value includes count, duration, and so on. For detailed description on attributes and values for analytics cubes, see Prime Collaboration Analytics Custom Report – [Attributes and Values](#) page.

You can generate Analytics custom reports for:

Call Quality

- **Caller Call Status and Callee Call Status:** Displays call status, such as dropped, failed and so on for the originated or destination endpoint.
- **Caller Call Grade and Callee Call Grade:** Displays call quality data, such as No MOS, poor call, short call, and so on for the originated or destination endpoint. It also provides details on the call grades (using the CMR records) for the originated or destination EP.
- **Caller Call Class and Callee Call Class:** Displays call traffic types, such as external, internal, conference, and so on for the originated or endpoint information. It also provides the onnet and offnet call indicator.
- **Caller Call Cause Code and Callee Call Cause Code:** Displays call termination code, such as temporary failure (41), Destination out of order (27), no user responding (18), and so on for the originated or destination endpoint information.

Capacity Planning

- **Location CAC Bandwidth Utilization:** Displays CAC bandwidth usage details along with the number of calls failed because of less bandwidth.
- **Conferencing Devices Video Utilization:** Displays channel utilization for conferencing devices, such as Cisco MCU, Cisco TPS.
- **Busy-Hour Trunk Capacity:** Displays ABBH (Average Bouncing Busy Hour) data that are collected from the Unified CM CDR.
- **Utilization:** Trunk, DSP, MTP/Transcoder, Route Group and Trunk Group.

Conference

- Conference Locations: Displays conference details, such as conference category, count, and so on for endpoints.
- Conference Statistics: Displays conference details, such as participants count, duration and so on.

System Performance

CPU and memory utilization.

Creating Custom Reports

To create a custom report:

-
- Step 1** Choose **Analytics > Custom Report Generator**.
- Step 2** Choose a report from the Reports drop-down list.
- Step 3** From the Attributes and Values panes, choose the elements.

Double-click the Attributes element to view and select the required parameters.

The elements of a Attributes can be organized as a hierarchy, a set of parent-child relationships, where a parent member summarizes its children. Parent elements can further be aggregated as the children of another parent; for example, May 2014's parent is second Quarter 2014 which is in turn the child of Year 2014.

For network analysis or UC utilization related custom reports, if you have selected to view hourly data for over 13 months, the report may take a long time to generate. It is recommended to select hourly data for a time period less than 13 months.

- Step 4** Click **Save**.
-



Note Custom Report Generator is not supported in MSP mode.

You can view the generated report in chart or grid mode. You can export the report in PDF, MS Excel, PNG, and so on based on the view mode.

For the query that you have defined, you can view the corresponding query in the MDX language. MDX is a language for querying an OLAP cube. MDX is similar to SQL, but has added support for the multidimensional nature of cubes. For more details on the MDX query, see the [Mondrian Documentation](#). While writing the MDX query, you must use the attributes and values to generate the report; you can refer to the [Attributes and Values](#) page.

Scheduled Reports

This dashboard displays the list of entities (reports) that have been scheduled (when you click **Schedule Report** from the drop-down on the bottom-left of a dashlet). To view this dashboard, go to **Analytics > Scheduled Reports**.

You can view the report name, report type, frequency of the schedule, the filters that you have used while scheduling (displayed in **Filter Settings** when you click **Schedule Report** from the drop-down on the

bottom-left of a dashlet), the status indicating success/failure when the report was last generated, and next scheduled run time.

The top Metric panel displays data on the disk utilization, reports e-mailed and reports exported to SFTP server.

You can also suspend or resume a job (select a job and click Suspend/Resume). In case of errors, rest your mouse over a job to view the errors.

Also, you can add or remove the columns displayed, based on your business needs. To do this, click **Settings** icon available on the top-right corner of the page and rest your mouse on **Columns**.

To generate the report immediately:

- Click Run Now (at the end of the row of each report listed).
- Click the Run History (adjacent to Run Now) - shows the number of times the report has been run but the number of files listed are limited for the last 30/35 days only. List of reports that have been run are displayed.
- You can download a report or purge the selected report.



Note

- You cannot use Run Now on a report for which the schedule time has expired (reached end date).
- Clicking Run Now does not change the original schedule of the job (daily, weekly, and such).

For Cisco Prime Collaboration Release 11.6 and later

Concurrent Hourly Report (Top N Call Traffic Locations):

1. Launch PCA.
2. Click Analytics.
3. Click 'Traffic Analysis' from the drop down list.
4. Click 'See Details' on the right bottom, from the 'Top N Call Traffic Locations' dashlet to view the Detailed Analysis page.
5. Click 'Export' and then click on 'Scheduled Export' to generate Scheduled Reports dialogue box.
6. Check the box against '**check this to Schedule hourly reports for previous day**' to generate Concurrent Hourly Scheduled Reports which is available in the bottom of 'Scheduled reports' Dialogue box below the 'Filter Settings'.

If you do not check the Concurrent Call Hourly check box, then "Time period" in filter remains the same and so, the generated PDF will not have hourly data.

For Top N locations dashlet, when you select one-day interval, generated scheduled reports (PDF) is in a 'Bar Chart' manner. Grid/Table will have Concurrent hourly/ daily data. Bar chart/grids both are shown in the same PDF report generated from Top N locations dashlet.

Daily Report (Top N callers and Top N dialed numbers):

1. Launch PCA.
2. Click Analytics.

3. Click 'Traffic Analysis' from the drop down list.
4. From the 'Top N callers/Top N Dialed Numbers' Dashlet click ➞ (right bent arrow) which is in the bottom of Top N callers and Top N dialed numbers dashlets.
5. Click Scheduled Reports from the drop down menu to see the Scheduled Report window.
6. Click the check box against 'Check this to schedule daily report' to view daily reports.
Check this box to see the modified title and time period in the filters shown in Scheduled Reports.

Troubleshooting Prime Collaboration Analytics Dashboard

The following table has the details to troubleshoot data population in individual dashboard:

Table 72: Troubleshooting details for individual dashboard

Dashboards	Prerequisite	Data Source	Associated reports to confirm data collection
Asset Usage	Endpoints must be discovered.	CDR and Prime Collaboration Inventory	
Traffic Analysis		CDR	
Capacity Analysis	<ul style="list-style-type: none"> • Trunk Utilization: Configure maximum SIP trunk capacity, and define custom trunk groups . • Busy-Hour Trunk and Busy-Hour Route-Group Capacity: Maximum CDR trunk capacity must be configured. • Route Group/Trunk Group Utilization: Configure Maximum SIP trunk capacity, and define custom trunk groups, and Associate trunks to route group . • Conferencing Devices Video Utilization: Conference bridges must be deployed and discovered in device work center, and calls from any of these media resources (MCU, TPS, CTMS) must be present. • DSP Utilization: Gateways must be discovered. 	Voice Utilization Polled Data	Monitor > Utilization Monitor

Service Experience	CMR must provide MOS and SCSR grade details.	CDR and Prime Collaboration Inventory	Network Health Overview > Service Experience
For Cisco Prime Collaboration Release 11.1 and earlier Video Conferences For Cisco Prime Collaboration Release 11.5 and later Video Conference Analysis	<ul style="list-style-type: none"> At least two video endpoints in a conference must be available. Video Conference Statistics: Endpoints visibility must be set to Full (Inventory > Edit (under Current Inventory)) and session details must be polled. 		Diagnose > Conference Diagnostics



PART **VIII**

Perform Diagnostics

- [Diagnostics for Voice Endpoints, on page 473](#)
- [Troubleshooting Workflow for Video Endpoints, on page 527](#)
- [Media Path Analysis, on page 547](#)
- [Collect Logs, on page 551](#)
- [Analyze Call Signaling, on page 557](#)



CHAPTER 26

Diagnostics for Voice Endpoints

This section explains the following:

- [Diagnostics for Voice Endpoints, on page 473](#)

Diagnostics for Voice Endpoints

Cisco Prime Collaboration Assurance enables you to run multiple diagnostics tests to identify issues related to Unified Communications phone network.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can select the customers for which you want to see the test results. Use the global customer selection list on the top right of the user interface to select the customer(s) and then perform the test. The endpoints available to you to perform the tests will depend on the customers you have selected. In the test results, you can see the customer to which the device belongs to. In case you select or deselect customers from the global customer selection list after creating, importing or scheduling, or modifying any fields for the tests, the resultant changes will be visible when the page refreshes.

You can run the following diagnostics tests for voice endpoints:

Phone Status Test

Phone status testing uses Cisco IOS IP SLA technology to monitor the reachability of key phones in the network. Phone status testing is protocol-independent. You can perform tests on phones that operate under these protocols SCCP, and SIP. A phone status test consists of the following:

- A list of IP phones to test, selected by you.
- A testing schedule that you configure.
- IP SLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the IP phones. Optionally, it also pings from Cisco Prime Collaboration Assurance to the IP phones.

A phone is considered unreachable after there is no response to either an IP SLA-based ping, or a Cisco Prime Collaboration Assurance ping, and the phone status is unregistered in the phone status process. Cisco Prime Collaboration Assurance generates the PhoneReachabilityTestFailed event.

When a router is rebooted, the phone status tests are lost. However, Cisco Prime Collaboration Assurance reconfigures the test when the router becomes available. While the router is down, the Cisco Prime Collaboration Assurance ping continues to run, if you have enabled Cisco Prime Collaboration Assurance ping.

Phone status tests continue to run, except when phone information (IP address or extension number) changes and phone-related devices are not monitored by Cisco Prime Collaboration Assurance; update the seed file and add the test again.

You can create phone status tests by using the Create Phone Status Test page or by using a seed file. If you want to configure the test on the IP SLA-capable device closest to the new Cisco Unified CM, update the seed file and add the test again.



Note Before uninstalling Cisco Prime Collaboration Assurance, be sure to delete all the phone status tests from the application. If you do not delete these tests, they will continue to run on the router.

If you have managed IP SLA capable devices with SNMP V3 credentials, ensure that it has write permission to CISCO-RTTMON-MIB. The following are some of the sample commands:

```
snmp-server view .1.3.6.1.4.1.9.9.42 ciscoMgmt included
snmp-server group v3group1 v3 priv write .1.3.6.1.4.1.9.9.42
snmp-server user user1 v3group1 v3 auth sha Cisco123 priv aes 128 Cisco123
```



Note For more information, see respective IOS device configuration guides to view the exact commands.

Create a Phone Status Test

You can create phone status tests to monitor the reachability of key phones in the network.

To create a phone status test using the Create Phone Status Test page:

Before you begin

- You must be able to provide IP SLA-capable devices and IP phones (extensions and IP addresses) for testing.
- Phone status tests do not require information from Cisco Prime Collaboration Assurance device inventory. However, when Cisco Prime Collaboration Assurance monitors phone-related devices, it can update phone status tests whenever phone information changes.
- The source device for a phone status test must be monitored in Cisco Prime Collaboration Assurance.

Step 1 Choose **Synthetic Test Center > Phone Status Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests > Phone Status Test**.

Step 2 Click **Create**.

Step 3 In the Source pane, use the device selector to select a source device, or enter the device name (or IP address) in the Name field.

Step 4 Click **Add From Phone Report**.

- Step 5** In the Endpoint Diagnostic report page, check the check box next to the phones for which you want to add the test, and click **Add Phones**.
- Step 6** In the Run area of the Create Phone Status Test page, do the following:
- Schedule when to run the test.
 - Enter a name for the test.
 - Check the **Do not use ping from Cisco Prime Collaboration server** check box to disable ping from Cisco Prime Collaboration Assurance server.
- Step 7** Click **Save**.
- You can edit, view, and delete the phone tests from the Phone Status Test page.
-

Import Phone Status Test

You can create phone status test by importing a seed file with a list of extensions to include in the test.

Before you begin

- Verify that your seed file is formatted correctly. See [Format Phone Status Test Import File](#) for details on the seed file format.

To create a phone status test using a seed file:

- Step 1** Choose **Synthetic Test Center > Phone Status Test**.
- For Cisco Prime Collaboration Release 11.5 and later**
- Choose **Synthetic Tests > Phone Status Test**.
- Step 2** Click **Import**. Click **Browse** to add the seed file.
- Step 3** In the Run area, do the following:
- Schedule when to run the test.
 - Enter a name for the test.
 - Check the **Do not use ping from Cisco Prime Collaboration server** check box to disable ping from Cisco Prime Collaboration Assurance server.
- Step 4** Click **OK**.
-

Format Phone Status Test Import File

A phone status testing seed file should list all the phones that are to be tested. You can use a six-column or eight-column file format. The first six columns are the same for both file formats.

The information that you must provide for each phone is extension number, IP address, and MAC address. For:

- Shared lines—Enter one or both phones; Cisco Prime Collaboration Assurance can run one test for each phone on a shared line.
- Multiple extensions—Even if you enter multiple extensions for a phone, Cisco Prime Collaboration Assurance runs only one test for the phone.

Soft phones will display the device name in the MAC address fields.

You can use a six-column or eight-column file format. The first six columns are the same for both file formats. Each line of the seed file must contain:

- Six or eight columns. If a column is not used, you must enter a space.
- Colons separating the columns.

You must also provide the IP address and read and write community strings for the router closest to the Cisco Unified CM to which the phone is registered.

The following table shows the seed file format for testing the phone status.

Table 73: Seed File Format for Phone Status Testing

Column Number	Description
1	Phone extension.
2	Phone MAC address.
3	Phone IP address.
4	For Cisco Prime Collaboration Release 11.1 and earlier IP SLA-enabled device (router, switch, or voice router).
5	For Cisco Prime Collaboration Release 11.1 and earlier Read community string for the IP SLA-enabled device.
6	For Cisco Prime Collaboration Release 11.1 and earlier Write community string for the IP SLA-enabled device.
7	SNMPv3 username (used in the eight-column format only)
8	SNMPv3 password (used in the eight-column format only)

Examples

For Cisco Prime Collaboration Release 11.1 and earlier

Example 1: Phone Status Testing Six-Column Import File

```
[Extension]:[MAC Address]:[IPAddress]:[IPSLA Router]:[Read Community]:[Write community]
4000:2000000000001:172.20.121.1:10.76.34.194:private:private
```

The following example shows a sample eight-column import file.

Example 2: Phone Status Testing Eight-Column Import File

```
2) [Extension]:[MAC Address]:[IPAddress]:[SAA Router]:[Read Community]:[Write community]:
[snmpv3UserName]:[snmpv3Passwd]

#4000:2000000000001:172.20.121.1:10.76.34.194:!!{[NOVALUE]}!!{[NOVALUE]}!!:admin:admin
```

Synthetic Test

Synthetic tests are used to check the availability of voice applications. These tests verify whether the voice application can service requests from a user. For example, you can use synthetic tests to verify whether phones can register with a Cisco Unified CM. You can configure these test to run periodically.

Synthetic tests use synthetic phones to measure the availability of voice applications by emulating your actions. For example, a synthetic test places a call between clusters and then checks whether the call is successful.

Cisco Prime Collaboration Assurance monitor the information returned from the synthetic tests and generate events based on the results. If a synthetic test fails, Cisco Prime Collaboration Assurance generates a critical event. Such events are displayed in Event Browser.

Cisco Prime Collaboration Assurance supports synthetic testing for the following applications:

- Cisco Unified CM and Cisco Unified CM Express
- Cisco TFTP Server
- Cisco HTTP Server
- Cisco Emergency Responder
- Cisco Unity, Cisco Unity Express, and Cisco Unity Connection



Note

Creating synthetic tests with RTP transmissions in NATed environment is not supported.

The following table lists the synthetic tests and the results that each test must produce to pass.

Table 74: Synthetic Test Descriptions and Expected Results

Synthetic Test	Description	Expected Results
Phone Registration Test	Opens a connection with the Cisco Unified CM and registers a simulated IP phone.	Successful registration of the phone.

Synthetic Test	Description	Expected Results
Dial-Tone Test	Simulates an off-hook state to Cisco Unified CM and checks for receipt of a dial tone.	Receives a dial tone signal from Cisco Unified CM.
End-to-End Call Test	Initiates a call to a second simulated or real IP phone.	<ul style="list-style-type: none"> Registers, goes off-hook, and places the call Ring indication Destination phone goes off-hook to accept the call <p>If call progress tones and announcements are configured on the gateway for your end-to-end call, the test may succeed even before the phone rings or after a couple of rings. This indicates that your gateway is working correctly.</p>
TFTP Download Test	Performs a TFTP get-file operation on the TFTP server.	Successful download of a configuration file from the TFTP server.
For Cisco Prime Collaboration Release 11.6 and later HTTP Download Test	Performs an HTTP get-file operation on the HTTP server.	Successful download of a configuration file from the HTTP server.
Emergency Call Test	Initiates a call to the emergency number to test the dynamic routing of emergency calls.	<ul style="list-style-type: none"> All calls initiated Ring indication on Public Safety Answering Point (PSAP) and On Site Alert Number (OSAN), if configured.
Message-Waiting Indicator Test	<p>Calls the target phone and leaves a voice message in the voice mailbox.</p> <p>The destination phone for the Message-Waiting Indicator Test should be configured as Call Forward after X number of rings before moving to voicemail.</p> <p>If it is configured for Call Forward Always, the test will fail.</p>	Activation of the phone's message-waiting indicator. The message is then deleted and the message-waiting indicator is deactivated.

Prerequisites for Synthetic Tests

You can configure synthetic tests for each Cisco Unified Communications Manager and only for supported Cisco voice applications in your network. For each synthetic test, you must configure one or more phones in the related Cisco Unified Communications Manager or supported Cisco voice applications.

Follow these guidelines while creating synthetic tests:

- The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff and must be in the format 00059a3b7700.
- Create one phone extension number and one MAC address for each test and use it for that test only.
- Configure only one synthetic test per Cisco Unified CM.
- The SIP URI should be in the format sip:extn@ccm; for example, sip:7690@ct-sd.cisco.com.



Note You may use the following special characters in the extension: +, @, (.), (-), ?, \,], [, (-), !, X, ^, *, and #.

- Make sure that the combination of the phone extension number and the MAC address used in a test is unique across the voice cluster.
- Only Cisco 7960 IP Phones are simulated as synthetic endpoints in synthetic tests.
- If the synthetic phones are not preconfigured in Cisco Unified CM and Auto Registration is enabled, then the first execution of synthetic tests will fail but subsequent executions will work properly.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see [Supported Devices for Cisco Prime Collaboration Assurance](#) for 12.1 SP1.

See [Synthetic Test Worksheet](#) for list of worksheets that can help you in configuring applications and determining the number of phones for synthetic tests.

Create an Emergency Call Synthetic Test

For the target phones, the outgoing PSAP must use a local phone (not 911). Also, for the OSAN, use a synthetic phone only (do not use your local onsite security phone).



Note The Emergency Call synthetic test is supported on Cisco Emergency Responder 1.x and later.

To create an emergency call synthetic test:

Step 1 Choose **Synthetic Test Center > UC Application Synthetic Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests > UC Application Synthetic Test**.

Step 2 Click **Create**.

Step 3 From the Test Type drop-down menu, select **Emergency Call Test**.

Step 4 In the CER Parameters pane, do the following:

- Select the name or IP address of the system where Cisco Emergency Responder is installed.

You can use the Select Voice Application group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the **Cisco Emergency Responder** field.

- Enter the Emergency phone number.

Step 5 In the Caller pane, do the following:

- Select the name or IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express for the caller's phone.

You can use the Select Voice Application group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- Enter the synthetic phone's MAC address. If you used the group selector to choose the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system, the MAC address field is automatically populated.

Cisco Prime Collaboration Assurance verifies only that the MAC address number entered in the Create Synthetic Test page is syntactically valid. It is your responsibility to make sure the correct numbers are entered, as configured in the Cisco Unified Communications Manager. See [Prerequisites for Synthetic Tests](#), for MAC address limitations.

Step 6 In the PSAP pane, do the following:

- Select the Public Safety Answering Point (PSAP) Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

You can use the Select Voice Application group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- Enter the PSAP phone's MAC address.

Step 7 (Optional) If there is an On Site Alert Number (OSAN), select the **On Site Alert Number** check box, and enter the following in the OSAN pane:

- The name or IP address of the OSAN Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- The OSAN phone's MAC address.

Step 8 In the Run pane, name the test and configure when the test should run.

Note The test name that you enter in the Run pane cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 9 Click **Create**.

Create a Message-Waiting Indicator Synthetic Test

The following are the requirements for the target phones to run this test.

While creating the subscriber on Cisco Unity Connection that you are going to use for synthetic testing, configure the subscriber according to the following:

- The **Set subscriber for self-enrollment at next login** check box must be deselected, or you must use a real phone to dial into the Cisco Unity, device and complete the personalization process.
- Set the password option to Password never expires. The destination phone for the Message-Waiting Indicator Test should be configured as CALL FORWARD after X number of rings before moving to voicemail. If it is configured for CALL FORWARD ALWAYS, the test will fail.

This test is only supported on SCCP end-points. SIP endpoints are not supported for this test.



Note For Cisco Prime Collaboration Release 11.1 and earlier

After you perform a Cisco Unified CM version upgrade, Cisco Unity, synthetic tests that use the Cisco Unified CM that you upgraded might stop working. If this problem occurs, you should delete the Cisco Unity synthetic test, and then add the synthetic test again.

To create a message-waiting indicator synthetic test:

-
- Step 1** Choose **Synthetic Test Center > UC Application Synthetic Test**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Synthetic Tests > UC Application Synthetic Test**.
- Step 2** Click **Create**.
- Step 3** From the Test Type drop-down menu, select **Message-Waiting Indicator Test**.
- Step 4** In the Unity Parameters pane, enter the Cisco Unity, Cisco Unity Express, or Cisco Unity Connection system details.
- Step 5** Enter the appropriate information and click **Create**.
-

Create a TFTP Download Synthetic Test

You can configure only one TFTP download test for each Cisco Unified Communications Manager.

To create a TFTP download synthetic test:

-
- Step 1** Choose **Synthetic Test Center > UC Application Synthetic Test**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Synthetic Tests > UC Application Synthetic Test**.
- Step 2** Click **Create**.
- Step 3** From the Test Type drop-down menu, select **TFTP Download Test**.

- Step 4** From the Select Voice Application group selector, select the Cisco Unified CM or Cisco Unified CM Express for which you want to set up the test.
- Step 5** In the Run pane, name the test and schedule when to run the test.
- Note** The test name that you enter in the Run pane cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.
- Step 6** Click **Create**.

Create an HTTP Download Synthetic Test

For Cisco Prime Collaboration Release 11.6 and later

You can configure only one HTTP download test for each Cisco Unified Communications Manager.

To create an HTTP download synthetic test:

- Step 1** Choose **Synthetic Tests > UC Application Synthetic Test**.
- Step 2** Click **Create**.
- Step 3** From the Test Type drop-down list, select **HTTP Download Test**.
- Step 4** From the Select Voice Application group selector, select the Cisco Unified CM or Cisco Unified CM Express for which you want to set up the test.
- Step 5** In the Run pane, name the test and schedule when to run the test.
- Note** The test name that you enter in the Run pane cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.
- Enter the file name.
- Step 6** Click **Create**.

Create an End-to-End Call Synthetic Test

You have the option of configuring the target phone as a real phone or a synthetic phone. The default setting is a synthetic phone.

SIP-based end-to-end call tests that include a non-virtual destination phone with RTP enabled will not work under NAT/multiple end-customer environments. The test execute, but only the signaling portion passes. The RTP transmission will fail.

In this instance, the test is run to a real phone with the Enable RTP transmission option selected. The End-to-End Call Test is unable to do media transmission to a phone in a NAT environment.



- Note** Do not create more than 100 end-to-end call tests that run at 1-minute intervals. Configure any additional end-to-end call tests to run at various intervals greater than 1 minute.

To create an end-to-end call synthetic test:

-
- Step 1** Choose **Synthetic Test Center > UC Application Synthetic Test**.
For Cisco Prime Collaboration Release 11.5 and later
Choose **Synthetic Tests > UC Application Synthetic Test**.
- Step 2** Click **Create**.
- Step 3** From the Test Type drop-down menu, select **End-to-End Call Test**.
- Step 4** In the Caller pane, do the following: (Depending on the type of phone you select, some selections might become unavailable.)
- Enter the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system.
You can use the Select Voice Application group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.
 - Enter the synthetic phone's MAC address.
If you used the group selector to choose the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system, the MAC address field is automatically populated.
See [Prerequisites for Synthetic Tests](#) for MAC address limitations.
 - Select a protocol type.
 - Select a parameter type:
 - If you select Extension, enter the extension for the phone.
 - If you select SIP URI, enter the SIP Uniform Resource Identifier (SIP URI). The SIP URI should be in the format sip:extn@ccm; for example, sip:7690@ct-sd.cisco.com.
- Note** You may use the following special characters in the extension: +, @, (.), (-), ?, \,], [, (-), !, X, ^, *, and #.
- Step 5** In the Recipient pane, do the following:
- Select either the Synthetic Phone or Real Phone radio button.
 - Enter the name or IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system (if you selected the Real Phone radio button, this option is grayed out).
You can use the Select Voice Application group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.
 - Enter the phone's MAC address (if you selected the Real Phone radio button, this option is grayed out).
 - Select a protocol type (if you selected the Real Phone radio button, this option is grayed out).
 - Select a parameter type (if you selected the Real Phone radio button, this option is grayed out): If you select Extension, enter the extension for the phone. If you select SIP URI, enter the URI.
The Parameters area is grayed out when Synthetic Phone is selected.
- Step 6** In the Parameters pane, do the following:
- (Optional) Select Wait for Answer. If you selected the Synthetic Phone radio button, this option is grayed out.
 - (Optional) Select Enable RTP transmission. If you selected the Synthetic Phone radio button, this option is grayed out.
 - Choose a criterion for success, either Call Success or Call Failure.

- If desired, you can change the call setup time threshold setting (default is 10000 milliseconds).

The call setup time threshold measures the time between when you are done dialing the number to when the Cisco Unified Communications Manager sets up the call (using SIP or SCCP phones). If the threshold is exceeded, a warning event is generated.

Step 7 In the Run pane, name the test and schedule when the test should run.

Note The test name that you enter in the Run pane cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 8 Click **Create**.

Note The synthetic phone as well as the recipient phone can operate under either SCCP or SIP protocols.

Create Dial-Tone Synthetic Tests

To create a dial-tone synthetic test:

Step 1 Choose **Synthetic Test Center > UC Application Synthetic Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests > UC Application Synthetic Test**.

Step 2 Click **Create**.

Step 3 From the Test Type drop-down menu, select **Dial-Tone Test**.

Step 4 From the Select Voice Application group selector, select the Cisco Unified CM or Cisco Unified CM Express system for which you want to set up the test.

Step 5 Enter the synthetic phone's MAC address. See [Prerequisites for Synthetic Tests](#) for MAC address limitations.

If desired, you can change the dial-tone time threshold setting (default is 500 milliseconds).

The dial-tone time threshold measures the time between when an SCCP phone goes offhook to when it receives a dial tone from Cisco Unified CM. If the threshold is exceeded, a warning event is generated.

Step 6 In the Run pane, name the test and schedule when to run the test.

Note The test name that you enter in the Run pane cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 7 Click **Create**.

Note Dial-tone synthetic test supports only SCCP endpoints. SIP endpoints are not supported for this test.

Create a Phone Registration Test

To create a phone registration test:

Step 1 Choose **Synthetic Test Center > UC Application Synthetic Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests > UC Application Synthetic Test**.

- Step 2** Click **Create**.
- Step 3** From the Test Type drop-down list, select **Phone Registration Test**.
- Step 4** From the Select Voice Application group selector, select the Cisco Unified CM or Cisco Unified CM Express for which you want to set up the test.
- Step 5** Enter the synthetic phone's MAC address. See [Prerequisites for Synthetic Tests](#) for MAC address limitations.
- Step 6** Select a protocol and parameter type.
- If you select Extension, enter the extension for the phone.
 - If you select SIP URI, enter the SIP Uniform Resource Identifier (SIP URI). The SIP URI should be in the format sip:extn@ccm; for example, sip:7690@ct-sd.cisco.com.
- Step 7** Select a criteria for success (Registration Success or Registration Failure).
- If desired, you can change the registration time threshold setting (default is 2000 milliseconds). The phone registration threshold measures the time that it takes for a phone (SIP or SCCP phone) to register with a Cisco Unified CM. If the threshold is exceeded, a warning event is generated.
- Step 8** In the Run pane, name the test and schedule when to run the test.
- Note** The test name that you enter in the Run pane cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.
- Step 9** Click **Create**.
-

Import Synthetic Tests

You can import multiple synthetic tests at one time by using a comma-separated values (CSV) file.

To import synthetic tests:

Before you begin

- Verify that your seed file is formatted correctly. For details, see [Format Synthetic Test Import Files](#).

-
- Step 1** Choose **Synthetic Test Center > UC Application Synthetic Test**.
- For Cisco Prime Collaboration Release 11.5 and later**
- Choose **Synthetic Tests > UC Application Synthetic Test**.
- Step 2** Click **Import**.
- Step 3** In the Import Synthetic Test page, browse to the seed file, and click **OK**.
- The scheduled time and day for a synthetic test is configured in the import file. If you want to run a synthetic test on demand, you can use the Run Now button.
-

Format Synthetic Test Import Files

The general format for a synthetic test seed file is as follows:

- If you create the import file manually, the import file should have plain text content (Comma, AND, OR, Pipe separated) without header.
- All values must be separated with a vertical bar (|).
- The schedule column must use the following formatting:

MONTH, DAYSOFTMONTH, DAYSOFTWEEK, HOUR, MINUTE

- Month—0-11
- Day of month—1-31
- Day of week—0-6 (0 = sunday)
- Day of week—0-6 (0 = sunday)
- Minute—0-59

Each specifier can be a number, a range, comma-separated numbers and a range, or an asterisk.

Month and days of the month fields cannot be changed. You should enter an asterisk (*).

Day of week can have an asterisk to represent all days, or it can have a comma-separated list of days. For Hour, you can enter an asterisk to represent 24 hours, or you can enter a range. Minute can be an asterisk, to represent all, or it can be a range.

Day of week can have an asterisk to represent all days, or it can have a comma-separated list of days. For Hour, you can enter an asterisk to represent 24 hours, or you can enter a range. Minute can be an asterisk, to represent all, or it can be a range.

Only the following schedule types are supported:

- *,*,*,*,* —All days, 24 hours
- *,*,2-4,*,* —Tuesday to Thursday, 24 hours
- *,*,*,8-20,* —All days between 8:00 a.m. and 8:00 p.m
- *,*,*,8;20-59:*,*,*,9-19:*,*,*,20;0-40 —All days between 8:20 a.m. and 8:40 p.m.

Phone Registration Tests

Phone Registration Test Seed File Format

REGISTRATION|TestName|PollInterval|Schedule|CCMAddress|MACAddress|SrcPhoneProtocol|SIPURI_OR_EXTN

Phone Registration Test Example

REGISTRATION|reg test|60|*,*,*,*,*|ipif-skate.cisco.com|00059A3B7780|SCCP|4002

Table 75: Import File Format for Phone Registration Tests

Column Number	Description
1	Type of test—REGISTRATION
2	Test name
3	Polling interval
4	Schedule
5	Cisco Unified CM to which the phone is connected
6	Phone's MAC address. See Prerequisites for Synthetic Tests , for information on MAC details
7	Phone's protocol (SCCP or SIP)
8	SIP URI or extension number
9	Customer name

Dial-tone Tests

Dial-tone Test Seed File Format

OFFHOOK|TestName|PollInterval|Schedule|CCMAddress|MACAddress

Dial-tone Test Example

OFFHOOK|dial-tone|60|*;*;*;*;*|ipif-skate.cisco.com|00059A3B7781

Table 76: Import File Format for Dial-tone Tests

Column Number	Description
1	Type of test—DIALTONE/OFFHOOK
2	Test name
3	Polling interval
4	Schedule
5	Cisco Unified CM to which the phone is connected
6	Phone's MAC address. See Prerequisites for Synthetic Tests , for information on MAC details.
7	Customer name

End-to-End Call Test

End-to-End Call Test Seed File Format

```
ENDTOENDTEST|TestName|PollInterval|Schedule|SrcCCM|SrcMAC|isDestRealPhone|DestCCM|DestMAC|Extn|
WaitForAnswer|EnableRTP|SrcPhoneProtocol|SRC_SIPURI_OR_EXTN|DestPhoneProtocol
```

End-to-End Call Test Example

```
ENDTOENDTEST|endtoend test|60|*;*;*;*|ipif-skate.cisco.com|00059A3B7782|FALSE
|ipif-skate.cisco.com|00059A3B7783|4002|TRUE|FALSE|SCCP|4004|SCCP
```

Table 77: Import File Format for End-to-End Call Tests

Column Number	Description
1	Type of test—ENDTOENDTEST
2	Test name
3	Polling interval
4	Schedule
5	Caller Cisco Unified CM
6	Caller MAC address. See Prerequisites for Synthetic Tests , for information on MAC details.
7	Whether or not the recipient phone is a real phone. Enter true or false.
8	Recipient Cisco Unified CM
9	Recipient MAC address. See Prerequisites for Synthetic Tests , for information on MAC details.
10	Recipient extension number
11	Wait for answer. Enter true or false
12	Enable RTP transmission. Enter true or false
13	Phone's protocol (SCCP or SIP)
14	SIP URI or extension number
15	Destinations phone's protocol (SCCP or SIP)
16	Customer name

TFTP Download Test

TFTP Download Test Seed File Format

```
TFTP test format: TFTP|TestName|PollInterval|Schedule|CCMAddress
```

TFTP Download Test Example

```
TFTP|tftp download|60|*;*;*;*|ipif-skate.cisco.com
```

Table 78: Import File Format for TFTP Download Tests

Column Number	Description
1	Type of test—TFTP
2	Test name
3	Polling interval
4	Schedule
5	Cisco Unified CM
6	Customer name

For Cisco Prime Collaboration Release 11.6 and later

HTTP Download Test

HTTP Download Test Seed File Format

HTTP test format: HTTP|TestName|PollInterval|Schedule|CCMAAddress|PhoneConfigurationFileName

HTTP Download Test Example

HTTP|HTTP Download Test|60|*;*;*;*|10.78.86.158|SEPDefault.cnf

Table 79: Import File Format for HTTP Download Tests

Column Number	Description
1	Type of test—HTTP
2	Test name
3	Polling interval
4	Schedule
5	Cisco Unified CM
6	Phone configuration file name

Message-Waiting Indicator Test

Message-Waiting Indicator Test Seed File Format

MWITEST|TestName|PollInterval|Schedule|UnityAddress|SrcCCM|SrcMAC|DestCCM|DestMAC|Extn|Password

Message-Waiting Indicator Test Example

MWITEST|mwi test|300|*;*;*;*|10.76.91.155|10.76.91.148|00059A3B7B00|10.76.91.148
|00059A3B7B01|71418001|13579

Table 80: Import File Format for Message-Waiting Indicator Tests

Column Number	Description
1	Type of test—MWITEST
2	Test name
3	Polling interval
4	Schedule
5	Cisco Unity system
6	Caller Cisco Unified CM
7	Caller MAC address. See Prerequisites for Synthetic Tests , for information on MAC details.
8	Recipient Cisco Unified CM
9	Recipient MAC address. See Prerequisites for Synthetic Tests , for information on MAC details.
10	Recipient extension number
11	Recipient voicemail password
12	Customer name

Emergency Call Test

Emergency Call Test Seed File Format

EMERGENCYCALLTEST|TestName|PollInterval|Schedule|CERAddress|SrcCCM|SrcMAC|PsapCCM|PsapMAC|EmergencyNumber|enableOsan|OsanCCM|OsanMAC

Emergency Call Test Example

EMERGENCYCALLTEST|emergency call test|600|*;*;*;*|10.76.35.211|10.76.93.75|00059A3B7789|10.76.93.75|00059A3B7790|911|TRUE|10.76.38.111|00059A3B7791

Table 81: Emergency Call Test Tests

Column Number	Description
1	Type of test—CCCTEST
2	Test name
3	Polling interval
4	Schedule

Column Number	Description
5	Cisco Emergency Responder system
6	Caller Cisco Unified CM
7	Caller MAC address. See Prerequisites for Synthetic Tests , for information on MAC details.
8	Public Safety Answering Point (PSAP) Cisco Unified Communications Manager
9	PSAP MAC address. See Prerequisites for Synthetic Tests , for information on MAC details.
10	Emergency number
11	Enable On Site Alert Number (OSAN). Enter true or false.
12	OSAN Cisco Unified CM
13	OSAN MAC address
14	Customer name

Manage Synthetic Tests

The following table describes the tasks that you can perform from the Synthetic Tests page.

Tasks	Description
Export Synthetic tests	You can export the synthetic tests that you have created to a file on your Cisco Prime Collaboration Assurance server. If needed, you can use this file to import your configured synthetic tests back into Cisco Prime Collaboration Assurance, or to import the tests into another Cisco Prime Collaboration Assurance system.
Edit Synthetic tests	<p>Every time you create or edit a test that requires a phone extension number and a MAC address, you should edit them as a pair. Do not edit one independently of the other.</p> <p>While editing the Synthetic test, if you get an error message stating that the MAC address is already in use, then delete the Synthetic test and add the test back with the same MAC address.</p>
View Synthetic test details	<p>In the Synthetic Test Details page you can view the parameters that have been configured for a test.</p> <p>The details displayed vary depending on the type of test.</p>
Start and stop Synthetic tests	Synthetic tests can be started or stopped. You can select multiple tests at one time to start or stop. If a test is running while you are trying to stop it, a message appears stating the test's details.

Tasks	Description
View Synthetic test results	<p>The results are displayed in a report format. As with any of the reports in Cisco Prime Collaboration Assurance, you can print the report or export it to a file.</p> <p>The Synthetic Tests Results report provides the following information:</p> <ul style="list-style-type: none"> • The Test status (passed or failed). • The day and time that the test finished. • Any error messages.
Schedule Synthetic tests	<p>When you create a synthetic test, you have the option of running the test now, or scheduling the test to run at regular intervals.</p> <p>If you want to change the time at which the test should run, you must edit the synthetic test in the Edit Synthetic Test page.</p> <p>If the system time of the Cisco Prime Collaboration Assurance server is changed backward, the synthetic tests will not execute until the time has elapsed and the system time reaches the original time at which the change was done.</p> <p>For example, if at 10:00 a.m. the system time is changed to 9:00 a.m., the tests will not start executing until the system time is 10:00 a.m.</p> <p>Your login determines whether or not you can perform this task.</p>

Synthetic Test Notes

The following table contains information you should be aware of while creating synthetic tests:

Summary	Explanation
Synthetic tests do not run for 30 minutes after the Cisco Prime Collaboration Assurance processes are started. However, during this time, you can still create, edit, or delete tests.	Starting Cisco Prime Collaboration Assurance processes places a high load on the system. To prevent synthetic tests from failing during this time, Cisco Prime Collaboration Assurance delays starting them.
<p>Synthetic tests may either be skipped or take an extended period of time to run if the server CPU RAM reaches 85%.</p> <p>This anomaly will be reflected in the portlets.</p>	<p>Whenever the server CPU is greater than 85%, synthetic tests are either skipped or would take more time for execution.</p> <p>Therefore, the portlet data about these tests will reflect a lesser number of tests executed than scheduled per hour. To avoid this situation, schedule tests during off-peak hours.</p>

Summary	Explanation
When the interval of a synthetic test is decreased from a high value to a low value, the first results for the new value may take longer than the new interval to report.	Each synthetic test executes at a time that is controlled by its interval setting. Immediately after you decrease the interval setting for a synthetic test, that transaction might not run until the time elapsed is longer than the new interval. For example, if you decrease an interval from 180 seconds to 60 seconds, the first results for the new interval may take as long as 240 seconds to report.
One-time synthetic test failures sometimes occur.	Occasionally, one-time synthetic test failures occur. Such failures can be due to high loads on the Cisco Prime Collaboration Assurance or other factors that cause Cisco Prime Collaboration Assurance to be unable to receive some events from applications.
Cisco Unity message-waiting indicator synthetic tests may fail.	If a Cisco Unity Connection synthetic test fails and the Message-Waiting Indicator light is on, you must configure a real phone with the same extension number used in the test and delete the voicemails manually. Alternatively, you can use the Message Store Manager tool to remove the voicemails. After this is completed, the test will pass.
End-to-end call test may fail in NAT environment.	The end-to-end call synthetic test is not supported when phones are in a NAT environment. In this instance, the test is to a real phone with the Enable RTP transmission option selected. The end-to-end call synthetic test is unable to do media transmission to a phone in a NAT environment.

IP SLA Voice Tests

IP SLA Voice tests monitor the response time and availability of multiprotocol networks on both end-to-end and hop-by-hop basis. After collecting this data, you can use the Cisco Prime Collaboration Assurance graphing function to examine changes in network performance metrics. You can select, display, and chart network performance data in real time. To understand and deploy the IP SLA on your network devices, see the [IP Service Level Agreements \(IP SLAs\)](#) technology page on Cisco.com.

Prerequisites:

- You must configure Cisco IOS IP SLAs Source and Responder in your network.
- Verify whether the IPSLA responder feature is enabled on the device using Cisco Prime Collaboration Assurance Inventory.
- Ensure that the read-write community string of SNMP credentials is enabled when you configure IP SLA voice tests.

IP SLA Voice tests can be configured to trigger events when certain thresholds are crossed.

You can create IP SLA Voice tests one at a time, or import a file to create more than one test at a time.

You can create the following IP SLA Voice tests:

Test Name	Description
UDP Jitter for VoIP	<p>Starting Cisco Prime Collaboration Assurance processes places a high load on the system. To prevent synthetic tests from failing during this time, Cisco Prime Collaboration Assurance delays starting them.</p> <p>Measures packet loss, round-trip latency, and delay variance (or jitter) in IP networks by generating synthetic UDP traffic.</p> <p>This test uses the UDP protocol to measure latency, one-way jitter, and packet drop. Jitter is interpacket delay. The source device sends a number of packets from the source device to the destination device with a specified interpacket delay.</p> <p>The destination (an IP SLA Responder) time stamps the packet and sends it back. Using this data, the one-way positive and negative jitter (from the source to the destination and back again), packet loss (also from the source to the destination and back again), and round-trip latency are obtained.</p> <p>Positive jitter occurs when the one-way delay for a packet is longer than the previous packet delay. Negative jitter occurs when the one-way delay for a packet is shorter than the previous packet delay. If the sequence numbers become jumbled, the test reflects the error.</p>
Ping Echo	<p>Measures end-to-end response time between a source device and any IP-enabled device.</p> <p>The test sends ICMP packets from the source device to the destination device and measures the time it takes to complete the round trip.</p>
Ping Path Echo	<p>Measures hop-by-hop response time between a source device and any IP device on the network by discovering the path using traceroute, and then measuring response time between the source device and each hop in the path.</p> <p>Note If you want to change the Round-Trip Response Time threshold, in the Thresholds pane, select the check box and enter a new setting (default is 300 m/secs). The setting must be a positive integer (32 bit).</p>
UDP Echo	<p>Measures UDP response time between a source device and any IP-enabled device.</p> <p>The UDP echo test sends a packet with the configured number of bytes to the destination with the specified port number and measures the response time.</p> <p>There are two destination device types for the UDP echo operation: RTR Responders, which use IP SLA, and UDP servers, which do not.</p>

Test Name	Description
Gatekeeper Registration Delay	<p>Measures the time required for a gateway to register with a gatekeeper.</p> <p>This test sends a lightweight Registration Request (RRQ) from an H.323 gateway to an H.323 gatekeeper and receives a Registration Confirmation (RCF) from the gatekeeper. The test then measures the response time.</p> <p>For the Gatekeeper Registration Delay test to run, the source gateway must have SIP or H323 configured on it.</p>
Real-Time Transport Protocol	<p>Measures voice quality metrics from DSP to DSP by integrating with the DSP software. The operation involves placing a test call from the source gateway to the destination, sending actual RTP packets and then collecting statistics from DSPs.</p> <p>This test provides DSP-to-DSP measurement of voice quality metrics by integrating with the DSP software. Test calls are placed from the source gateway to the destination gateway, sending actual real-time protocol (RTP) packets and then collecting statistics from DSPs.</p> <p>In some networks, the remote end may not have DSP. In such situations, the real-time protocol test should measure the metrics by making the remote end loop back the RTP stream.</p> <p>The Real-time Transport Protocol test includes delays in the voice path (path from telephony interface to IP interface on originating gateway and path from IP interface to telephony interface on terminating gateway) in these measurements.</p> <p>Note For the real-time transport protocol test to run, the source must have a dsp module type of either C5510 or C549 and must have ds0-group of voice ports configured on it.</p>

Retention period for IP SLA Voice test result data is 30 days. If you want to retain IP SLA Voice test or performance polling data files beyond the retention period, you should back them up or move them to another folder or server.



Note Before uninstalling Cisco Prime Collaboration Assurance, be sure to delete all the IP SLA Voice tests from the application. If you do not delete these tests, they will continue to run on the router.

If you have managed IP SLA capable devices with SNMP V3 credentials, ensure that it has write permission to CISCO-RTTMON-MIB. The following are some of the sample commands:

```
snmp-server view .1.3.6.1.4.1.9.9.42 ciscoMgmt included
snmp-server group v3group1 v3 priv write .1.3.6.1.4.1.9.9.42
snmp-server user user1 v3group1 v3 auth sha Cisco123 priv aes 128 Cisco123
```



Note For more information, see respective IOS device configuration guides to view the exact commands.

Required Cisco IOS and IP SLA Versions

IP SLA Voice tests rely upon Cisco IOS IP SLA technology. The following table lists the versions of IP SLA and Cisco IOS that are required to successfully configure and run each type of IP SLA Voice tests.

Test	IP SLA	Cisco IOS
Ping Echo	2.1.0 and higher	12.0(5)T, 12.1(1), and higher
Ping Path Echo		
UDP Echo		
UDP Jitter for VoIP Without ICPIF/MOS values.		
UDP Jitter for VoIP With ICPIF/MOS values.	2.2.0 and higher	12.3(4)T and higher
Gatekeeper Registration Delay		12.3(14)T and higher
Real-Time Transport Protocol	2.20 and higher	<ul style="list-style-type: none"> • Voice port of type - ds0-group. • DSP of type either C5510 or C549. • IOS version greater than or equal to 12.4(19.12)T

Create an IP SLA Voice Test

To create an IP SLA Voice test:

Step 1 Choose **Synthetic Test Center > IP SLA Voice Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests > IP SLA Voice Test**.

Step 2 Click **Create**.

Step 3 From the Test Type drop-down menu, select one of the following:

- UDP Jitter for VoIP. See [Table 82: UDP Jitter for VoIP Test Parameters](#) for details on the parameters.
- Ping Echo. See [Table 84: Ping Echo Test Parameters](#) for details on the parameters.
- Ping Path Echo. See [Table 85: Ping Path Echo Test Parameters](#) for details on the parameters.
- UDP Echo. See [Table 86: UDP Echo Test Parameters](#) for details on the parameters.
- Gatekeeper Registration Delay
- Real-time Transport Protocol. See [Table 87: Real-time Transport Protocol Test Parameters](#) for details on the parameters.

Step 4 In the Source pane, do the following:

- Select a source device using the device selector.

If you recently added an IP SLA-enabled device and it does not appear in the IP SLA Devices group in the selector in the Source pane on the IP SLA Voice Test Configuration dialog box, refresh the device group membership (**Device Inventory > Inventory Management**).

For Cisco Prime Collaboration Release 11.5 and later

If you recently added an IP SLA-enabled device and it does not appear in the IP SLA Devices group in the selector in the Source pane on the IP SLA Voice Test Configuration dialog box, refresh the device group membership (**Inventory > Inventory Management**).

- Choose a source interface setting. You can leave it at **Default**, or enter a new setting.

Step 5 In the Destination pane, select a destination device using the device selector.

If you want to swap the source and destination devices with each other, click the Swap Source and Destination button.

Step 6 Enter the required information in the Parameters pane.

Step 7 Enter the required information in the Threshold pane.

Step 8 In the Run pane, name the test and schedule when to run the test.

Note The test name that you enter in the Run pane, cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 9 Click **Save**.

Example

Table 82: UDP Jitter for VoIP Test Parameters

Parameter	Default Value	Available Values	Description
Codec Type	—	<ul style="list-style-type: none"> • G.711ulaw • G.711alaw • G.729 	Used to determine the packet interval and the request payload.
Call Duration	8	1 - 59 seconds	Time of the call.
Voice Quality Expectation	Land line	<ul style="list-style-type: none"> • Land line • Wireless campus • Wireless on the move • Multi-hop 	Corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF).

Parameter	Default Value	Available Values	Description
IP QoS	IP Precedence	<ul style="list-style-type: none"> • IP Precedence • DSCP 	Defines the quality of service policies for the IP SLA packets.
	5	<ul style="list-style-type: none"> • IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11) 	This is converted to Type of Service (TOS) and set on the device.

Table 83: UDP Jitter for VoIP Test Threshold Settings

Parameter	Default Value	Available Values	Description
Source to Destination	3 (Packet Loss) 40 msec (Jitter)	Any positive integer ¹	Threshold setting for packet loss and jitter.
Destination to Source	3 (Packet Loss) 40 msec (Jitter)		Threshold setting for packet loss and jitter.
Average Latency	300 msec		Threshold setting for latency.
Node-to-Node Quality	Fair	Excellent, Good, Fair, or Poor	Threshold setting for the test's quality. The values are associated with a MOS score. The value and equivalent MOS are as follows: <ul style="list-style-type: none"> • Excellent—5 (500) • Good—4 (400-499) • Fair—3 (300-399) • Poor—2 (200-299) • Bad—1 (100-199)

Table 84: Ping Echo Test Parameters

Parameter	Default Value	Available Values	Description
Request Payload	32 bytes	28 to 16384 bytes	A default ICMP Ping packet has 32 bytes. Allows for variably sized operations.

Parameter	Default Value	Available Values	Description
IP QoS	IP Precedence	<ul style="list-style-type: none"> • IP Precedence • DSCP 	Defines the quality of service policies for the IP SLA packets.
	0 (none)	<ul style="list-style-type: none"> • IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11) 	This is converted to TOS and set on the device.

Table 85: Ping Path Echo Test Parameters

Parameter	Default Value	Available Values	Description
Request Payload	32 bytes	28 to 16384 bytes	A default ICMP Ping packet has 32 bytes. Allows for variably sized operations.
IP QoS	IP Precedence	<ul style="list-style-type: none"> • IP Precedence • DSCP 	Defines the quality of service policies for the IP SLA packets.
	0 (none)	<ul style="list-style-type: none"> • IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11) 	This is converted to TOS and set on the device.

Table 86: UDP Echo Test Parameters

Parameter	Default Value	Available Values	Description
Request Payload	16 bytes	4 to 1500 bytes	Allows for variably sized operations.

Parameter	Default Value	Available Values	Description
IP QoS	IP Precedence	<ul style="list-style-type: none"> • IP Precedence • DSCP 	Defines the quality of service policies for the IP SLA packets.
	0 (none)	<ul style="list-style-type: none"> • IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11) 	This is converted to TOS and set on the device.

Table 87: Real-time Transport Protocol Test Parameters

Field	Description
General Parameters	
General information about a test.	
Codec Type	Used to determine the packet interval and the request payload.
Call Duration	Test duration. Default is 20 seconds.
Voice Quality Expectation	Corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (CPIF).
Threshold Parameters	
Threshold settings for the Real-Time Transport Protocol test.	
Interarrival Jitter	Threshold Setting. The Destination to Source Inter-Arrival Jitter (Milliseconds) metric is supported.
Packet Loss	Threshold Setting. The Destination to Source Packet Loss (Number) metric is supported.
R Factor	Threshold Setting. A numerical score derived from other VoIP metrics, such as latency, jitter and packet loss, per ITU-T recommendation G.107. A typical range is 50-90, with a score of 80 or higher indicating satisfactory VoIP call quality. Default is 40.
Conversational Quality	Threshold Setting. Tracks the conversational audio signals based on these settings: Excellent, Good, Fair, and Poor. Default is Fair.
Listening Quality	Threshold Setting. Tracks the listening audio signals based on these settings: Excellent, Good, Fair, and Poor. Default is Fair.
Operation-Specific Parameters	
When and how often the test runs.	

Field	Description
Polling Time	Number of times in minutes in a 24-hour period during which polling occurs.
Occurrence Pattern	Dates on which the test starts and ends, and hours during which the test is scheduled to run. If the test runs weekly, the Schedule parameter displays days of the week when the test is scheduled to run.
Test Name	User-defined test name. Cisco Prime Collaboration Assurance also uses the test name to name the folder in which test data is stored. See the description of the Data Directory field in this table.

Import Multiple IP SLA Voice Tests

You can import up to 64 tests, the maximum that Cisco Prime Collaboration Assurance can support, by importing a seed file.

To import multiple tests:

Before you begin

- Before you can import a test, you must first add the source devices.
- Make sure your seed file is formatted correctly.
- To configure the IP SLA Voice test for NAT-enabled devices, ensure the import file contains the private/local IP address for the target router instead of public/global IP address.

Step 1 Choose **Synthetic Test Center > IP SLA Voice Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests > IP SLA Voice Test**.

Step 2 Click **Import**.

Step 3 Click **OK**.

Cisco Prime Collaboration Assurance performs the following actions:

- If this is a file you have imported before, Cisco Prime Collaboration Assurance checks to see if any of the devices exist in Cisco Prime Collaboration Assurance. If all the information in the import file is the same as what already exists in Cisco Prime Collaboration Assurance, a message to that effect appears. Click **OK**.
 - Cisco Prime Collaboration Assurance displays an error message if there are problems with the format of the import file. Click **OK**, then open the file and correct the listed problems. You cannot import the file until all problems are corrected.
 - If there are no errors, a confirmation dialog box appears. The dialog box displays the number of new tests created and the number of tests that will be updated. Click **Yes**.
-

Format IP SLA Voice Test Import Files

You can import up to 64 tests, the maximum that Cisco Prime Collaboration Assurance can support at one time.

All test seed files should have the following information:

- Test name
- Operation type
- Source device name
- Destination device information (it must be the private IP address of the device if it is NAT-enabled)
- Operation parameters
- Schedule parameters

The general format for a test seed file is as follows:

- If you create the import file manually, the import file should have plain text content (Comma, AND, OR, Pipe separated) without header.
- All values must be separated by commas.
- Start and end dates must be formatted as mm/dd/yyyy; for example, 12/01/2004.
- Start and end times must be formatted on a 24-hour clock as hh:mm; for example, 23:30.
- Entering the source-ip-address is optional. This address is the same as the alternate test address.
- Fill in optional fields with double quotation marks; for example, "".
- For all days of the week, enter a one; otherwise, it should be a zero. If the entry for all days of the week is zero, then you need to enter the days of the week. Separate the days of the week with a vertical bar (|); for example, Mon|Tue|Thu|Fri.

Ping Echo Test Import File

Import File Format

```
<testName>,<Ping-Echo>,<source>,<source-ip-address>,<Destination-Name>,<sample-interval>,<IPQosType><IPQosValue>,<request-payload>,<LSRHop1|LSRop2|LSRHop3|LSRHop4|LSRHop5|LSRHop6|LSRHop7|LSRHop8>,<completionTimeThreshold or ">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for all days otherwise 0>,<DaysOfWeek,&br/>if AllDaysOfWeek is 0>
```

LSRHop<number> is an optional field.

Import File Example

```
echo-import1,Ping-Echo,source-1,"",dest-1,1,DSCP,9,64,lsr-hop1|lsr-hop2,300,09:00,17:00,1  
echo-import2,Ping-Echo,source-1,"",dest-1,1,IPPrecedence,4,64,lsr-hop1|lsr-hop2,"",  
09:00,17:00,0,mon|tue|wed|fri
```

Ping Path Echo Test Import File

Import File Example


```
ping-path-import2,Ping-Path-Echo,source-2,"",dest-2,3,DSCP,10,32,250,17:00,23:00,0,
mon|tue|wed|thu|fri
ping-path-import2,Ping-Path-Echo,source-2,"",dest-2,3,IPPrecedence,5,32,"",17:00,23:00,1
```

UDP Echo Test

Import File Format

```
udp-import2,UDP-Echo,source-1,"",udp-dest,IPSLA-Responder,1,DSCP,48,2001,32,"",17:00,23:00,1
```

The destination type can be either UDP-Server or IP SLA-Responder.

UDP Jitter for VoIP Test

Import File Format without Codec (IP SLA Voice Quality) Support

Import File Example

The destination type can be either UDP-Server or IP SLA-Responder.

Import File Format with Codec (IP SLA Voice Quality) Support, valid for Cisco IOS version 12.3(4)T or higher

```
<testName>,Data-Jitter,<source>,<source-ip-address>,<IPSLA-Responder>,<sample-interval>,
<IPQoSType>,<IPQoSValue>,<codecType>,<voiceQualityBenchMark>,<number-of-packets>,<destination-port>,
<pktlossSDThreshold or "">,<pktlossDSThreshold or "">,<jitterSDThreshold or
"">,<jitterDSThreshold or "">,
<avgLatencyThreshold or "">,<nodeToNodeQualityThreshold or
"">,<start-time>,<end-time>,<AllDaysOfWeek.
1 for all days otherwise 0>,<DaysOfWeek,if AllDaysOfWeek is 0>
```

Import File Example

```
jitter-import2,Data-Jitter,source-1,source-1,dest-with-IPSLA-Responder,3,IPPrecedence,
5,G.711ulaw,LandLine,20,2002,30,30,25,25,50,"",17:00,23:00,1
```

Read-community-string is an optional field. If you specify a community string, Cisco Prime Collaboration Assurance validates the IP SLA Responder.

VoIP Gatekeeper Registration Delay Test (Scheduled Daily)

Import File Format without Codec (IP SLA Voice Quality) Support

```
<testName>,Voip-GKReg-Delay,<source GateWay>,<sample-interval>,
<GatekeeperRegistrationTimeThreshold or "">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for
all days otherwise 0>,
<DaysOfWeek, if AllDaysOfWeek is 0>
```

Import File Example

```
gkregdelay-import1,Voip-GKReg-Delay,source-gateway,3,50,17:00,23:00,0,mon|tue|wed|thu|fri
gkregdelay-import2,Voip-GKReg-Delay, source-gateway,5,"",17:00,23:00,1
```

The destination type can be either UDP-Server or IP SLA-Responder.

Manage IP SLA Voice Tests

The following table describes the tasks that you can perform from the IP SLA Voice Test page.

Tasks	Description
Edit IP SLA Voice tests	You can use this function to edit the parameters of an existing test. For example, you can change the operation parameters of a test or change the schedule. You cannot change the destination device. To edit the tests, select the test you want to edit, and then click Edit .
Delete IP SLA Voice tests	You can use this function to delete one or more tests. You can delete tests in any state. To delete the tests, select the test you want to edit, and then click Delete .
View test trending	<p>You can select and examine changes in network performance metrics. You can select, display, and chart network performance data in real time. To view test trending, select the test you want to trend, and click Trend.</p> <p>If you have selected a UDP Jitter for VOIP test, you get an option to select the graph and then the IP SLA Voice Test Trend graph is displayed. The graph selection option is not displayed for other IP SLA Voice tests.</p>
View test information	You can find all the details about a particular test on the Test Details page. From this page, you can print or export test information. To view test information, select the test you want to view, and click View .
Export test details	<p>You can export and save all the details about a single test as shown on the Test Details page, including configuration and status.</p> <p>When you export the test details from Internet Explorer browser, the Windows Security popup window may prompt for your credentials. You can cancel the Windows Security popup and click Save or Save as to download the report.</p> <p>To export test details,</p> <ol style="list-style-type: none"> 1. Select the test you want and click View. 2. Click the Export icon in the upper-right corner of the window.

IP SLA Voice Test Result

The threshold settings that you set during test creation or during modification determine when a IP SLA Voice event is generated.

The events are raised on the source device. A threshold event is generated when the threshold violation occurs for three consecutive polling cycles. The event is cleared if the value falls below the threshold in the following polling cycle. The following IP SLA Voice events can be generated:

Table 88: IP SLA Voice Test Events

NodeToNodeTestFailed To determine why a IP SLA Voice test failed and how to clear it, see the IP SLA documentation located on Cisco.com.	PacketLossSD_ThresholdExceeded	RFactorDS_ThresholdExceeded
RoundTripResponseTime_ThresholdExceeded	PacketLossDS_ThresholdExceeded	MosCQDS_ThresholdExceeded

RingBackResponseTime _ThresholdExceeded	IAJitterDS_ThresholdExceeded	RTPPacketLossDS_ThresholdExceeded
RegistrationResponseTime _ThresholdExceeded	JitterDS_ThresholdExceeded	
AverageLatency _ThresholdExceeded	Quality Dropped Below Threshold	

You can verify whether a test ran and completed correctly. You can also troubleshoot the test if necessary. To do this, select **Synthetic Tests > IP SLA Voice Test**.

The IP SLA Voice Test page appears. All current IP SLA Voice tests appear in the page. The last column in the table shows the status of each test.

Table 89: IP SLA Voice Test Status Definition

Test Status	Description
Running	Test is active and collecting data.
Config Pending	Either the device is not responding or configuration of the test is under way.
Delete Pending	Intermediate state, before the test is deleted. No actions can be performed on the test.
Suspended	Test is suspended from data collecting or polling. This occurs because the device was suspended.
Scheduled	Appears after you create or update a test. The status will change to Running at the first polling cycle.
Dormant	Test is active but not currently collecting data. Tests are in the Dormant state between polling cycles.
Config Failed	Test was not configured correctly. Possible problems include incorrect device credentials or low device memory.

IP SLA Voice Test Data

Cisco Prime Collaboration Assurance saves the data collected by tests to disk.

The following topics provide information you will need to use the data, keep the data safe, and prepare to run additional tests.

Store IP SLA Voice Test Data

IP SLA Voice test data is stored on the Cisco Prime Collaboration Assurance server in the `/opt/emms/cuom/data/N2Ntests` folder. The IP SLA Voice test data is retained for 30 days. The two different types of files stored in the data storage directory are:

- `YYYYMMDD.csv`—Test data. Each file has multiple records. Each record is a comma-separated values (CSV) record, and there is one record in a file for each polling interval.

- StudyInfo.log—Log includes test name, description, polling interval, devices, start date, end date, operation type, polling interval, and status.
-

All configuration information for the IP SLA Voice test is available in the file IPSLATestInfo.log.

Maintain IP SLA Voice Test Data

You should perform all the following tasks to maintain the test data:

- **Verify that there is sufficient disk space to store test data:** Check disk space before a test is scheduled to run. Cisco Prime Collaboration Assurance appends data to a test's log files. Cisco Prime Collaboration Assurance produces one data file for each running test per day when a test is running. Assess the amount of space used by previous tests to derive an estimate.

For example, a test with a 16-hour polling cycle and a 1-minute sampling interval uses approximately 60 to 100 KB per day. A path echo test with a 16-hour polling cycle, a 1-minute sampling interval, and 12 hops uses approximately 1.2 MB per day.

- **Export and save test data.** Cisco Prime Collaboration Assurance purges all data files more than 31 days old. You must save the test to another server to maintain data for more than 31 days.
- **Back up the test data.** Cisco Prime Collaboration Assurance writes test data to the Data Storage Directory, displayed in the Test Details window. Perform regular backups using the same method you use to back up your file system.
- **Determine when to copy data to another server.** You should copy test data to another server before you examine it.
- **Display and use the data.** You can analyze the results of the test after you import the test data into Microsoft Excel or by using a third-party report-generating tool.

Do not open test data files using any application that acquires an exclusive read-only lock on files while the test is in the Running state. If test data files are locked, Cisco Prime Collaboration Assurance will not be able to write output data and will instead write errors to the log files.

Examples of applications that acquire an exclusive lock are Microsoft Excel and Microsoft Word. You can use these applications when the test is not running.

Copy Test Data to Another Server

You must copy test data to another server before you examine it. You may also want to copy the test data to another server as a means of backup. Test data is in ASCII format. You can copy it to another server using whatever method is available to you; for example, SSH or copy-and-paste.

Copy the test data files from the Data Storage Directory. Test data files are those whose names end with .csv, because the test data is written to CSV files.

Data Format

The Echo test data record format captures end-to-end statistics for the following types of tests:

- ICMP Echo
- UDP Echo
- Gatekeeper Registration Delay

Table 90: Echo Test Data Format

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Record type 200	200
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	Completion time	Number	Round-trip time (RTT), in milliseconds	Between 0 and 4294967295
5	Completion status	Number	<p>The allowed numbers are:</p> <ul style="list-style-type: none"> • 1—OK • 2—disconnected • 3—overThreshold • 4—timeout • 5—busy • 6—notConnected • 7—dropped • 8—sequenceError • 9—verifyError • 10—applicationSpecific • 11—dnsServerTimeout • 12—tcpConnectTimeout • 13—httpTransactionTimeout • 14—dnsQueryError • 15—httpError • 16—error 	Between 1 and 16
6	Application-specific completion status	Number	(Optional) An application-specific status that is valid only when completion status is set to applicationSpecific (10).	Between 1001 and 2147483647

7	Status description	Number	(Optional) The description for the completion status when completion status is set to applicationSpecific (10). Default value is blank.	ASCII characters
8	None	Null indicator	Not used	*
Note Fields 9 through 37 are not used and contain the null indicator “*”.				
38	Test name	Text	Name of the IP SLA Voice test	Sjc-VGtest

The Ping Path Echo record format captures hop-by-hop statistics for Ping Path Echo tests. The tests record information from source to destination.

Table 91: Hop-by-hop Statistics for Ping Path Echo Test Data Format

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Record type 201	201
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	Completion time	Number	Round-trip time (RTT), in milliseconds	Between 0 and 4294967295
5	Hop ID	Number	Unique ID chosen by the study and given to a hop on this path.	Maximum value is 30
6	Hop address	String	IP Address of the hop	ASCII characters

7	Completion status	Number	The allowed numbers are: <ul style="list-style-type: none"> • 1—OK • 2—disconnected • 3—overThreshold • 4—timeout • 5—busy • 6—notConnected • 7—dropped • 8—sequenceError • 9—verifyError • 10—applicationSpecific • 11—dnsServerTimeout • 12—tcpConnectTimeout • 13—httpTransactionTimeout • 14—dnsQueryError • 15—httpError • 16—error 	Between 1 and 16
8	Application-specific completion status	Number	(Optional) Application-specific status that is valid only when completion status is set to applicationSpecific (10).	Between 1001 and 2147483647
9	Status description	Text	(Optional) Description for the completion status when completion status is set to applicationSpecific (10). Default value is blank.	ASCII characters
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator “*”.				
38	Test name	Text	Name of the IP SLA Voice test	Sjc-VGtest

This record format captures end-to-end statistics for Ping Path Echo tests. The tests are from the source to the destination.

Table 92: End-to-end Statistics for Ping Path Echo Test Data Format

Field Number	Field ID	Content	Description	Value
--------------	----------	---------	-------------	-------

1	Record ID	nnn	Record type 204	204
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	Completion time	Number	Round-trip time (RTT) in milliseconds	Between 0 and 4294967295
5	Hop ID	Number	Unique ID given to a hop on this path chosen by the study. For this record, the hop ID is always 1.	1
6	Hop address	String	Mandatory: IP address of the destination	ASCII characters
7	Completion status	Number	<p>The allowed numbers are:</p> <ul style="list-style-type: none"> • 1—OK • 2—disconnected • 3—overThreshold • 4—timeout • 5—busy • 6—notConnected • 7—dropped • 8—sequenceError • 9—verifyError • 10—applicationSpecific • 11—dnsServerTimeout • 12—tcpConnectTimeout • 13—httpTransactionTimeout • 14—dnsQueryError • 15—httpError • 16—error 	Between 1 and 16
8	Application-specific completion status	Number	(Optional) The application-specific status that is valid only when Completion Status is set to applicationSpecific (10).	Between 1001 and 2147483647

9	Status description	Text	(Optional) This is the description for the completion status when Completion Status is set to applicationSpecific (10). Default value is blank.	ASCII characters
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator “*”.				
38	Test name	Text	Name of the IP SLA Voice test	Sjc-VGtest

Jitter MOS, ICPIF, and Processed Data record format stores MOS and ICPIF values and processed jitter statistics values.

Table 93: Jitter MOS, ICPIF, and Processed Data Record Format

Field Number	Field ID	Content	Description	Value
1	Record ID	205	Mandatory: record type 205	205
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	ICPIF	Number	Mandatory: Icpif Value	
5	IP SLA Voice quality	Number	Mandatory: MOS value	Example: 3.6
6	Source to destination packet loss	Number	Mandatory: number of packets	Any positive integer. Positive integers must be 32 bit.
7	Destination to source packet loss	Number	Mandatory: number of packets	Any positive integer. Positive integers must be 32 bit.
8	Source to destination jitter	Number	Mandatory: milliseconds	Greater than or equal to 0 and less than or equal to 100
9	Destination to source jitter	Number	Mandatory: milliseconds	Greater than or equal to 0 and less than or equal to 100
10	Average latency	Number	Mandatory: milliseconds	Greater than or equal to 0 and less than or equal to 100
11	None	Null indicator	Not used	*
Note Fields 12 through 37 are not used and contain the null indicator “*”.				

38	Test name	Text	Name of the IP SLA Voice test	Sjc-VGtest
----	-----------	------	-------------------------------	------------

Create a Batch Test

Batch tests enable you to test the health and connectivity of a branch office. Batch tests consist of a set of synthetic tests that are run on voice applications (for example, Cisco Unified Communications Manager Express or Cisco Unity Express) that are deployed in a branch office and a set of phone tests that are run on real phones in the branch office. Batch tests can be configured to run once a day to verify the health of the voice network in the branch office.

Batch tests can be run once a day to verify the health of the voice network.

You can create batch tests by importing an XML file. Each individual batch test consists of multiple synthetic tests and phone tests.

For Cisco Prime Collaboration Release 12.1 SP1 and later

1. Two different synthetic tests cannot use the same Secure JTAPI User and Instance ID.
2. JTAPI users configured for synthetic test cannot be the same as the one used to Manage CUCM.

To create a batch test:

Before you begin

- Verify that your seed file is formatted correctly. See [Format Batch Test Import Files](#) for details on import file format.

Step 1 Choose **Synthetic Test Center** > **Batch Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests** > **Batch Test**.

Step 2 Click **Create**.

Step 3 Browse to the seed file, and click **OK**.

The scheduled time and day for a batch test is configured in the import file. If you want to run a batch test on demand, you can use the Run Now button.

Format Batch Test Import Files

The batch test import file is an XML file. You can find an example of an import file (batchtest.xml) in the */opt/emms/cuom/ImportFiles* directory.

A batch test import file contains information for one batch test. Each batch test import file contains all the information required to configure the [Prerequisites for Synthetic Tests](#) and [Phone Tests—Batch and On Demand Tests](#) for that particular batch test.

When creating a batch test import file, observe the following guidelines for the listed fields:

- TestSchedule—Can have multiple schedule entries.

- Each ScheduleEntry—Must have the following five fields:
 - Month—Not supported.
 - DayOfMonth—Not supported.
 - DayOfWeek—Must be 0 through 6 or asterisk to indicate all days.
 - Hour—Must be between 0 and 23.
 - Minute—Must be between 0 and 59.
- CallAgent—Can be a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Express.
- PhoneMACAddress—The MAC address of a synthetic phone. It must be in the range of 00059A3B7700 to 00059A3B8AFF.



Note Soft phones will display the device name in the MAC address fields.

- PhoneProtocol—The protocol of the synthetic phone, either SCCP or SIP.
- PhoneURIorExtension—The extension or URI of a SIP phone. This is ignored for SCCP phones.
- OnsiteAlertNumber—Required only when IsOSANEnabled is set to true.
- DialingNumber—Optional. PhoneNumber is used if no input is present. This field is valid for intercluster call only. It must provide the complete number that has to be dialed from source phone to reach destination phone on a different cluster.

For example, just the phone number or the dial pattern/access digits plus the phone number.

You can change an existing batch test by importing a new batch test import file. The previous batch test information is overwritten by the new import file. To change the import file, you must manually edit the file.

Manage Batch Tests

The following table describes the tasks that you can perform from the Batch Test page.

Tasks	Description
View Batch Test Details	You can see all details about a particular batch test on the Test Details page. This page lists all the Synthetic Test and Phone Tests—Batch and On Demand Tests that are part of the batch test.
Edit batch tests	To edit batch tests, choose Synthetic Tests > Batch Test . In the Batch Tests page, select the batch test that you want to change and click Edit .

Tasks	Description
Verify the status of a test	<p>You can verify whether a test ran and completed correctly. You can also troubleshoot the test if necessary.</p> <p>To verify the status of a test, choose Synthetic Tests > Batch Test.</p> <p>The Batch Tests page is displayed. All current batch tests are displayed on the page. The last column in the table shows the status of each test.</p> <ul style="list-style-type: none"> • Running—The test is active and collecting data. • Suspended—The test is suspended from data collecting or polling. This occurs because the device was suspended. • Scheduled—Appears after you create or update a test. The status will change to Running at the first polling cycle.
Suspend/resume a batch test	<p>When you suspend a batch test it no longer runs at its scheduled time. The test is not removed from the system. If you want to remove the test, it must be deleted.</p> <p>To suspend and resume a batch test, choose Synthetic Tests > Batch Test.</p> <p>The Batch Tests page appears.</p> <ul style="list-style-type: none"> • If the batch test is active and you want to stop it from running, click Suspend. • If the batch test is suspended and you want it to run it at its scheduled time, click Resume. <p>The scheduled time and day that a batch test is to run is configured in the import file (see Format IP SLA Voice Test Import Files). But if you want to run a batch test on demand, you can use the Run Now button.</p>

Tasks	Description
View batch test results	<p>No events are generated when a component of a batch test fails. You must use the Batch Test Results report to see the results of a batch test. A new Batch Test Results report is generated every 24 hours for each batch test.</p> <p>Cisco Prime Collaboration Assurance saves the data collected by the batch tests on the Cisco Prime Collaboration Assurance server in the <i>/opt/emms/cuom/data/bt</i> folder.</p> <p>The Batch Test Results report provides the following information for the overall batch test:</p> <ul style="list-style-type: none"> • Test status • Date and time that the test started and finished. <p>The Batch Test Results report provides the following information for the individual tests that are a part of the batch test:</p> <ul style="list-style-type: none"> • Test type. • Whether or not it is a negative test. • Test status (passed or failed). • Date and time that the test finished. • Any error messages. <p>To view the results of a batch test, choose Synthetic Tests > Batch Test. In the Batch Tests page, select the batch test that you want to see the results for, and click Results.</p>
Print batch test results	In a batch test report, click the printer icon in the upper-right corner of the page.
Export batch test results	<p>You can use the export functionality to save the test results on your client system.</p> <p>To export the results of a batch test:</p> <ol style="list-style-type: none"> 1. In a batch test report, click the export icon in the upper-right corner of the page. 2. Select either CSV or PDF format for export and click OK.
Delete batch tests	To delete a batch test, choose Synthetic Tests > Batch Test . In the Batch Tests page, select the batch test that you want to change and click Delete .

Phone Tests—Batch and On Demand Tests

The phone tests that are run as part of batch testing and on-demand testing take control of a real phone in the network and make a call from that phone to another phone. Phone tests use JTAPI credentials.

For the phone test feature in Cisco Prime Collaboration Assurance to work properly, the JTAPI credentials need to be configured in Cisco Unified CM as well.

While creating a phone test, follow these guidelines:

- The test phones and test probes must belong to the same Cisco Unified CM because Cisco Prime Collaboration Assurance takes control of these phones and probes through Cisco Unified CM using JTAPI. If the test phones (phones being tested) and test probes (phones being used to run the tests) belong to a different Cisco Unified CM, the tests will fail.
- Only when the call test type is an intercluster call can the destination phone belong to a different Cisco Unified CM. In this instance, the user needs to provide the credentials of the destination Cisco Unified CM in the XML file.
- Before running the phone tests, verify that the configurations are correct in Cisco Unified CM and that the various phone operations are working using the real phones.

**Note**

Do not confuse these phone tests with other Cisco Prime Collaboration Assurance phone tests (synthetic tests or phone status tests). These phone tests are created as part of batch testing and can also be launched on-demand, from IP Phone reports. These tests take control of real phones to conduct the tests.

The following table describes the different types of phone tests.

Table 94: Phone Test Descriptions—Batch and On-Demand Tests

Test	Description
Call Hold	<p>Takes control of two phones and performs the following:</p> <ol style="list-style-type: none"> 1. Places a call from phone A to phone B. 2. Has phone B put the call on hold. 3. Disconnects the call.
Call Forward	<p>Takes control of three phones and performs the following:</p> <ol style="list-style-type: none"> 1. Places a call from phone A to phone B. 2. Forwards the call to phone C from phone B. 3. Verifies that the call is received by phone C. 4. Disconnects the call.

Test	Description
Call Park	<p>Takes control of three phones and performs the following:</p> <ol style="list-style-type: none"> 1. Places a call from phone A to phone B. 2. Has phone B park the call. The call is removed from phone B and a message is displayed to tell you where the call is parked (for example, Call Park at 80503). 3. Has phone C dial the number where the call is parked. The parked call is transferred to the phone that you made the call from. 4. Disconnects the call.
Call Conference	<p>Takes control of three phones and performs the following:</p> <ol style="list-style-type: none"> 1. Places a call from phone A to phone B. 2. Places a conference call from phone A to phone C. 3. Disconnects the call.
Call Transfer	<p>Takes control of three phones and performs the following:</p> <ol style="list-style-type: none"> 1. Places a call from phone A to phone B. 2. Has phone B transfer the call to phone C. 3. Has phone C accept the call. 4. Disconnects the call.
Call Test	<p>Takes control of a phone and places a call to a given number. The call can be from a real phone to a number, in which case the test is controlling the caller only.</p> <p>Alternatively, the call can be from a real phone to a real phone, in which case the test is controlling both the caller and the receiver.</p>

Create a Phone Test on Demand

You can select one or more phones from an IP Phones/Lines report display and run a phone test on demand. The selected phones must belong to the same Cisco Unified CM. Phone tests use the JTAPI credential. The JTAPI credential must be configured in Unified CM.

The JTAPI phone tests support E.164 (“+”) dialing and phones with extensions in this format.

To create a phone test, choose **Synthetic Test Center > Audio Phone Features Test**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Synthetic Tests > Audio Phone Features Test**.

The following table describes the fields, which you can select while creating the on-demand phone test:

Table 95: Phone Test Descriptions—Batch and On-Demand Tests

Item	Description
Cisco Unified Communications Manager	Lists the Unified CM for the phones selected from the phone report. You can select a Unified CM from the left pane and click the >> button to add it to the Unified CM field. The previous Test Phones and Helper Phones selections are cleared; you need to specify them again.
JTAPI Username and Password	Enter the JTAPI username and password configured on Unified CM.
Test Phones	<p>To add more phones to Test Phones:</p> <ol style="list-style-type: none"> 1. Click Add from Phone Report. 2. In the phone report window, select the additional phones to add and click Select. <p>The phones added must belong to the same Cisco Unified CM provided at the beginning for this test.</p> <p>If you select a single phone which shares its extension with other phones in the personalized report, the report generated will have details about all the phones (including the selected phone).</p>
Helper Phones	<p>To add more phones to Helper Phones:</p> <ol style="list-style-type: none"> 1. Click Add from Phone Report. 2. Select the additional phones to add and click Select. <p>The phones added must belong to the same Cisco Unified CM provided at the beginning for this test.</p> <p>If you select a single phone which shares its extension with other phones in the personalized report, the report generated will have details about all the phones (including the selected phone).</p>
Phone Tests	<p>Select the phone test that you want to see the results for. See Phone Test Descriptions—Batch and On-Demand Tests.</p> <p>When Call Test is selected Call Type, Success Criterion, and Phone Number fields are enabled.</p>
Call Type	From the drop-down list, choose the call type. When Inter Cluster Call is selected, the following fields are enabled: Cisco Unified Communications Manager JTAPI Username JTAPI Password.

Success Criterion	From the drop-down list, choose the success criterion.
Phone Number	The destination phone number to be dialed for the call test needs to be specified in this field.
Dialing Number	When Inter Cluster Call is selected for Call Type, enter the complete phone number that the source phone must dial to reach the destination phone on a different cluster. This may include dial pattern or access digits, for example 94151234567. This field is not mandatory. If left blank, the Phone Number field is used instead.
Cisco Unified Communications Manager	When Inter Cluster Call is selected for Call Type, enter the Cisco Unified CM for the phone number specified in the Phone Number field.
JTAPI Username and Password	When Inter Cluster Call is selected for Call Type, enter the JTAPI username and password for the Cisco Unified CM provided in the previous field.

Audio Phone Features Test

The Audio Phone Features Test portlet displays the phone tests summary for all the Cisco Unified Communications Manager nodes.

It provides the following details:

- Number of phones tested
- List of tested features
- Date and time test was last completed
- Result of latest phone test
- Customer Name (only in MSP mode)

The following are some of the requirements for Phone Features Test:

• **JTAPI User (Application User) Requirements:**

Standard Role	Privileges/Resources for the Role
Standard AXL API Access	Allows access to the AXL database API
Standard CCM Admin Users	Login rights to Cisco Unified Communications Manager Administration.
Standard SERVICEABILITY Administration	A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.
Standard CTI Enabled	Enables CTI application control
Standard CTI Allow Call Monitoring	Allows CTI applications or devices to monitor calls

Standard Role	Privileges/Resources for the Role
Standard CTI Allow Control of Phones supporting Connected Xfer and conf	Allows control of all CTI devices that supports connected transfer and conferencing
Standard CTI Allow Control of all devices	Allows control of all CTI-controllable devices

**Note**

- The “Standard CTI Allow Control of all devices” is an optional role to replace the other CTI Standard roles. This role is recommended only when a dedicated JTAPI test user is created.
- All test phones must be listed as controlled in the Application User's listing, and the users must exist in all Unified CM nodes.
- **For Cisco Prime Collaboration Release 12.1 SP1 and later**
 1. Two different synthetic tests cannot use the same Secure JTAPI User and Instance ID.
 2. JTAPI users configured for synthetic test cannot be the same as the one used to Manage CUCM.

• Phone Requirements:

- Standard CTI Enabled
- All test users must be registered to the same subscriber (or Unified CM node)
- The phone must be in a Managed state in Cisco Prime Collaboration Assurance
- The phone must be listed as “AllFine” as the Management Status Reason in the Phone Report that is used to select the phones

• Processor Requirements:

- JTAPI credentials must be in use, and the test valid for each Unified CM node
- CTI Manager must be running in the Test node
- AXL Web Services must be running in the Test node
- Cluster IDs must be unique and configured in each Unified CM node for each cluster
- The processor must be in a Managed state in Cisco Prime Collaboration Assurance

• Secure JTAPI Requirements



Note For Cisco Prime Collaboration Release 12.1 SP1 and later

1. JTAPI users configured for synthetic test cannot be the same as the one used to Manage CUCM.
2. Two different synthetic tests cannot use the same Secure JTAPI User and Instance ID.

Table 96: Secure JTAPI Field Description

Field Name	Description
<p>JTAPI</p> <p>Used to retrieve the session status information from the Cisco Unified CM.</p>	<p>A new set of JTAPI specific parameters are introduced to secure the JTAPI (TLS1.2) connection.</p> <p>Following are a set of JTAPI specific parameters.</p> <ol style="list-style-type: none"> 1. JTAPI User Name: Specify JTAPI User Name configured on Unified Communications Manager. 2. JTAPI Password: Specify JTAPI Password configured on Cisco Unified Communications Manager. 3. Secure JTAPI check box: <ol style="list-style-type: none"> a. Check the check box: Checking this option enables you to have a secure TLS connection to Cisco Unified Communications Manager. <p>Note Ensure that “Standard CTI Secure Connection” role is associated with this JTAPI user, along with other required roles".</p> b. Uncheck the check box - If the check box is not checked, JTAPI cannot make a secure connection. <p>Note Ensure that “Standard CTI Secure Connection” role associated with this JTAPI user is removed. To continue to Monitor Conferences, ensure that the required roles are configured"</p> <p>For more information, see Setting up Devices for Cisco Prime Collaboration Assurance.</p> <p>The check box enables you to enter the parameters in (enable or disable) the new Secure JTAPI fields.</p>

Field Name	Description
------------	-------------

Field Name	Description
	<p>4. TFTP Server IP Address - Specify the IP address of the TFTP Server</p> <p>Note The value must be one of the nodes on the CUCM cluster. Make sure that the TFTP service is running on that node.</p> <p>5. TFTP Server Port - The TFTP Server Port defaults to 69.</p> <p>Note Do not change the default value unless the System Administrator recommends.</p> <p>6. CAPF Server IP Address - Specify the IP address of the CAPF Server.</p> <p>Note</p> <ol style="list-style-type: none"> 1. For more information on the method to secure the CTI, JTAPI, and TAPI applications and to know more about the certificate authority proxy function, see the Chapter on “Authentication and Encryption Setup for CTI, JTAPI, and TAPI” and “Certificate Authority Proxy Function” respectively in the “Security Guide for Cisco Unified Communications Manager”. 2. Ensure to select RSA Only from the Key Order drop-down list while creating the CAPF profile on CUCM. 3. You must always provide the CUCM Publisher IP Address. <p>7. CAPF Server Port - The CAPF Server Port number defaults to 3804.</p> <p>Note Ensure that the value entered matches with the value that is configured in Cisco Unified Communication Manager.</p> <p>8. Instance ID for Publisher - This field specifies the application instance identifier configured in CAPF Settings section of Application or End User CAPF profile configuration page in the Cisco Unified Communication Manager cluster.</p> <p>9. Secure Authentication String – Enter the Authentication String configured in CAPF Settings section of Application or End User CAPF profile configuration page in the respective Communication Manager Publisher.</p>

Field Name	Description
	<p>Note The section on Troubleshooting Secure JTAPI Connections lists the details of troubleshooting the possible errors and recommended actions "with setup of CUCM for Secure JTAPI and Sessions not coming up on Conference Diagnostics" respectively.</p>

Troubleshooting

Perform troubleshooting for the following Phone Feature Test scenarios in Cisco Prime Collaboration Assurance.

• Issue

The Phone Feature Test fails and displays the following error message:

“Address XXXXXX is not in provider's domain”

Recommended Action

- Ensure that the endpoints that are selected for the feature test are all assigned to the same JTAPI user
- Ensure that the “Standard CTI Allow Control of all devices” role is selected for the JTAPI user.

• Issue

The Phone Feature Test fails and displays the following error message:

“ Unable to create provider -- Connection refused”

Recommended Action

- Ensure that the JTAPI credentials of the user are configured in Unified CM
- Ensure that the phones that are used in the feature test are assigned to the same JTAPI user
- Ensure that the CTI Manager is active and running in the Unified CM node that is used for testing
- Update the JTAPI Java Archive (JAR) files in Cisco Prime Collaboration Assurance, if the JTAPI implementation in Unified CM has been modified

CME Diagnostics

The CME Diagnostics (**Diagnose > CME Diagnostics**) page displays information about Cisco Unified Communications Manager Express (Cisco Unified CME) devices and associated Cisco Unity Express devices.

You can launch the device 360 view for Cisco Unified CME devices.

It also displays the following information:

- Number of ephones registered with each CME. You can click on the number to cross-launch to the Endpoint Diagnostics page.

- Number of unregistered ephones. Click on the number to cross-launch to the Endpoint Diagnostics page.
- Total number of active and acknowledged alarms on the CME. Click on the number to launch the Alarms tab, in the Alarms & Events page..
- Registration status of CUE with CME. If the CUE is not integrated with the CME or if the CUE is not managed in Cisco Prime Collaboration Assurance, this column displays N/A.
- Total number of active and acknowledged alarms on the CUE.



Note **Endpoint Name** field in **Endpoint Diagnostics** page is not supported for CME phones.

Limitation

For Cisco Prime Collaboration Release 12.1 SP3 and later

- Cisco Prime Collaboration Assurance uses multiple OIDs (like 1.3.6.1.4.1.9.9.439.1.1.47.1.4 for DN) to pull phone information from CME phones.
- Cisco Prime Collaboration Assurance does not support SIP phone discovery from CME phones.

Monitoring IP Phones Using Cisco Unified CME Syslog Messages

1. Add the Cisco Prime Collaboration Assurance IP configuration in CME to successfully receive Cisco Unified Communications Manager Express syslog messages.

```
CME # (config) # logging <PCA_IP>
```

2. Use the IP phone registration or deregistration events to send syslog message to the Cisco Prime Collaboration Assurance when the syslog is configured in CME.
3. Use this example to configure the IP phone registration:

Error Message:

```
%IPPHONE-6-REGISTER_NEW: ephone-3:SEP003094C38724 IP:1.4.170.6 Socket:1  
DeviceType:Phone
```

has registered.



CHAPTER 27

Troubleshooting Workflow for Video Endpoints

This section explains the following.

- [Troubleshooting Workflow for Video Endpoints, on page 527](#)

Troubleshooting Workflow for Video Endpoints

For Cisco Prime Collaboration Release 11.6 and later

You must understand the Cisco Prime Collaboration Assurance discovery workflow before reviewing this section. For information on the device discovery process, see the *Discover Devices* section in the [Cisco Prime Collaboration Assurance Guide- Advanced, 11.x](#).

During the troubleshooting workflow, the devices are polled, based on the values defined for the System Status Polling Interval, and Flow Statistics Polling Interval in the Conference Path Threshold Settings page.

During the troubleshooting workflow, the endpoints and conference devices are polled every minute to check the status.

You can view details, such as CPU utilization, memory utilization, interface, and so forth for a network device.



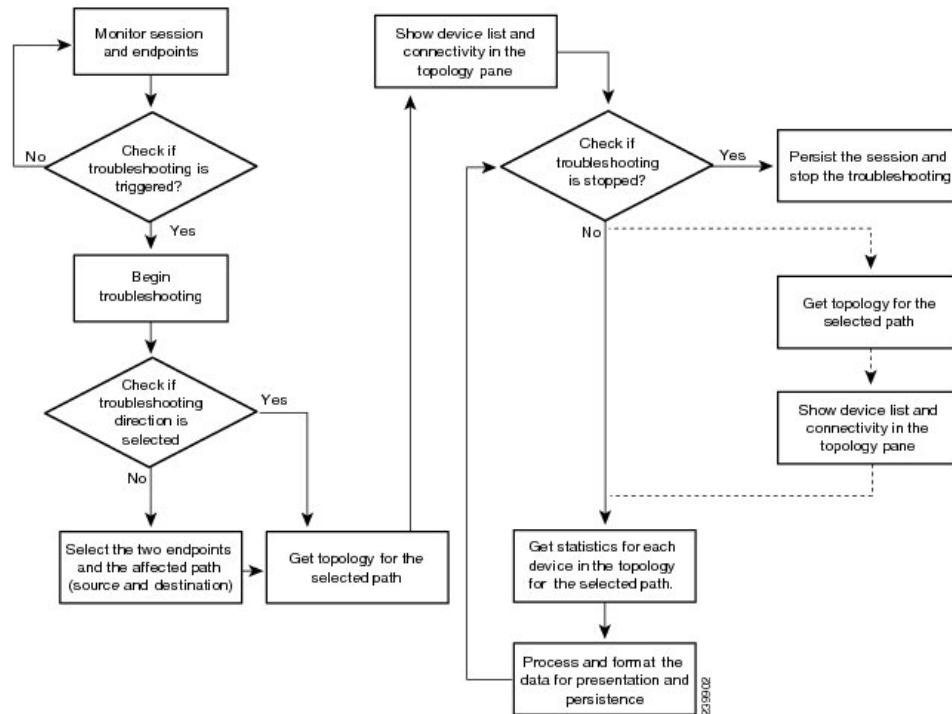
Note Conference troubleshooting is not supported, if you have deployed Cisco Prime Collaboration Assurance in MSP mode

The troubleshooting workflow impacts the Cisco Prime Collaboration Assurance system performance. Add a conference or an endpoint to the watch list only if it is required.

The troubleshooting workflow for a conference is represented below.

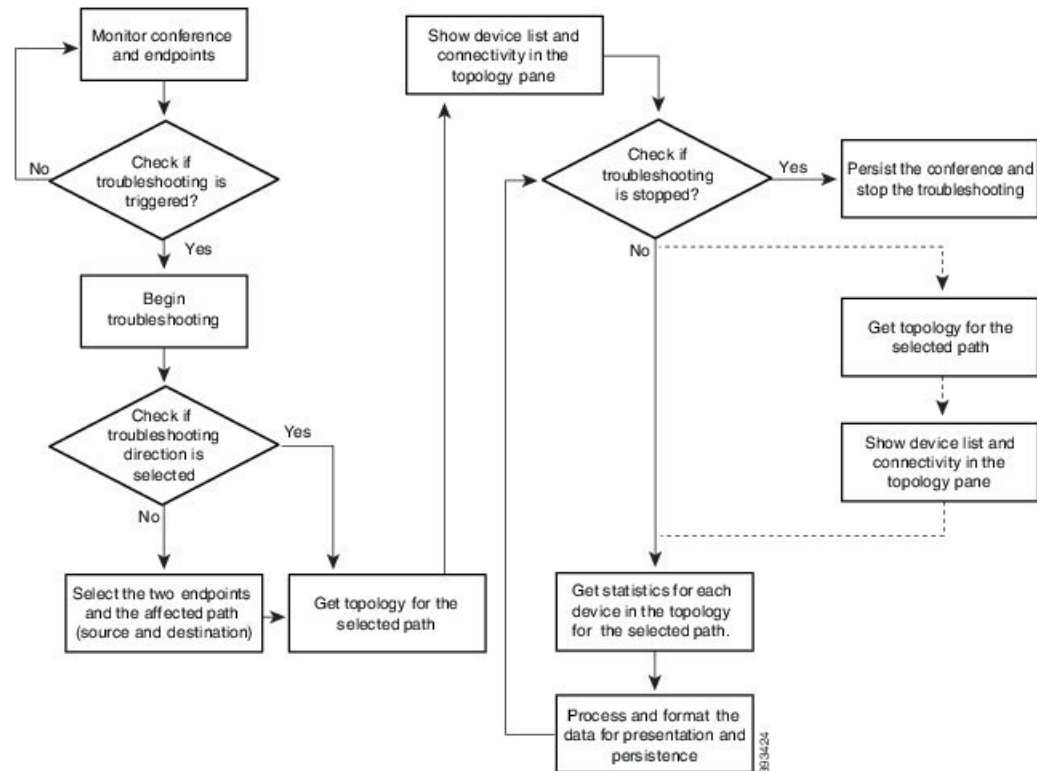
For Cisco Prime Collaboration Release 11.1 and earlier

Figure 9: Troubleshooting Workflow for a Session



For Cisco Prime Collaboration Release 11.6 and later

Figure 10: Troubleshooting Workflow for a Conference



Related Topics

[Discover Devices](#)

Features of the Troubleshooting Workflow

The following are the key features of the troubleshooting workflow:

- It can be started automatically or manually:
 - Automatic troubleshooting is triggered when the conference is added to the watch list.
 - Automatic troubleshooting is triggered when one of the endpoints is in the watch list. You can start a troubleshooting workflow only if the endpoints are in the Managed state.
 - Automatic troubleshooting is triggered if the value for packet loss, jitter, or latency alarm exceeds the defined threshold value. This is applicable only for a point-to-point conference.
 - Automatic troubleshooting is not triggered when the packet loss, jitter, or latency alarm occurs in a multipoint conference.
- Manual troubleshooting can be started from the Conference Diagnostics page.

See [Start a Troubleshooting Workflow, on page 533](#) for details on how to start a troubleshooting workflow for conferences and endpoints.

- When there is a packet loss, jitter, or latency alarm between the two endpoints, the troubleshooting workflow starts if you have configured for the automatic troubleshooting; when this alarm is cleared, the troubleshooting workflow stops.
- Troubleshooting is supported between two endpoints in both directions. You can select the direction for troubleshooting between the endpoints, if you are manually starting the troubleshooting workflow.
- Troubleshooting is supported between a video endpoint and SBC. The troubleshooting direction is from a video endpoint to SBC, and not in the reverse direction.
- Troubleshooting is supported between an endpoint and Cisco TelePresence Server. The troubleshooting direction is from an endpoint to Cisco TelePresence Server, and not in the reverse direction.
- Troubleshooting is supported between an endpoint and Cisco MSE. The troubleshooting direction is from an endpoint to Cisco MSE, not in the reverse direction.
- Troubleshooting is supported between an endpoint and Cisco VCS. The troubleshooting direction is from an endpoint to Cisco VCS and not in the reverse direction.
- If the endpoint is in an Unknown state, you can troubleshoot from a known endpoint to this unknown endpoint. For multipoint conferences also, you can troubleshoot in the same manner.
- The troubleshooting workflow lasts for a maximum of four hours from the time it is started. If the troubleshooting workflow does not end within this time, Cisco Prime Collaboration Assurance ends the workflow automatically.
- You can have a maximum of 50 concurrent troubleshooting workflows at a time.

If this limit is exceeded, an error message is displayed in the troubleshooting log file.

Features of the Troubleshooting Workflow for Conferences

The following are the key behaviors of the troubleshooting workflow, when scheduled conferences are added to the watch list:

- The automatic troubleshooting workflow starts for all conferences added to the watch list.
- In a multipoint conference, the troubleshooting starts as soon as the endpoints join the conference.
- In a multipoint conference, if a troubleshooting is stopped for an endpoint, the troubleshooting workflow continues for the other endpoints in the conference. You need to manually start the troubleshooting for this endpoint.
- In a multipoint conference, if an endpoint restarts because of a problem, a new troubleshooting workflow is triggered for this endpoint after it rejoins the conference. There is no impact on the other endpoints in the conference.
- If a conference is removed from the watch list, the associated troubleshooting workflow stops, provided:
 - There are no packet loss, jitter, or latency alarms triggered for that conference.
 - There are no manually triggered troubleshooting workflows.
- If a troubleshooting workflow is triggered because of a packet loss, jitter, or latency alarm, the troubleshooting workflow stops when the packet loss, jitter, or latency alarm is cleared, provided:
 - The conference is not added to watch list.
 - There are no manually triggered troubleshooting workflows.

- The troubleshooting workflow is manually stopped, or the conference ends.
- If a troubleshooting workflow is triggered manually, the troubleshooting workflow can only be stopped manually; otherwise, it stops when the conference ends.
- If a conference is added again to the watch list, a new troubleshooting workflow starts.

Features of the Troubleshooting Workflow for Endpoints

You can start a troubleshooting workflow only if the endpoints are in the Managed state. The following are the key behaviors of the troubleshooting workflow, when an endpoint is added to the watch list:

- The automatic troubleshooting for an endpoint starts as soon as it joins a conference. You can stop the troubleshooting workflow for a conference that is associated with an endpoint (added to a watch list). You need to manually start the troubleshooting for this conference.
- During the conference, if an endpoint is removed from the watch list, the troubleshooting stops for that endpoint.
- If a conference and the associated endpoints are part of the watch list and if an endpoint is removed from the watch list, the troubleshooting workflow continues for the conference until it ends.
- If a conference and the associated endpoints are part of the watch list and if the conference is removed from the watch list, the troubleshooting workflow continues for the endpoints, until they disconnect from the conference. That is, if the conference and endpoints are part of the watch list, the endpoints are given higher priority.
- For MRA endpoints, the troubleshooting legs are not displayed. For non-MRA endpoints, the troubleshooting workflow happens from the endpoints to the Cisco VCS with Cisco Collaboration Edge.

Support Matrix for Troubleshooting Source and Destination Endpoints

The following table shows the details of troubleshooting support between source and destination endpoints:

For Cisco Prime Collaboration Release 11.5 and earlier



Note

- In case of troubleshooting for multi-point calls, ensure that first hop router/ switch of the source device (for example MCU) has CLI access.
- For mediatrace statistics ensure that
 - 5-tuple (Source Address, Source Port, Destination Address, Destination Port, and Protocol) should be available on the source or destination device
 - There is mediatrace initiator in the path and it has mediatrace version 1.0 or 3.0 (2.0 is not supported).
- For devices such as MCU, CTMS and MXP, and E20, 5 tuple is not available.

For Cisco Prime Collaboration Release 11.5 and earlier

Source	Destination
CTS	CTS, CTMS , C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, , E20, Router

Source	Destination
C_CODEC	CTS, CTMS , VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, MCU, E20, Router
CIUS	CTS, CTMS , C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, MCU, E20
MXP	CTS, CTMS , VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, MCU, E20
Phone	CTS, CTMS , VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber , MCU, E20
Cisco Jabber	CTS, CTMS , VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber MCU, E20
POLYCOM	CTS, (CTMS) VCS, C_CODEC, TPS, CIUS, MXP, MCU, PHONE, Cisco Jabber, E20
E 20	E20, CTS, (CTMS), VCS, C_CODEC, TPS, CIUS, MXP, MCU, PHONE, Cisco Jabber,
Switch	Switch, Router
Router	Switch, Router, C_CODEC, MCU, TPS, (CTMS)
VSAA	VSAA
CTMS	CTS, Router
MCU	C_CODEC, E20, MXP, CIUS, IP Phone, Cisco Jabber, Router
TPS	C_CODEC, E20, MXP, CTS, CIUS, IP Phone, Cisco Jabber, Router
VCS	C_CODEC, E20, MXP, CIUS, IP Phone, Cisco Jabber,

For Cisco Prime Collaboration Release 11.6 and later

Source	Destination
Cisco endpoint	Cisco endpoint, MCU, TPS, virtual TPS, VG, CUBE, VCS, Expressway-Core, Unknown endpoint

**Note**

- Cisco Prime Collaboration Assurance supports troubleshooting only when the source device is a Cisco endpoint that contains 5-tuple information.
- Cisco Prime Collaboration Assurance does not support troubleshooting for Cisco Jabber endpoints.

Start a Troubleshooting Workflow

You can start the troubleshooting workflow for a conference from the 360° Conference View in the Conference Diagnostics page.

For Cisco Prime Collaboration Release 11.1 and earlier



Note

To reduce troubleshooting time, it is recommended that the devices in the media path are already discovered and available in **Inventory** before you start troubleshooting.

You can start the troubleshooting workflow for an endpoint from the quick view window in the Endpoint Diagnostics page.

For Cisco Prime Collaboration Release 11.6 and later

Table 97: Launch Points for the Troubleshooting Workflow

Troubleshooting Type	Launch Points
Automatic	<ol style="list-style-type: none"> 1. Choose Diagnose > Conference Diagnostics. 2. Select a scheduled conference. 3. Rest your mouse pointer over the Conference Subject column in the Video Collaboration Conference table and click the 360° Conference view icon. 4. Click Add to Watch List.
Automatic	<ol style="list-style-type: none"> 1. Choose Diagnose > Conference Diagnostics. 2. Select an endpoint, which is in the Not In Use usage status. 3. Rest your mouse pointer over the Endpoint Name column in the List of Endpoints table and click the quick view icon that appears. 4. Click Add to Watch List. <p>The troubleshooting workflow starts as soon as the endpoint joins a conference.</p>

Troubleshooting Type	Launch Points
Manual	<ol style="list-style-type: none"> 1. Choose Diagnose > Conference Diagnostics. 2. Select an in-progress conference. We recommend that you select an alarmed in-progress conference. 3. Rest your mouse pointer over the Conference Subject column in the Video Collaboration Conference table and click the 360° Conference view icon. 4. Click icon to launch the Troubleshooting page and select the direction from where you want to start the troubleshooting.
Manual	<ol style="list-style-type: none"> 1. Choose Diagnose > Conference Diagnostics. 2. Select an endpoint, which is in the In Use usage status. 3. Rest your mouse pointer over the Endpoint Name column in the List of Endpoints table and click the quick view icon. 4. Click Add to Watch List. The troubleshooting workflow starts immediately.

Troubleshoot Data Analysis

You can view troubleshooting data for both in progress conferences and completed conferences, if manual or automatic troubleshooting is/was activated for conferences or endpoints.

After the troubleshooting job is completed the following data is displayed:

Troubleshooting

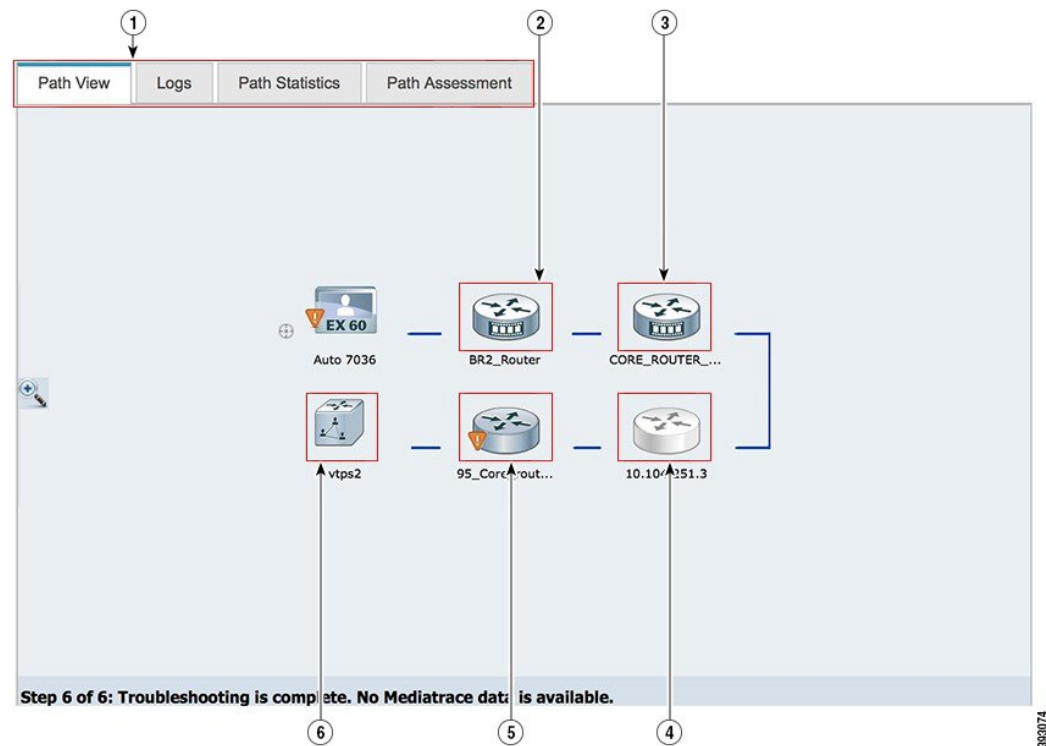
You can view the topology (Layer 2 and Layer 3) for the selected direction between endpoints in the Path View tab.

- A straight line between the devices indicates that the devices are directly connected to each other.
- A dotted line between the devices indicates that the devices may not be connected.

The following image shows a troubleshooting conference between endpoints.

For Cisco Prime Collaboration Release 11.1 and earlier

Figure 11: Troubleshooting Session Between Endpoints

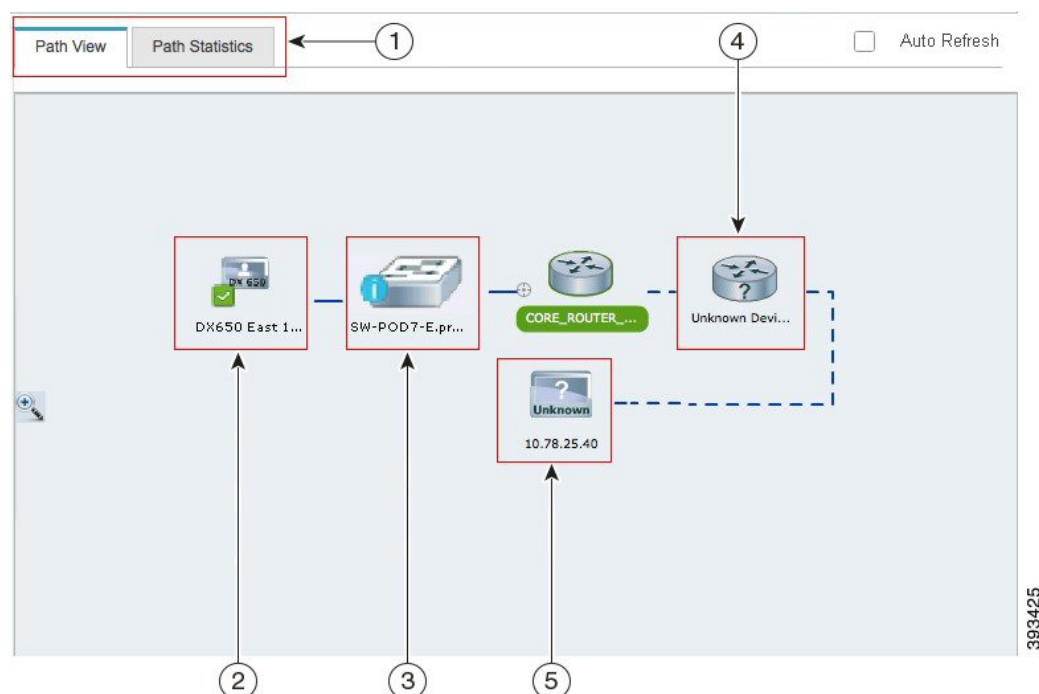


1	Troubleshooting results tab. Based on the configurations (mediatrace, performance monitor) on the devices, some of the tabs may not be displayed.	2	Devices that contains the Cisco Prime Network Analysis Module (Prime NAM) application are displayed with an additional badge on the device. Inaccessible devices are displayed in gray.
3	Mediatrace enabled devices are displayed with an additional badge on the device.	4	Inaccessible devices are displayed in gray
5	An alarm badge on the endpoint indicates that there is a fault in the endpoint.	6	An information badge on a discovered device indicates that there is an issue with the Memory, CPU utilization, and/or Call Quality Statistics (RTP Packet Loss, RTP Packet Jitter, DSCP) for media flows. The threshold value for the Call Quality Statistics and utilization (memory and CPU) is defined in the Conference Path Threshold Settings page (Alarm & Report Administration > Conference Path Threshold Settings).

If the devices are accessible, you can rest your mouse pointer over the device and click the quick view icon, to view the system, interface details.

For Cisco Prime Collaboration Release 11.6 and later

Figure 12: Troubleshooting Conference Between Endpoints



1	Troubleshooting results tab.	2	The source endpoint from where the troubleshooting is initiated.
3	<p>The midpoint (router or switch) that is in the path. A blue badge on the midpoint indicates that the threshold value has exceeded the configured limit for Rx packet loss, jitter, or latency for all devices.</p> <p>The threshold value is defined in the Conference Path Threshold Settings page (Alarm & Report Administration > Conference Path Threshold Settings).</p>	4	Unknown devices that are not identified by Cisco APIC-EM. The unknown devices are displayed with a question mark (?).
5	<p>The destination endpoint.</p> <p>Cisco Prime Collaboration Assurance supports troubleshooting even when the destination device or endpoint is in Unknown state.</p>		

For Cisco Prime Collaboration Release 11.6 and later

By default, the Conference Troubleshooting page auto refreshes every 30 seconds. To disable the auto refresh functionality, uncheck the **Auto Refresh** check box at the top right corner of the Conference Troubleshooting page. You can rest your mouse pointer over the device and click the quick view icon, to view the system, interface, and flow details.

The following table lists the system, interface, and flow details that are listed in the quick view.

For Cisco Prime Collaboration Release 11.1 and earlier

Table 98: System, Interface, and Flow Details

Field		Description	
Hostname		Hostname configured for the device.	
IP Address		IP address used for managing the device. You can launch to the endpoint or infrastructure device log in page, using this link.	
Mediatrace Capable This information is displayed only if you have enabled Mediatrace on the device.	Mediatrace Role	Configured Cisco Mediatrace role on the device.	
	IP SLA Role	Configured IP SLA role on the device.	
	Performance Monitor	Configured Performance Monitor.	
System Status	Physical Memory Utilization (in%)	Percentage of the physical memory utilization.	
	CPU Utilization (in%)	Percentage of the CPU utilization.	
	Interface Details	Operation Status	Administrative status of the interface as specified in the ifOperStatus object.
Input Metrics		The data displayed are based on the RFC1213 MIB attributes.	
Output Metrics		The data displayed are based on the RFC1213 MIB attributes.	
Network Diagnosis	This is displayed only if you are managing these devices in the Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime LMS.		

Field		Description
Media Flow Information	The following information is a consolidated report for all managed codec on the device. This information is displayed only if you have enabled Mediatrace on the device.	
	DSCP	DSCP value configured on the device.
	IP Packet Drop Count	Number of IP packets dropped.
	RTP Packet Loss	Packet loss indicated by the Real-time Transport Protocol (RTP).
	RTP Packet Jitter (RFC 3550)	Jitter indicated by the Real-time Transport Protocol (RTP).
	Ingress Interface	Details on ingress interface.
	Egress Interface	Details on egress interface.

For Cisco Prime Collaboration Release 11.6 and later

Table 99: System, Interface, and Flow Details

Field		Description
Hostname		Hostname configured for the device.
IP Address		IP address used for managing the device. You can launch to the endpoint or infrastructure device log in page, using this link.
System Status	Physical Memory Utilization (in%)	Percentage of the physical memory utilization.
	CPU Utilization (in%)	Percentage of the CPU utilization.
Interface Details	System Status	Administrative status of the interface as specified in the ifOperStatus object.
	Input Metrics	The data displayed are based on the RFC1213 MIB attributes.
	Output Metrics	The data displayed are based on the RFC1213 MIB attributes.
Media Flow Information		
Note The negative value –1 indicates that the particular statistical data is not available from the platform/device.		

Field		Description
	DSCP	DSCP value configured on the device.
	IP Packet Drop Count	Number of IP packets dropped.
	RTP Packet Loss	Packet loss indicated by the Real-time Transport Protocol (RTP).
	RTP Packet Jitter (RFC 3550)	Jitter indicated by the Real-time Transport Protocol (RTP).
	Ingress Interface	Details on ingress interface.
	Egress Interface	Details on egress interface.

Path Statistics

The Path Statistics View displays the statistics for each node in the path.

The following graphs are displayed in the Path Statistics View:

CPU and Memory

The graph is displayed for all devices and includes the following information:

- The vertical axis (y-axis) provides the CPU utilization details of last 5 minutes as a percentage.
- The horizontal axis (x-axis) provides lists of all network devices that were discovered during the path trace.
- The spheres in the graph provides the processor memory utilization details as a percentage. The tool tip on the sphere indicates the exact memory utilization value.
- The size of the sphere varies, based on the processor memory utilization. The smaller the sphere size, the less the processor memory utilization.

Click on the sphere (red icon) to view the system, interface, and flow details.

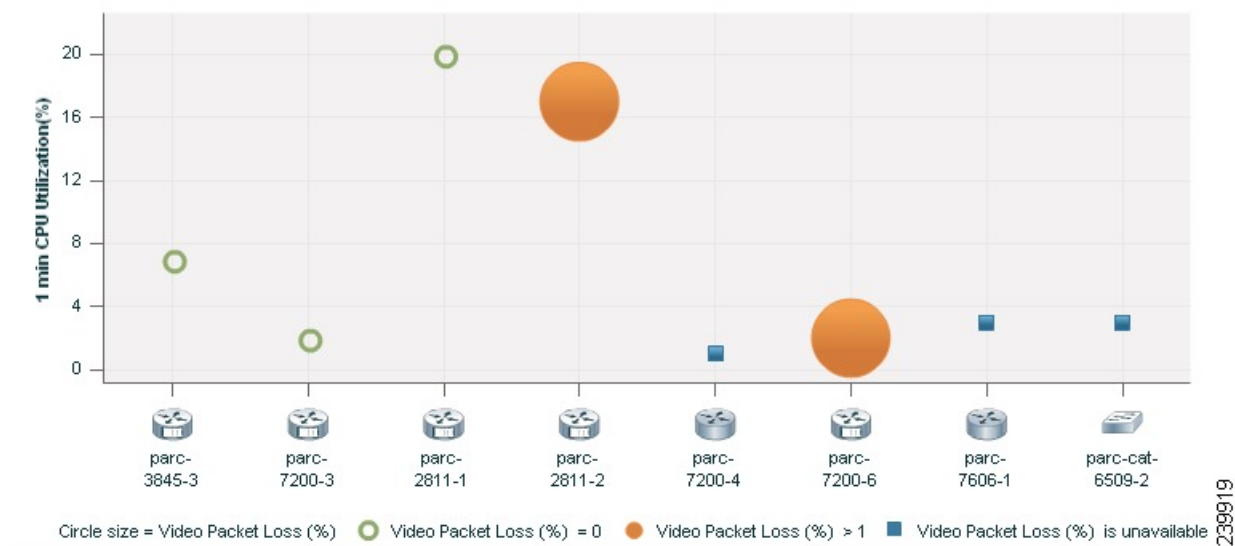
CPU and Packet Loss

This graph is displayed for all devices and includes the following information:

- The vertical axis (y-axis) provides the CPU utilization details of last 5 minutes as a percentage.
- The horizontal axis (x-axis) provides lists of all network devices that were discovered during the path trace.
- The spheres in the graph provides video packet loss details as a percentage:
 - Green sphere indicates that the video packet loss is zero.
 - Orange sphere indicates that the video packet loss is more than 1%. The size of the sphere varies, based on the video packet loss. The smaller the sphere size, the less the video packet loss.

You can click on the sphere to further analyze the packet loss at the interface-level.
- Blue square box indicates that the perfmon counter statistics are not available from the devices.

Figure 13: CPU and Packet Loss Graph



Click on the sphere or square box (red icon) to view the system, interface, and flow details.

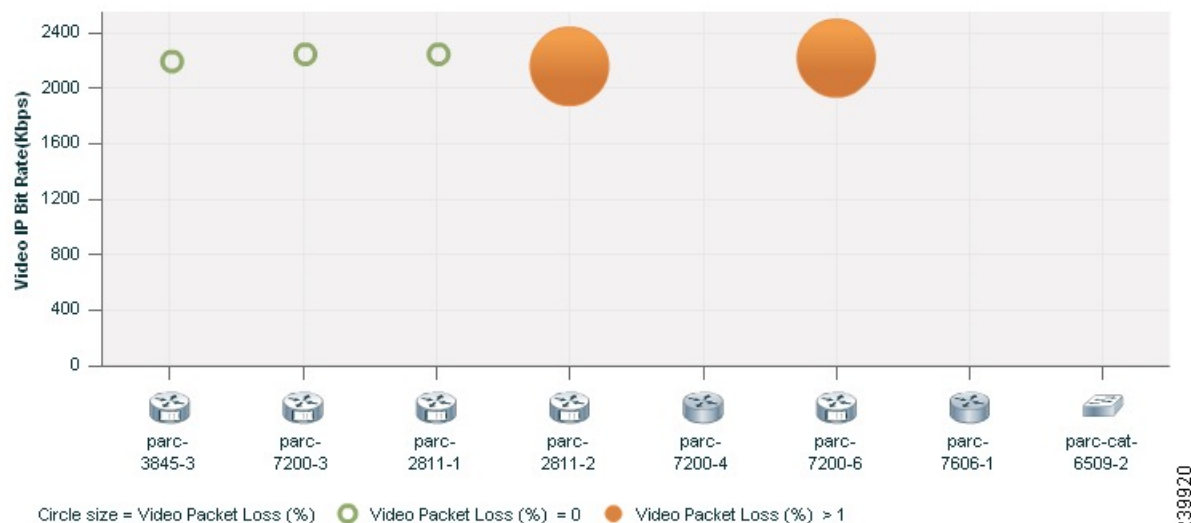
Video IP Bit Rate and Packet Loss

This graph is displayed for all devices and includes the following information:

- The vertical axis (y-axis) provides the video IP bit rate in kilobits per second (kbps).
- The horizontal axis (x-axis) provides lists of all network devices that were discovered during the path trace.
- The spheres in the graph provides the video packet loss details as a percentage.
 - Green sphere indicates that the video packet loss is zero.
 - Orange sphere indicates that the video packet loss is more than 1%. The size of the sphere varies, based on the video packet loss. The smaller the sphere size, the less the video packet loss.

You can click on the sphere to further analyze the packet loss at the interface-level.

Figure 14: Video IP Bit Rate and Packet Loss Graph



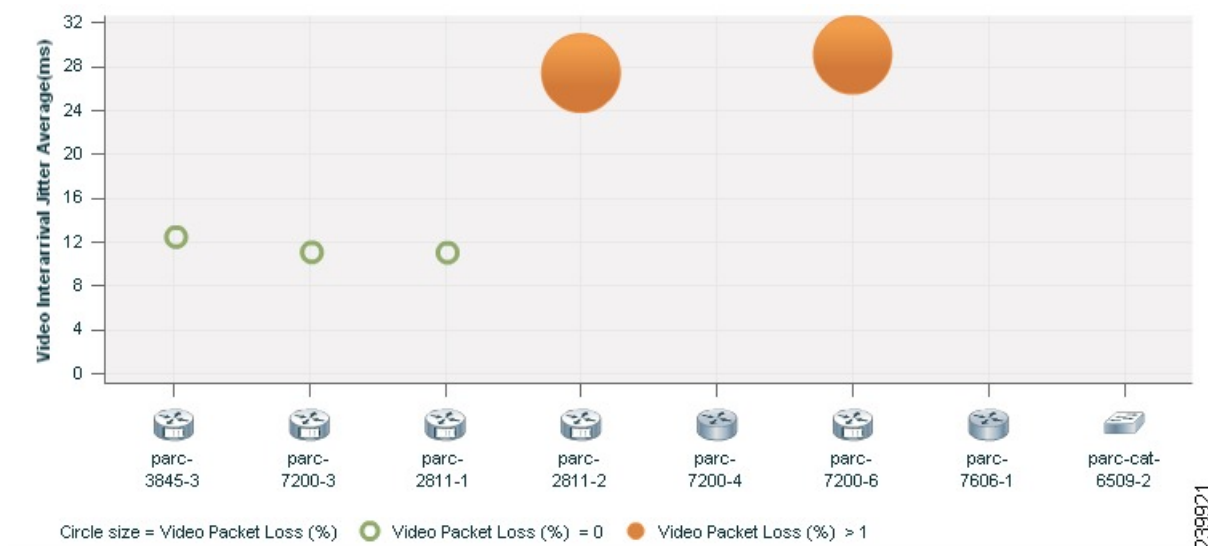
Click on the sphere (red icon) to view the system, interface, and flow details.

Video Interarrival Jitter and Packet Loss

This graph is displayed for all devices and includes the following information:

- The vertical axis (y-axis) provides the average video interarrival jitter in milliseconds (ms).
- The horizontal axis (x-axis) provides lists of all network devices that were discovered during the path trace.
- The spheres in the graph provide the video packet loss details as a percentage.
 - Green sphere indicates that the video packet loss is zero.
 - Orange sphere indicates that the video packet loss is more than 1%. The size of the sphere varies, based on the video packet loss. The smaller the sphere size, the less the video packet loss.

Figure 15: Video Interarrival Jitter and Packet Loss Graph



Click on the sphere (red icon) to view the system, interface, and flow details.

IP DSCP and Packet Loss

This graph is displayed for all devices and includes the following information:

- The vertical axis (y-axis) provides the average IP DSCP (Differentiated Services Code Point). This value is pre-configured on the device.
- The horizontal axis (x-axis) provides lists of all network devices that were discovered during the path trace.
- The spheres in the graph provides the video packet loss details as a percentage.
 - Green sphere indicates that the video packet loss is zero.
 - Orange sphere indicates that the video packet loss is more than 1%. The size of the sphere varies, based on the video packet loss. The smaller the sphere, lesser the video packet loss.

Click on the sphere (red icon) to view the system, interface, and flow details.

Export Troubleshooting Data

You can export the data only after the conference ends. After the troubleshooting job is completed, the troubleshooting job status is displayed in the Conference Monitoring page.

To export the troubleshooting data:

Step 1 Choose **Diagnose > Session Diagnostics**.

The Session Diagnostics page is displayed.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Diagnose > Conference Diagnostics**.

The Conference Diagnostics page is displayed.

- Step 2** Select a past conference, where the troubleshooting status icon displays Troubleshooting Report Available.
- Step 3** Rest your mouse pointer over the Conference Subject column in the Video Collaboration Conference table and click the 360° Conference view icon.
- Step 4** Click **Export Troubleshooting Data** icon in the 360° Conference view window.

The Troubleshooting Report in the HTML file format appears in a new browser window.

Understand the Export Troubleshooting Report

The export troubleshooting report contains the following details:

Report Field	Description
Conference Identifier	A unique ID for the conference.
Conference Subject	Displays whether the conference is ad hoc, scheduled, or static.
Conference Date	Date when the conference occurred.
Conference Start Time	Conference start time.
Conference Duration in Minutes	Duration of the conference.
Conference Type	Displays whether the conference is point-to-point or multipoint.
Endpoints	Details of the endpoints that were part of the conference.
Call Segment	Displays the direction that was used while troubleshooting.
Troubleshooting Conference	Start and end time of troubleshooting workflow.
Troubleshooting Conference ID	A unique ID for the troubleshooting workflow.
Troubleshooting Start Time	Start time of the troubleshooting workflow.
Troubleshooting Initiation	Displays whether the troubleshooting was started manually or whether it started automatically.

Report Field	Description
Path Topology and Metrics	<p>Displays information on the troubleshooting path topology and metrics.</p> <p>The following are the fields and their description:</p> <ul style="list-style-type: none"> • Host Name/IP Address—Name of the host or IP address. • CPU Utilization (Max, Avg)—Displays the maximum and average CPU utilization. • Memory Utilization (Max, Avg)—Displays the maximum and average memory utilization. • Max Packet Loss (Video, Audio)—Displays maximum packet loss for video and audio. • Max Jitter (Video, Audio)—Displays maximum jitter for video and audio. • DSCP (Video, Audio)—Displays DSCP value for video and audio.
Troubleshooting End Time	Start time of the troubleshooting workflow.
Troubleshooting Termination	Displays whether the troubleshooting workflow was ended manually or whether it stopped automatically.

Cisco Prime Infrastructure Cross-Launch

Cisco Prime Collaboration Assurance allows you to perform network diagnosis using the Infrastructure applications. The Cisco Prime Infrastructure 4.1 and 4.2 versions are supported in Cisco Prime Collaboration Assurance.

Cisco Prime Collaboration Assurance requires the Cisco Prime Infrastructure hostname and user credentials to launch the Cisco Prime Infrastructure.

Prerequisites:

- You must ensure that the device is managed in both Cisco Prime Infrastructure and Cisco Prime Collaboration Assurance applications.
- You must ensure that all the required credentials for routers and switches are added in Cisco Prime Collaboration Assurance. For more information, see the [Setting Up Devices for Cisco Prime Collaboration Assurance](#).
- You must ensure that the network devices that contain the Cisco Prime Infrastructure software is accessible from Cisco Prime Collaboration Assurance.

Based on the Cisco Prime Infrastructure user privilege, you can launch the following features of the Cisco Prime Infrastructure application:

- **Device View** — A graphical device management tool that provides real-time views of network devices. These views deliver a continuously updated physical picture of device configuration and performance conditions.
- **Connected Hosts** — Displays details on all hosts that are connected to the access switch.
- **Change Audit Report (24 hours)** — Displays a summary of all changes on the device for the last 24 hours. The changes can be on the software image, configuration file, and hardware.
- **View/Edit Configuration** — Displays the archived device configuration file in the raw and processed format. If you have the required privilege you can also edit the configuration file.
- **Faults (24 hours)** — Displays details on the alerts and events that were triggered on the device in the last 24 hours.
- **Syslog Messages** — Displays details on the syslog messages that were triggered on the device.
- **System Performance** — Displays all performance parameters of the device, such as memory utilization, CPU utilization, interface utilization, environmental temperature, and poller failures.

Cross-Launch Cisco Prime Infrastructure



Note For Cisco Prime Collaboration Release 11.5 and later

Cross launch of Cisco Prime Infrastructure from 360 Integration page is not supported for Cisco Prime Collaboration Assurance 11.5.

To setup cross-launch for Cisco Prime Infrastructure:

- Step 1** Choose **System Administration > 360 Integration**.
- Step 2** Enter the required details in the Cisco Prime Infrastructure Setup pane. See [Cisco Prime Infrastructure Pane - Field Descriptions](#) for more details on field descriptions.
- Step 3** Click **Save**.

Cisco Prime Infrastructure Pane - Field Descriptions

Table 100: Field Descriptions for the Cisco Prime Infrastructure Pane

Field	Description
Cisco Prime Infrastructure Server	<p>Hostname or the IP address of the Infrastructure server.</p> <p>If you have deployed the Cisco Prime Infrastructure in a multiserver setup, you must enter the Cisco Prime Infrastructure master server details.</p>

Field	Description
Prime Infrastructure User and Password	<p>A dummy user, configured on the Cisco Prime Infrastructure server.</p> <p>The Cisco Prime CM server uses these credentials to interact with the Cisco Prime Infrastructure server internally. This user should not have any administrative-related privileges on the Cisco Prime Infrastructure server</p>



CHAPTER 28

Media Path Analysis

This section explains the following:

- [Media Path Analysis, on page 547](#)

Media Path Analysis

This chapter provides information on the various methods to analyze media path analysis.

Analyze Media Paths Using VSAA

The Video SLA Assessment Agent (VSAA) is used in Cisco Prime Collaboration Assurance to provide network path characteristics (that is, latency, jitter, and packet loss) metrics before deploying or upgrading Cisco Video, TelePresence, or IP Video Surveillance (IPVS) systems and site extensions.

Before you begin



Note If you have deployed Cisco Prime Collaboration Assurance in MSP mode, Media Path Analysis is not supported in a NAT environment.

Verify that the VSA Agent is up and running at the two endpoints, and synchronized to the NTP server. You can download the VSA Agent software from the Cisco Prime Collaboration Assurance [software download](#) site on Cisco.com. See [Video SLA Assessment Agent 3.1 Installation Guide](#) for the installation guidelines.

-
- Step 1** Choose **Diagnose > Media Path Analyzer**.
 - Step 2** Enter the required assessment details.
 - Step 3** Enter the [Table 101: Profile Details](#).
 - Step 4** Click **Start**.
-

Table 101: Profile Details

Field	Description
Profile	Displays the profile settings you want to assess. RTP packets sent will be of based on the device type.
Count	Number of devices or streams you want to add to the network. You can add upto five devices.
DSCP	DSCP value indicates priority to traffic quality. The highest quality DSCP value is selected to ensure good quality video streaming.

You must use CTS1000 profile to deploy CTS 500 and 1000 and CTS3000 profile to deploy CTS 3000. You can create, edit, and delete profiles.

VSA Agent Assessment Results

For the individual streams, you can view the topology (layer 2 and layer 3) for the selected direction between endpoints in the **Troubleshooting** tab.

You can view the detailed troubleshooting workflow status for the top level and the individual streams using the **Log** tab. The VSA Agent Assessment result also provides details on the path through the Path Assessment tab. You can view the troubleshooting summary information for testable devices, nontestable device, devices with packet loss threshold violation, devices with jitter threshold violation, and devices with DSCP violation.

A set of tests are run for the devices determined during troubleshooting. To start the Path Assessment test, click **Path Assessment Tests**, after the proactive troubleshooting is complete for the conference.

The Test Result tab displays the following charts. For these charts, only the results of last twenty tests are displayed.

Test Summary

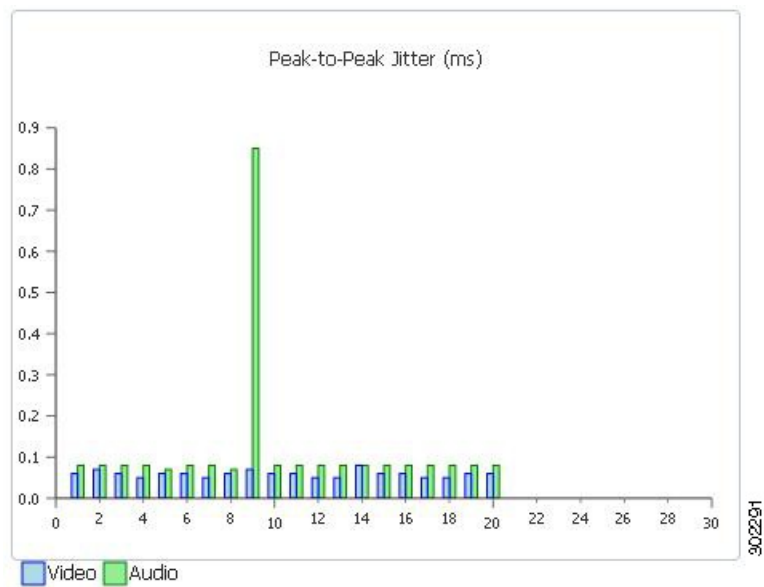
Figure 16: Test Summary

Statistics	Video Result	Audio Result
DSCP	af42(36)	af42(36)
Profile	CTS-1000	CTS-1000
Max Rate	30.02 frames/s	50.04 packets/s
Total Packets Received	439079 packets	44627 packets
Total Packet loss due to Network Drops	0 packets	0 packets
Maximum Seconds of Concealment	0.0 s	0.0 s
Maximum Severe Seconds of Concealment	0.0 s	0.0 s
Maximum Packet Loss	0.0 %	0.0 %
Maximum Jitter	0.01 ms	0.03 ms
Maximum Peak-to-Peak jitter	0.81 ms	0.85 ms
Maximum Peak Playout Delay	0.87 ms	0.83 ms
Maximum Latency	2.32 ms	2.31 ms
Maximum Frame Jitter Average	0.01 ms	0.0 ms
Time Obtained	2012-May-03 21:47:52 PDT	2012-May-03 21:47:52 PDT

3/03/2012

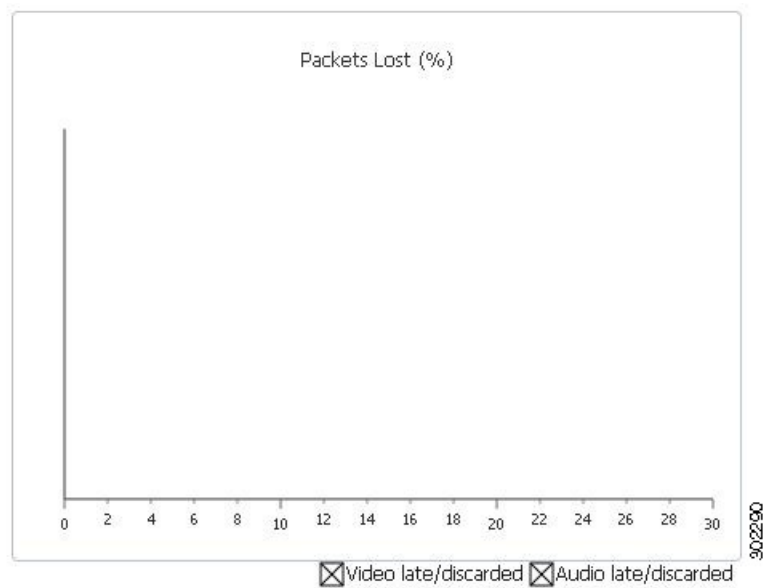
Peak-to-Peak Jitter

Figure 17: Peak-to-Peak Jitter Graph



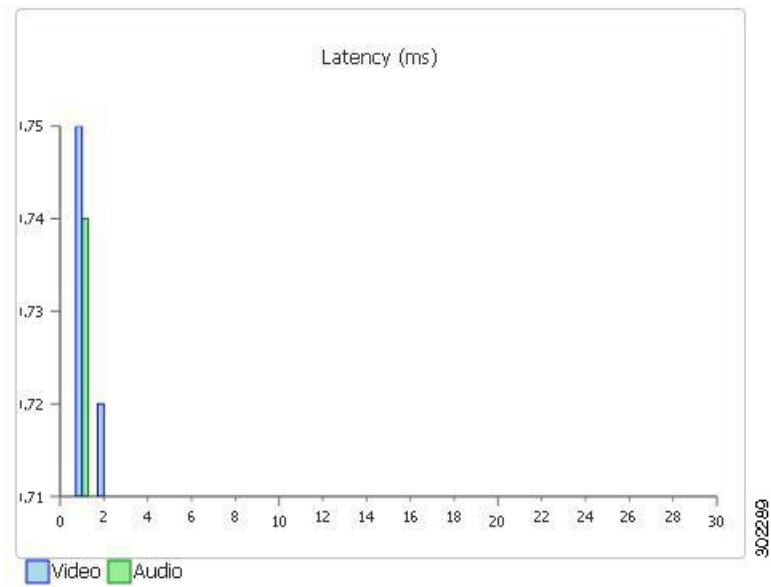
Packets Lost

Figure 18: Packets Lost Graph



Latency

Figure 19: Latency Graph





CHAPTER 29

Collect Logs

This section explains the following:

- [Collect Logs, on page 551](#)
- [Log Collection Center/Device Log Collector, on page 552](#)
- [Set the Trace Levels , on page 554](#)
- [Log Collection Template, on page 555](#)
- [Collect Call Logs, on page 555](#)

Collect Logs

Cisco Prime Collaboration Assurance enables you to collect call logs to identify faults in the calls for Cisco Voice Portal (CVP), Unified Contact Center Enterprise (Unified CCE), Cisco Unified Communications Manager (Unified CM), Cisco Unity Connection (CUC), Cisco IM and Presence (Cisco IM & P), and Cisco IOS Gateways. This feature enables you to troubleshoot issues in the calls. You can use the SIP Call Flow Analyzer feature to further zoom in on the collected calls and isolate faults in the messages. It also helps you to recreate the issue. For more information on the SIP Call Flow Analyzer feature, see [Analyze Call Signaling](#).

It helps you to:

- Reduce cost of troubleshooting issues in calls.
- Reduce time for troubleshooting issues in calls.

Prerequisites

- Ensure that you configure Debug Level for the devices using the Cisco Prime Collaboration Assurance User Interface.

The following is required/supported by this feature:

Maximum disk size required for this feature.	25 GB for small, 50 GB for medium, and very large profiles
Maximum number of devices from which log collection to be done concurrently.	100
Maximum number of log collection jobs to be run at the same time	3

Maximum size of a zipped log file that can be downloaded at one instance.	0.5 GB for small, and 1 GB for other profiles. Note This size is inclusive of all devices and calls. If the zipped file size exceeds the size mentioned above, the log is divided into multiple zipped files of sizes 0.5 GB for small profiles, and 1GB for other profiles.
---	--

**Note**

- Only logs collected from System CLI tool or another Cisco Prime Collaboration Assurance server 10.5 and later are supported.
- Time zone of the device is not collected from the System CLI tool.
- This feature also provides logs for devices which are not in Device Inventory.
- The Operator and Helpdesk users cannot collect call logs from devices and do not have access to **Device Log Collector** menu pages.

Log Collection Center/Device Log Collector

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Assurance enables you to collect call logs from the Device Log Collector available at **Diagnose > Device Log Collector** for the following Unified Communications (UC) components:

Device Type	Supported Release	Components or Type of Log
Cisco Unified Communications Manager (Unified CM)	9.x and later	All
IOS Gateways (TDM, CUBE (Enterprise Edition), VXML GWs)	15.1(4)M and later	Output of show logging command
Cisco Unity Connection (CUC)	9.x and later	All
Cisco IM and Presence	9.x and later	All

Devices Pane

The following information is available in the Devices pane.

- Hostname - Host name of the device
- IP Address - IP Address of the device
- Device type
- Managed in Device Inventory- Displays whether the device is in Managed state in Device Inventory or not. If the column value is No, it means that the device is not in Device Inventory and only added in Device Log Collector, or the device is not in Managed state in Device Inventory.
- Connectivity Status - Displays whether the device can be accessed with the credentials provided in Device Log Collector.

- TimeZone - Displays the device time zone.

To add or update device(s) (UC components) of Device Inventory to Device Log Collector, you can select a device, all devices of a device group and then click **Sync to Inventory Management**. The devices in the Device Log Collector and **Device Inventory** are synced in the following ways:

- Automatically: Devices from Device Inventory are synced every hour.
- Manually: When you click the **Sync to Inventory Management** button, the UC components from Device Inventory are added to the list of devices in the Device Log Collector.

Periodic sync happens every hour. Sync does not remove devices from Device Log Collector if the devices in Device Inventory are deleted. If a new device is added in Device Log Collector or any update to a device happens, then the Connectivity Status is updated after the sync.



Note

- The direction of the sync is only from Device Inventory to Device Log Collector.
- The credentials from Device Log Collector are overwritten by the credentials in Device Inventory after a sync. Thus we recommend you to keep the credentials same across Device Inventory and Device Log Collector.
- Only the devices in Managed state in Device Inventory are synced.
- If a device in Device Inventory is deleted but not deleted in Device Log Collector, you can still perform log collection in Device Log Collector,
- If the IOS gateway in Device Inventory does not have CLI credentials, it will not be synced to Device Log Collector.

Group a Device

In order to collect log from the same type of UC components on a same-time, you can create custom group of UC components and collect call logs by selecting the device group.

Predefined groups can not be added, edited, or deleted, and the devices in the groups cannot be modified too.

You can create, edit or delete user-defined groups. You can add or delete devices of the user-defined groups. You can do the following:

For Cisco Prime Collaboration Release 11.5 and later

Task	Details
Create a Group	Click Diagnose > Device Log Collector > Group > Create New .
Edit a Group	Click Diagnose > Device Log Collector , select a device or a group, and then click Group > Edit Group .
Delete a Group	Click Diagnose > Device Log Collector , select a device or a group, and then click Group > Delete Group . It takes
Add Devices to Group	Click Diagnose > Device Log Collector , select a device or a group, and then click Group > Delete Group . It takes
Delete Devices from Group	Click Diagnose > Device Log Collector , select device(s), and then click Group > Add to Group .
View Devices in Group	Select a group from the Device Group Center. The devices of that group are displayed in the Devices pane.

Other Tasks

You can perform the following tasks from the Device pane on the Device Log Collector page. Select device(s) from the Devices pane for which you want to perform the task, and then do the following as required.

Tasks	Details
Modify Credentials	Click the Modify Credentials button to edit the port number or credential details of device(s). You cannot modify the device type.
Modify Time zone	Click the Modify Time Zone button to modify the device time zone. Cisco Prime Collaboration Assurance server time zone is shown by default.

Test Connectivity of a Device

Select a device and click the **Test Connectivity** button to test if the device is accessible with credentials provided. A message is displayed to notify you about the result. The value of the column “Connectivity Status” is updated accordingly.

Troubleshoot Test Connectivity

If test connectivity fails, check the following:

- Port number
- Credentials of the device and ensure that they are same as Device Inventory.
- Ping from the Cisco Prime Collaboration Assurance Server to the device is successful.

Set the Trace Levels

This feature helps you to set the trace level for each component of the devices. You can set the trace level for the following devices:

- Cisco Unified Communications Manager
- IOS Gateway
- Customer Voice Portal
- Cisco Unity Connection
- Cisco IM and Presence

For Cisco Prime Collaboration Release 11.5 and later

Choose **Diagnose > Device Log Collector**.

Select the device or devices for which you want to set the trace level, and click on the **Set Trace Level to Devices** button. The Set Trace Level to Devices popup window is displayed. Select a device from the Device Type drop-down list. The components for the selected devices are listed. You can select the appropriate Trace level (No Change, Default, Warning, Information, Debug) for the components relevant to the problem you are experiencing, and click the Apply button.



Note

Setting trace levels may affect network performance adversely.

Log Collection Template

The log collection template enables you to collect logs of different devices and different components together. It is mandatory to use a template to collect logs. You can create a new template or use the default template.

To create a template:

Step 1 For Cisco Prime Collaboration Release 11.5 and later

Choose **Diagnose > Device Log Collector**, and click the **Manage Trace Template** button.

Step 2 On the Manage Trace Template page, click **Add**.**Step 3** Enter a template name and description, and select a Device Type and its components in the Component pane. You can select multiple (or all) devices and components also. For more information on the components, see [Log Collection Center/Device Log Collector](#).

There is a default template available called Call Trace. This template has four device types - (Unified CM, Unified CCE, CVP, and IOS Gateway), and has preselected components. You cannot modify this template.

Step 4 Click **Save**. A message notifies you that the template is saved successfully. You can view the new template listed under Templates on the Manage Trace Template page.

To view the components of a particular template, select a template, and click **Summary**. To modify a template, select a template. You can modify the template name, description, and the components. To delete a template, select a template, and click **Delete**.

Note Only a Super administrator can create, edit, and delete the template. Other users can only view the template summary and use the templates for log collection.

Collect Call Logs

Log collection is on-demand.

Select a single device or devices in a group and click the **Collect Logs** button to collect logs. The Collect Logs dialog box is displayed. Fill the required information. The job name and file name are autopopulated, but you can modify it too. The time zone you select here is used to collect the logs.

Select a template from the Use Template drop-down list.

Click **Run**. A message notifies you that the job is triggered or not. The job is listed under the Log Collection Jobs pane. The Progress Status column also shows the number of devices for which the logs are downloaded out of the total number of devices selected for log collection. For example 2 of 3. You can select the job and collect the logs by clicking the **Download to local** button. If the zipped log file size is more than 0.5 GB (for small profile) or 1 GB (for medium or large profiles), it is divided into multiple zipped files.



Note Ensure that you do not modify the extension **.zip** in the file name. Sometimes the extracted file from the zipped folder may have **.gz** extension.

You can delete the job using the **Delete** button under the Log Collection Jobs pane.

These jobs are also listed under the Job Management page (**System Administration > Job Management**), however you cannot download the log file from this page.



Note

If you want more information on log collection jobs, see <https://<ip-address>/emsam/log/Troubleshoot/LogCollectionManagerImpl.log> where IP address is the Cisco Prime Collaboration Assurance server IP address. This URL can be viewed by users with administrator role and helps you troubleshoot issues related to log collection.



CHAPTER 30

Analyze Call Signaling

This section explains the following:

- [Analyze Call Signaling](#) , on page 557
- [Supported Call Flows](#) , on page 559
- [Create a Call Ladder Diagram](#), on page 560
- [Filter a Message in the Call Ladder Diagram](#), on page 563
- [Understand a Call Ladder Diagram](#), on page 563

Analyze Call Signaling

The SIP Call Flow Analyzer enables you to determine the reason of call failure. SIP Call Flow Analyzer analyzes calls at a high level and then drills down to a lower level within the components themselves using the same tool.

The SIP Call Flow Analyzer helps you to:

- View the high-level view of the signaling path that includes originator, intermediate destination and final destination of calls to know the complete path of the call.
- View the signaling call ladder diagram to isolate any issues in the call.
- Drill down to individual components in that call to fix errors.
- View error messages, and possible root causes and recommendations.
- Automatically identify and highlight signaling errors and capability mismatches.
- Add any additional logs of Unified CCE to generate the Call Ladder Diagrams for Unified CCE deployments.

It analyzes call logs received from the following Unified Communications components:

Device Type	Supported Release in Advanced Mode	Components or Type Of Log
Cisco Unified Contact Center Enterprise (Unified CCE)	9.x and later	Router
Cisco Voice Portal (CVP)	9.x and later	All
Cisco Unified Communications Manager (Unified CM)	9.x and later	Call logs, and SDL logs

Device Type	Supported Release in Advanced Mode	Components or Type Of Log
IOS Gateways (TDM, CUBE (Enterprise Edition), VXML GWs)	15.1(4)M and later	Output of show logging command

Prerequisites

- You must add the Contact Center Assurance license to analyze call logs of Unified CCE and CVP devices. However, you can continue to use this feature for Unified CM.
- For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)
 - [Configure Devices for Cisco Prime Collaboration Assurance](#)
- Ensure that you complete the configuration mentioned in following sections:
 - Configure Debug Level 3 for Unified CCE - Section "Configure Debug Level 3 for UCCE Using System CLI"
 - Configure Debug Level 3 for CVP - Section "Configure Debug Level 3 for CVP Using System CLI"
 - Configure IOS Gateway - Section "Configure IOS Gateway"



Note

- The Advanced mode allows log analysis from any of supported devices (Unified CM, CVP, IOS Gateway, Unified CCE)
- Only SIP over TCP messages are parsed.
- For Unified CM - If both SDL/SDI and Call Logs are available then calls are parsed from SDL/SDI logs. If data is not available from the SDL/SDI logs, then call logs are used.
- Only logs collected from System CLI tool or another Cisco Prime Collaboration Assurance server 11.0 are supported.
- Time zone of the device is not collected from the System CLI tool.
- When Contact Center Assurance license expires, the SIP Call Flow Analyzer fails to analyze the logs received from Contact Center devices (UCCE and CVP). For more information on licensing, see the *Manage Licenses* chapter of [Cisco Prime Collaboration Assurance Guide-Advanced](#).
- The Operator and Helpdesk users cannot collect call logs from devices and do not have access to signaling call ladder diagram and **SIP Call Flow Analyzer** menu pages.

The following is required/supported by this feature:

Maximum disk size required for this feature.	18 GB for small, 35 GB for medium, and large profiles
Maximum file size that can be imported.	0.5 GB for small, and 1 GB for other profiles.
Maximum number of calls that can be selected for ladder generation at a time.	25

Maximum number of devices from which log collection to be done at a time.	100
Maximum size of a zipped log file that can be parsed at one instance.	0.5 GB for small, and 1 GB for other profiles. Note This size is inclusive of all devices and calls. If the zipped file size exceeds the size mentioned above, the log is divided into multiple zipped files of sizes 0.5 GB for small profiles, and 1GB for other profiles.
Maximum number of call records displayed on the user interface.	10,000
Maximum number of jobs supported concurrently.	Only one analysis job should be performed at a time.
Time to perform analysis of one log file.	It depends on the size of the file; however for a 1 GB file, the estimated time is 2 hours.

Supported Call Flows

The Call Trace feature enables you to analyze SIP-based calls.



Note The correlation of analysis of all the call legs of the same call (end-to-end call analysis) is only supported for Call Flow 1 and 2. To support end-to-end call analysis for these calls (Call Flow 1 and 2), the CISCO-GUID (SIP Message property) should be same across different products. End-to-end call analysis is not supported for the other call flows except Call Flow 1 and 2.

It supports the following call flows:

Figure 20: Call Flow 1

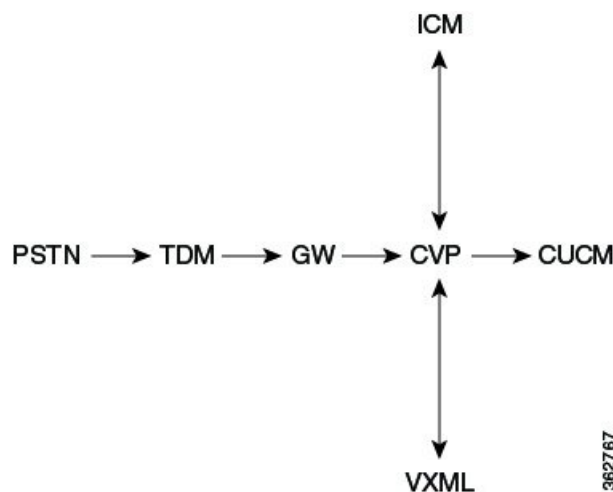


Figure 21: Call Flow 2

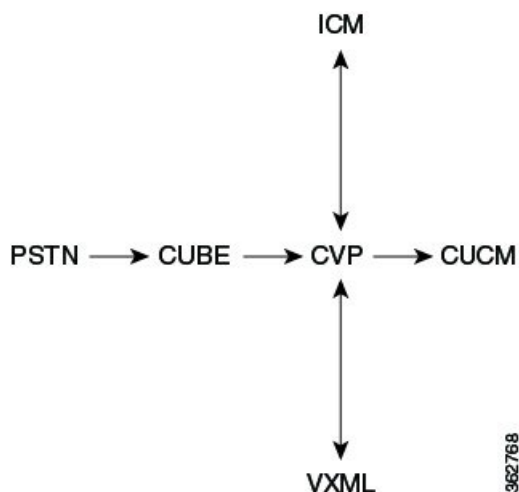


Figure 22: Call Flow 3



Figure 23: Call Flow 3 A

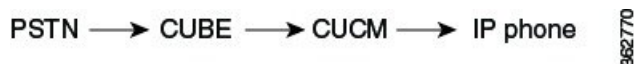


Figure 24: Call Flow 4



Figure 25: Call Flow 5

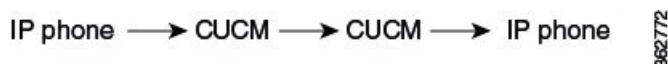


Figure 26: Call Flow 5 A

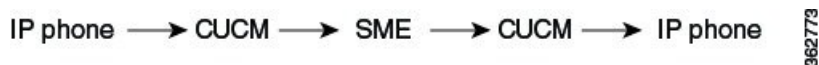
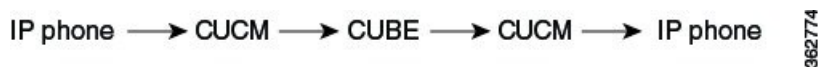


Figure 27: Call Flow 6



Create a Call Ladder Diagram

Step 1 Select a data source. Choose from the following options:

- Live Log Collection - The Group Type field is displayed. Click on the drop-down arrow, and select a device group from the Device Group dialog box. The devices available for the selected device group appear. Select a device from the options that are listed.

Note You can select a single or multiple devices.

- Local File System - You can select a log file from the options that appear. It includes log files collected from Device Log Collector and also from Live Log Collection. You can also click Import, to import the file(s) from your local file. Browse to the zipped log file through the Import dialog box. Based on the mode of deployment, you can associate a customer or a domain to the imported logs using domain/customer drop-down list in the Import dialog box. The imported file is updated in the options available under Log File System. For more information on Device Log Collector, see [Log Collection Center/Device Log Collector, on page 552](#). You can also export the log files using the Export button.

The .gz, .gzo and .zip file formats are supported for import. The files are exported in .gz, .gzo and .zip file formats too. You can attach a single log file only. If the zipped log file size is more than 0.5 GB (for small profile) or 1 GB (for medium or large profiles), it is divided into multiple files of sizes 0.5 GB (for small profile) or 1 GB (for medium or large profiles) for import tasks.

You can delete a log file also if you have selected the log file system. It takes time to cleanup folders and processed records and thus there may be delay in completion of this task.

Step 2

(Optional) Filter Calls - You can search for a call from the files selected from the preceding data sources, using the following parameters:

For Cisco Prime Collaboration Release 12.1 SP3 and later

Note During live log collection, you can now filter the results by the Calling Number/URI field. This is applicable for the following fields - Calling Number/URI, Called Number/URI, Call ID, and GUID. Ensure the following guidelines are met before performing a search.

- Give one or more digits of the calling number.
- Special characters like '*' search is not allowed.

For Cisco Prime Collaboration Release 12.1 SP3 and earlier

Field	Description
Calling Number/URI	A SIP-URI is the SIP addressing schema to call another person through SIP. By default ALL listed.
Called Number/URI	By default ALL listed.
Disconnect Code	The error code for that call, for example - 200 OK.
Call ID	An ID that uniquely identifies calls in a Cisco UC product. Each Call Leg of a call has a different Call ID.
GUI ID	An ID that uniquely identifies calls across product.
Time Zone	By default it displays the Cisco Prime Collaboration Assurance server time zone.
Heartbeat Messages	This includes the heartbeat messages - OPTIONS, and NOTIFY. If you select this field, performance of this feature may be adversely affected.
Time Range	You can specify the time range. if you have selected the Local File System, the option of past time details will not be available to you. Ensure that you select a time range within which the calls had happened.

Device Type to Parse	The device types that are part of the selected logs are listed here. You can select a particular device type to filter the calls that involve that device type.
Maximum Number of Calls	By default this value is set to 500. If you set a higher value, it may take longer time to display the records. Thus we recommend that you set appropriate filters.
Initial Message	Initial Message is selected as INVITE (first message of a call for a particular call ID) by default. You can select a different Initial Message.
Comment	You can add your comments to show when, where, and why the logs are collected.

Step 3 Click the **Retrieve Calls** button. If you have selected the Live Log Collection option, Log Parsing In Progress status bar is displayed. After the log parsing process is completed, the Log Download In Progress status bar is displayed, indicating the process completeness. If you have selected the Local File System option, the Log Download In Progress status bar is displayed directly. If you try to parse an uploaded or existing log file, the Log Analysis In progress status bar does not appear as that file is already parsed.

The IOS Gateways and Unified CM call logs can have older data. You need to apply appropriate filters to get the specific time range call list.

In case of Local File System option, the file is first unzipped, parsed and then analyzed.

In case of Live Log Collection option, the file is first downloaded, unzipped, parsed, and then analyzed.

Step 4 The Call List is displayed. Select the calls from this list, and click on **Show Ladder Diagram** for those calls. The Call Ladder diagram page is displayed.

Call Ladder diagram opens in a new tab.

Note If you are using the call processor - Unified CM in your deployment, each call Leg of a call has a different Call ID. Thus to view the Call Ladder diagram of the complete call, select all the call legs from the Call List and then click the **Show Ladder Diagram** button.

You can also click on the **Show Transition Diagram** button when the call list is displayed to view the message transitions of the call. The Unknown errors are the same as Unexpected errors.

Figure 28: Transition Diagram



The screenshot shows a web interface titled "Transitions : 44589780-33c197b4-d-b8ac12ac@172.18.172.184". It contains a table with three columns: From, To, and Event. The table lists the sequence of messages in a call, such as Init, WaitFor2xx, SendAck, Connected, and Success, along with the corresponding events like sent.invite, recv.1xx, and sent.Bye.

From	To	Event
Init	WaitFor2xx	sent.invite
WaitFor2xx	WaitFor2xx	recv.1xx
WaitFor2xx	WaitFor2xx	recv.1xx
WaitFor2xx	SendAck	recv.2xx
SendAck	Connected	sent.Ack
Connected	WaitForFinal2xx	sent.Bye
WaitForFinal2xx	Success	recv.2xx

If calls do not appear, check for the following:

- Filter is applied correctly.
- The selected time zone range matches the actual device time zone.
- Appropriate debug levels are set on the device before using the feature. See the list on setting up devices and configure devices for Cisco Prime Collaboration Assurance at the following locations:
 - [Setting Up Devices for Cisco Prime Collaboration Assurance](#)

- [Configure Devices for Cisco Prime Collaboration Assurance](#)

Filter a Message in the Call Ladder Diagram

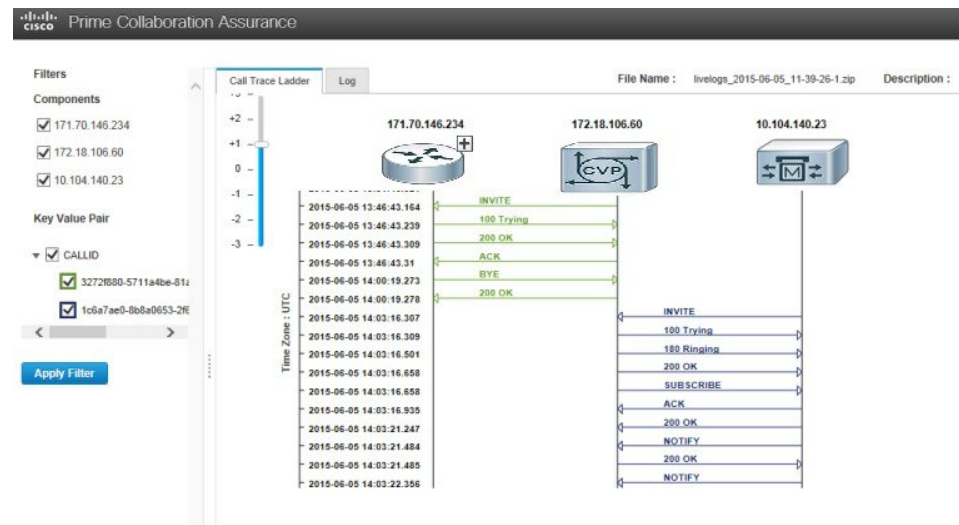
You can further create a call ladder diagram for a specific message.

- Step 1** You can also filter a message in the call ladder diagram on the following parameters:
- Components - The IP addresses of the devices (senders and receivers) in the call.
 - Key Value Pair - Attributes of the Call. This includes Call ID and GUID
- Step 2** Select the parameters and click **Apply**. The diagram is generated according to the filters you have applied.

Understand a Call Ladder Diagram

The Call Ladder diagram helps to visualize the SIP signaling for selected calls (both line and trunk side).

Figure 29: Call Ladder Diagram



You can see the following:

- Direction of the messages
- Sender and Receiver
- Time Stamp of the individual messages. The Call Ladder diagram shows UTC time zone only.
- Message and the Message Label. You can click on the message arrow to launch the Call Details popup window that displays the details of the call. You can do the following:
 - View details of the call.

- You can filter the on the Call ID through this window.
- You can view the device time stamp and time zone. This time stamp is converted into UTC and displayed too.
- You can click on **Click here for log** to see the log snippet of the message (highlighted in yellow) you had clicked on.

You can click on the **Logs** tab to view the log snippets of selected messages. When you click for the first time no logs are displayed.

**Note**

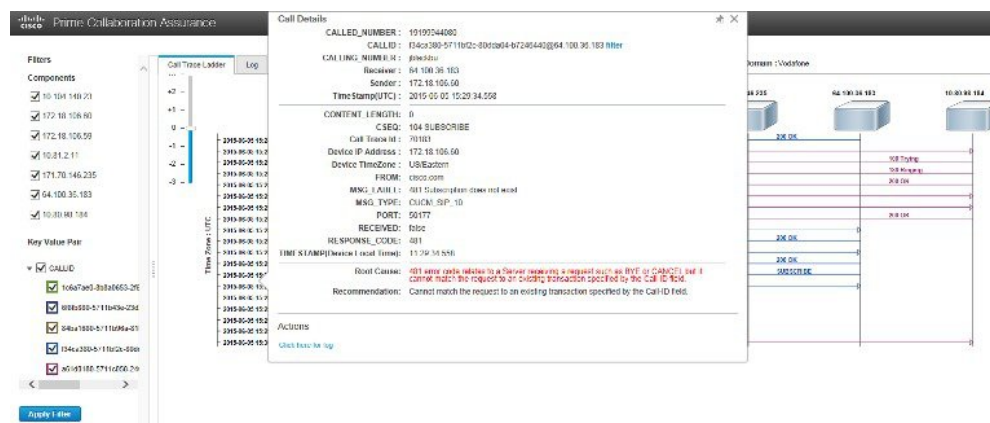
By default, the log snippets of the last message selected by clicking on the **Click here for log** button on the Call Details popup window appear. To see the logs for a particular message, click on the message arrow on the Call Ladder diagram to launch the Call Details popup window. Now, click the **Click here for log** button.

**Note**

If there are no details of the device type in the log, you see a plain grey device icon without any markings in the Call Ladder diagram. This shows that the device is unknown.

If you filter calls by selecting only certain devices in the Device Types to Parse field for creating a diagram, there may be components of the call (devices which have not been selected in the Device Types to Parse field) which can help in troubleshooting the call. Logs related to that device are also parsed and displayed to help you debug. These devices appear with a plus sign icon. Click the plus sign to expand the Call Ladder Diagram. The dotted line represents that a new component is added as part of the expansion. Based on time stamp order of the messages, rearrangement of the devices may happen.

Figure 30: Call Details Popup Window



If there is any error in the call, that message arrow is shown in red color. You can click on the arrow to open the Call Details popup window to view the Root Cause of the error and also the Recommendation to help you troubleshoot the cause of the call failure.

Each Call Id is differently color coded and the schema is represented below the diagram.

You can zoom in and zoom out the diagram.



PART IX

Maintain the Server

- [Manage Jobs, on page 567](#)
- [Purge Policies, on page 573](#)
- [Perform Backup and Restore, on page 575](#)
- [Set Log Levels, on page 583](#)



CHAPTER 31

Manage Jobs

This section explains the following:

- [Manage Jobs, on page 567](#)

Manage Jobs

Cisco Prime Collaboration Assurance allows you to view the details of all immediate and scheduled jobs in the Jobs pane. The manually scheduled jobs are discovery, update inventory, and import conferences. The polling jobs are triggered based on user-configured values.

[Table 102: Job Details](#) describes the fields that are displayed on the **Job Management** page (**System Administration > Job Management**). To get the latest information, refresh the page.

Table 102: Job Details

Field	Description
Name	Description of the job as defined in the Cisco Prime Collaboration Assurance server.
Type	Indicates the type of the job.
Description	Describes the job.

Field	Description
Status	<p>Status of a job. It can be:</p> <ul style="list-style-type: none"> • Completed—Job has completed. If a job has completed, it does not necessarily mean that the job has been successful. There may be instances, where the job might have failed to run on a few devices. You can view the job details in the Job Instances table by clicking the arrow on the far left of the page. • Cancelled—Job has been cancelled. You can cancel a scheduled job. However, you cannot cancel a running job or a system job (for example, a polling job). • Scheduled—Job is scheduled to execute at a specific time. It can be scheduled to run at a single time or at several times-recurring job. • Suspended—Job is halted temporarily and can be later resumed for execution. • Running—Job is in execution.
Owner	User, who created the job. If it is a predefined system job, the creator is displayed as <i>SYSTEM</i> .
Job Start Time	Time when the job is scheduled to run for the first time.
Job End Time	Time up to which the job remains active. The job becomes inactive after running all scheduled instances of the job.
Next Scheduled Time	Start time of a subsequent job instance. This applies to a recurring periodic job. If it is either an immediate job or one-time job, the time displayed for Job Start Time and Next Scheduled Time is the same.
Schedule Type	Whether the job is scheduled to run at a periodic frequency or once.
Job Details Pane	
Run ID	If it is a periodic job, it displays the job instances count. If it is not a periodic job, it displays zero.
Status	Status of the job instance of the same job. Hover the mouse over the quick view icon in this column to view the job instance results.
Status Progress	Indicates the stage of the job and the percentage complete.

Field	Description
Results	Indicates the job was successful or a failure.
Start Time	Start time of a job instance of the same job.
End Time	End time of a job instance of the same job.
Duration	Time taken between the Start Time and End time of a job instance of the same job.



Note For more information on Purge Policies, see [Purge Policies Table, on page 573](#).

Schedule a Job

You can schedule a job and set options using the **Schedule and Settings** tab under the **Job Details** pane.



Note The schedule and settings tabs are enabled for discovery jobs only. Discovery jobs can be scheduled through Inventory Management page only. You cannot schedule jobs in Job Management page.

You can only modify the schedule of discovery job that has one of the following status:

- Scheduled
- Failed

To schedule a job:

Step 1 Choose a job under the Jobs pane, and click the **Schedule** tab under the Job Details pane.

Step 2 In Schedule Options, choose the start time, end time and recurrence.

You can set the recurrence to Daily, Weekly or Monthly to specify a day and frequency. You should select Hourly to schedule a job every few hours as needed.

The schedule is defined. If you set the recurrence to None, you cannot specify other frequency details.

You can configure the following types of intervals:

Table 103: Types of Intervals and their Schedule

Type of Intervals	Schedule
None	You cannot specify other frequency details.
Hourly	Job begins at the specified start time for the first time and then at specified intervals, that is, for every few hours as specified (days:hours:minutes).

Type of Intervals	Schedule
Daily	<p>Job is completed once a day.</p> <p>Indicates the job starts every day at a designated time specified as HH:MM.</p> <p>For the time daily, the scheduler assumes a start time every day at a specified time.</p>
Weekly	<p>Job is completed once a week.</p> <p>Indicates that the job starts on a specified day of the week.</p> <p>Day of the week (dow) specified as one of the following: An integer such as 1 = Sunday, 2 = Monday, and so on.</p> <p>For example, The scheduler assumes a start time every Friday (if the selected day of the week is Friday) at a specified time.</p>
Monthly	<p>Job is completed once a month.</p> <p>Indicates the job starts on a specified day each month.</p> <p>If you specify either First, Second, Third, or Fourth the job is started on the specified week of the day every month.</p> <p>For example, For the time monthly, the scheduler assumes a start time on the specific week and on a specific day of every month at a specified time.</p>

Step 3 Click the **Settings** tab and choose the options that follow.

The job runs according to the settings you have defined. The job status for that job is set to Scheduled in the Jobs pane.

Note CMEPhoneDiscovery and PhoneXML Discovery Job is scheduled at regular intervals, that is, every 4 hour(s). If the Recurrence is set to 'None' you cannot change it back to schedule but rather restart Cisco Prime Collaboration Assurance.

Step 4 Click **Save**.

Defining a Timetable

You can define a timetable in the scheduler to be used with one or more jobs. The scheduler considers the current time.

For example, if the current date and time is 2017/06/23, 13:48:00 IST, then jobs are started as follows:

Scheduler
Start Time: 2017/06/20 06:27 PM
Recurrence: Hourly
Every: 5 hours

Scheduler
Job Start Time: 2017-Jun-20 13:27:00 IST
Next Scheduled Time: 2017-Jun-20 15:27:00 IST

The job runs once at the Job Start Time.

The next scheduled time of a job does not depend on the hour(s) of the Start Time. It takes the next immediate multiple of the number of hour(s). The sequence of the Next Scheduled Time of this job will be as follows -

1. 2017-Jun-20, 15:27 hours (Next Scheduled Time)
2. 2017-Jun-20, 20:27 hours (15:27 + 5)
3. 2017-Jun-21, 00:27 hours (Time resets to 00:27 hour(s))
4. 2017-Jun-21, 05:27 hours (00:27 + 5 = 05:27)
5. 2017-Jun-21, 10:27 hours (05:27 + 5 = 10:27)


Note

The scheduler will not begin the next occurrence of a job before the last one completes.

For example, if you have scheduled a job to be completed at one-minute intervals beginning at 22:00; but the job requires two minutes to complete. The scheduler starts the first job execution at 22:00, actual completion at 00:02.

Cancel a Job

You can cancel a discovery job that is in the **Scheduled** state, using **Cancel Job**. However, you cannot cancel a job if its status is one of the following:

- Cancelled
- Completed
- Failed
- Running

Also, you cannot cancel the following jobs:


- Polling—Any job starting with the word *Polling*; for example, *Polling_CTS-HEALTH_*, *Polling_TelepresenceSystem_*, *Polling_CtsMAN-HEALTH_*, and so on).
- Purging—Any job starting with the word *Purging*.

Predefined Quick Filters

Cisco Prime Collaboration Assurance supports the following predefined quick filters:

- All Discovery Jobs—An example of a discovery job is *DiscoveryFrmBackgroundPathtrace*. Discovery jobs are listed when you perform device discovery or rediscovery or update inventory tasks, by using

For Cisco Prime Collaboration Release 11.5 and later**Inventory > Inventory Schedule > IP Phone Inventory Schedule.**

You can view the Job Instance Result—Hover your mouse pointer on values in the Run ID column on the Job Details pane and click the Quick View icon  to view the Total Device Summary and Endpoint Device Summary.

- All Polling Jobs—An example of a polling job is MCU_Conference_Import. Polling jobs are automatically created at system setup.
- All Report Jobs—Report jobs are listed when a report is run.
- All Session Import Jobs—An example of a session import job is MNGD_Synch_CtsMAN-MEETING. Sessions are imported from Cisco TMS. A separate job is created for each of these management applications.

• For Cisco Prime Collaboration Release 11.5 and later

All Conference Import Jobs—An example of a conference import job is MNGD_Synch_TMS-MEETING. Conferences are imported from Cisco TMS. A separate job is created for each of these management applications.

- All System jobs—System-generated jobs such as discovery, polling, and so on. System-generated jobs are listed as soon as the system performs a job.
- All User Jobs—An example of a user job is RediscoverDevices_1347339631540. User jobs are listed as soon as a user runs a job.
- Jobs Run in Last 24 Hours—An example of a job run in the last 24 hours is Discovery 2012-Sep-13 10:32:40 UTC. Lists all jobs whose last complete time (the last run instance) is within the last 24 hours (from the current time).

Related Topics

[Discover Devices](#)



CHAPTER 32

Purge Policies

This section explains the following:

- [Purge Policies](#) , on page 573
- [Purge Policies Table](#), on page 573

Purge Policies

Cisco Prime Collaboration Assurance uses the following purge policies.

Purge Policies Table

Table 104: Purge Policies Table

Module	Purge Policy
Monitor Faults	Cleared alarms are purged in 30 days (4 weeks).
	Events are purged in 60 days (8 weeks).
	If an alarm is purged, all associated events are also purged. Active events and alarms are not purged.
	If the threshold rules for any performance counter of a device are purged, the associated active alarms are also purged.
Monitor the Network	All conferences and endpoint statistics data older than one day are purged.
	All sessions and troubleshooting details older than 14 days are purged every hour.
	For Cisco Prime Collaboration Release 11.1 and earlier All conferences details older than 14 days are purged every hour.

Module	Purge Policy
Dashboards	Call quality event history, and audio/video phone audit report data older than 30 days are purged.
	For Cisco Prime Collaboration Release 12.1 and later
	Call quality event history and endpoint related audit report data older than 30 days are purged.
	CDR reports older than seven days are purged.
	CMR records older than seven days are purged.
	Data from Sensor, older than seven days is purged.
	Data from Cisco Prime NAM/vNAM, older than seven days is purged.
	If a performance dashboard is not open for more than 30 minutes, the cache memory is purged until the next time the custom dashboard is launched.
	If the historical trend option is disabled for custom dashboard counter(s) or the dashboard is deleted, all the polled data in the database is purged.
Perform Diagnostics	IP SLA Voice Test Data - Cisco Prime Collaboration Assurance purges all data files (saved test data) more than 31 days old. You must save the test to another server to maintain data for more than 31 days.
Maintain the Server	Jobs that are older than 14 days and have a status of completed, failed, or cancelled are purged every hour.
	Event and Alarm Database - All events and alarms, including active and cleared, are persisted in the Cisco Prime Collaboration Assurance database. The relationships between the events are retained. The Alarm and Event Browser lets you review the content of the database. The purge interval for this data is four weeks.
Job Management	Jobs that are older than 32 days are purged.



CHAPTER 33

Perform Backup and Restore

This section explains the following:

- [Perform Backup and Restore](#), on page 575

Perform Backup and Restore

You can schedule periodic backups using the Cisco Prime Collaboration Assurance user interface.

Cisco Prime Collaboration Analytics data is backed up on a remote server using SSH. It does not use the Cisco Prime Collaboration Assurance backup repository. You can backup the analytics data only through User Interface, and restore the data through CLI.



Note

Linux server is recommended for Cisco Prime Collaboration Analytics backup.

You can also backup Cisco Prime Collaboration Analytics on Windows server. Backup supports in Cygwin UNIX shell. Backup support in Windows server is not available using other SSH tools or Unix Shell.

Related Topics

[Monitor Conferences](#)

[Troubleshooting Workflow for Video Endpoints](#), on page 527

[Purge Policies](#), on page 573

[Concepts](#), on page 39

Overview of Backup and Restore

Cisco Prime Collaboration Assurance uses the following purge policy:

- All conference and endpoint statistics data older than one day are purged.

- **For Cisco Prime Collaboration Release 11.5 and later**

All conference and troubleshooting details older than 14 days are purged every hour.

- **For Cisco Prime Collaboration Release 11.6 and earlier**

Call quality event history and audio/video phone audit report data older than 30 days are purged.

For Cisco Prime Collaboration Release 12.1 and later

Call quality event history and endpoint related audit report data older than 30 days are purged.

- Cleared alarms and events that are older than 14 days are purged every hour. If an alarm is purged, all associated events are also purged. Active events and alarms are not purged.
- Jobs that are older than 14 days and have a status of completed, failed, or cancelled are purged every hour.

The backup and restore service allows you back up the database, configuration files, and log files to either a remote location or a local disk. Files in following folders are backed up by the backup service:

Type of Data for Assurance Backup
Assurance database
Configuration files
Type of Data for Analytics Backup
Analytics database
Log files
Reports (Scheduled Reports and Custom Reports)
Logos

Backup Time Period

Depending on the number of managed devices in the Cisco Prime Collaboration Assurance server, the data backup should take:

- Upto 150,000 endpoints - 4 hours
- Upto 80,000 endpoints - 3 - 2.5 hours
- Upto 20,000 endpoints - 2 hours
- Upto 3,000 endpoints - 1 hour

**Note**

To achieve the preceding time periods, the network latency should not be more than 20 ms.

We recommend you to schedule backups during the non-business hours, because, this operation can slow down the Cisco Prime Collaboration Assurance user interface performance.

Create a Repository on FTP, Disk, SFTP, or TFTP Server

You must create a repository before backing up the Cisco Prime Collaboration data. By default, the backup service creates a *.tar.gpg file under the configured repository. The backed-up file is in a compressed format. The repository can be on CD-ROM, disk, HTTP, FTP, SFTP, or TFTP.

For Cisco Prime Collaboration Release 11.6 and earlier

Step 1 Log in to the Cisco Prime Collaboration server with the account that you created during installation. The default login is *admin*.

Step 2 Enter the following commands to create a repository on the local:

```
admin# config t
admin(config)# repository RepositoryName
admin(config-Repository)# url disk:
admin(config-Repository)# exit
admin(config)# exit
```

Enter the following commands to create a repository on FTP server:

```
admin# config t
admin(config)# repository RepositoryName
admin(config-Repository)# url ftp://ftpserver/directory
admin(config-Repository)# user UserName password {plain | hash} Password
admin(config-Repository)# exit
admin(config)# exit
```

Where:

- *RepositoryName* is the location to which files should be backed up. This name can contain a maximum of 30 alphanumeric characters.
- *ftp://ftpserver/directory* is the FTP server and the directory on the server to which the file is transferred. You can also use SFTP, HTTP, or TFTP instead of FTP.
- *UserName* and **{plain | hash}** *Password* are the username and password for the FTP, SFTP, or TFTP server. **hash** specifies an encrypted password, and **plain** specifies an unencrypted plain text password.

For example:

```
admin# config t
admin(config)# repository tmp
admin(config-Repository)# url ftp://ftp.cisco.com/incoming
admin(config-Repository)# user john password plain john!23
admin(config-Repository)# exit
admin(config)# exit
```

List the Repository Data

You can list the data within a repository. Log in to the Cisco Prime Collaboration server as *admin* and run the following command:

```
admin# show repository RepositoryName
```

For example:

```
admin# show repository myftp
assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg
```

Schedule Backup using Cisco Prime Collaboration Assurance and Analytics User Interface

For Cisco Prime Collaboration Release 11.1 and earlier

You can schedule and run backup for both Assurance and Analytics from the user interface.

For Cisco Prime Collaboration Release 11.5 and later

You must be logged in as an administrator to perform backup.

To create a new backup job:

Step 1 Choose **System Administration > Backup settings**.

Step 2 On the Backup page, click **New**.

Step 3 Enter a name for the backup job.

If backup name is not specified, the **Backup Title** field is defaulted with date stamp.

Step 4 Select the **Backup Category** from the drop-down list.

Step 5 In the **Assurance Connection Settings** pane, enter the following details.

You can use sFTP, FTP, or local connection to create backup.

If you select sFTP or FTP, provide the following details:

- IP address of the server where the backup files need to be saved
- Path to the backup location

Note The backup is taken in the specified user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, /backup Then, the Assurance backup location will be /user1/backup/assurance_backup.
The backup is saved in /user1/backup/assurance_backup.	

- Port (for sFTP only)
- Username
- Password

Click **Test** to test the sFTP or FTP connection using the credentials.

If you select local, specify the location to save the backup files on your local machine.

For a local backup, you can specify the number of backup files to be saved, using the **Backup History** drop-down list. By default, the last two backup files are saved. You can save up to nine backup files.

The Analytics Connection Settings pane is available only if you have enabled Cisco Prime Collaboration Analytics.

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Analytics is supported on the MSP deployments.

Step 6 In the **Analytics Connection Settings** pane, enter the following details.

You can use only a remote server to backup the Analytics data using SSH.

- IP address of the remote server where the backup files need to be saved
- Path to the backup location. You must provide relative path.

Note The backup is taken in the specified user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, /backup Then, the Analytics backup location will be /backup/pg_basebackup (followed by timestamp (for example, pg_basebackup_201707201255)).
The backup is saved in /user1/backup.	

The Analytics backup folder will be in the following format: pg_basebackup (followed by the timestamp (for example, pg_basebackup_201707201255)). The backup fails if the user does not exist on the sFTP server.

- SSH Port
- SSH Username
- SSH Password

Click **Test** to test the connection using the credentials.

Step 7 Specify the backup start time and recurrence interval.

The time displayed in the date picker is the client browser time.

Step 8 (Optional) Enter the email IDs to which the backup status notification needs to be sent. Separate the email IDs using comma.

Configure the SMTP server details in the Cisco Prime Collaboration Assurance server (**E-mail Setup for Alarms & Events**) to receive emails.

For Cisco Prime Collaboration Release 11.5 and later

Configure the SMTP server details in the Cisco Prime Collaboration Assurance server (**Alarm & Report Administration > E-mail Setup for Alarms & Events**) to receive emails.

Step 9 Click **Save**.

The scheduled backup job is listed on the **Backup Management** page.

You can click **Run Now** to run the backup immediately.

Troubleshooting

Issue: Cisco Prime Collaboration Assurance backup job status shows failure even after generating the reports. The backup files are generated and stored in a sFTP location when a backup job is scheduled in the Cisco Prime Collaboration Assurance. A non-zero size file is created at the location. The job scheduled in the Cisco Prime Collaboration Assurance is in the failed state every time it is executed.

Expectation: The job must not fail or if it fails there must be reasons for failure.

The Cisco Prime Collaboration Assurance backup job status displays failure in spite of generating reports in sFTP. Hence, while backing up, modify the path of the sFTP server. Use a non-root user location for setting up the sFTP location for reports in the Cisco Prime Collaboration Assurance. The issue is due to the absence of the GPG key in the user folder.

The sFTP location for backup can be any other directory other than the root directory since GPG encryption is not enabled for the root directory.

If you choose the location under the root directory, then you must enable GPG encryption in the root directory.

Backup Cisco Prime Collaboration Assurance Data using CLI

CLI is supported only through SSH; telnet is not supported. The port used for Cisco Prime Collaboration server is 26. After creating the repository, log in to the Cisco Prime Collaboration server as *admin* and run the following command to back up the data:

```
admin# backup Backupfilename repository RepositoryName application cpcm
```

Where,

- *Backupfilename*—Name of the backup file (without the extension-.tar.gpg). This name can be a maximum of 100 alphanumeric characters.
- *RepositoryName*—Location to which the files are be backed up. This name can contain a maximum of 30 alphanumeric characters.

The following message is displayed after the backup is complete:

```
% Creating backup with timestamped filename: Backupfilename-Timestamp.tar.gpg
```

The backup file is suffixed with the time stamp (*YYMMDD-HHMM*) and file extension .tar.gpg and saved in the repository.

For example, in case of backup on the ftp server:

```
admin# backup assurance repository myftp application cpcm
```

where, myftp is a repository name.

Check the Backup History

You can check the backup history. Log in to the Cisco Prime Collaboration Assurance server.

Path: System Administration > Backup Settings

All the backups scheduled or configured are listed on the Backup Settings page. You can check the history from the **Run History** column. Click the hyperlink on each log listed in the column for more information.

Restore Data on the Same System

The following sections describe the process of restoring the data on the same system.

To restore the data, log in to the Cisco Prime Collaboration application server as *admin* through VM console using vSphere client. we recommend you to not to trigger the restore from SSH/Putty prompt.

Run the following command to restore the Cisco Prime Collaboration data:

```
admin# restore Backupfilename repository RepositoryName application cpcm
```

Where, *Backupfilename* is the name of the backup file suffixed with the timestamp (*YYMMDD-HHMM*) and file extension *.tar.gpg*.

For example, to restore on the ftp server:

```
admin# restore assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg repository myftp application  
cpcm
```

Restore on a New System

Cisco Prime Collaboration allows you to back up the data of a system and restore the data in another system in the event of total system failure.

To restore the backup from another system:

Ensure that the system to which data is restored must have the same MAC address as that of the system that was backed up (IP address and the hostname can be different).

In the case you are unable to assign the MAC address of the original system (that was backed up) to another system, contact Cisco TAC for information on a new license file (for a new MAC address).

To restore the backup from another system, log in as administrator through the VM console using vSphere Client and perform restore as described in Restore Data. See also, Create a Repository.

**Note**

As a post requirement, you must rediscover all the devices after restoring the data.



Set Log Levels

This section explains the following:

- [Set Log Levels, on page 583](#)

Set Log Levels

This chapter provides information on the various log levels supported in the Cisco Prime Collaboration Assurance.

Log Levels

Cisco Prime Collaboration Assurance supports the following log levels:

- Debug - Helps you to debug the application.
- Information - Indicates the progress of the application.
- Warning - Indicates potentially harmful situations.
- Error - Indicates that the application can still continue to run.
- Fatal - Indicates critical error. This level is not listed for all modules.

You cannot disable logging. However, you can:

- Collect more data when needed by increasing the logging level (highest-level is Debug).
- Return to the default logging level (Error).

The log level settings can be changed from the Log Management page (**System Administration > Log Management**). The log files are also included in the backup file.



Caution

You should not change the log level settings without assistance from the Cisco Technical Assistance Center (TAC) team.

Download Logs

This feature provides information to resolve the network issues quickly by enabling you to download log files so that you can share the required logs.

Prerequisites - You must set the log level to **Debug** for the module you want to collect logs for. For more information on how to set the log level to debug, see the earlier section.

Click the **Download Log** button to download the logs. You are prompted to download a .tar file. The file name shows the username of the user who generated the log file, date and time-stamp (according to the Cisco Prime Collaboration Assurance server time) to indicate when the (.tar) file was generated. You need to open or untar this file to view the log file with the same name. The log file is a compressed file, which can be opened using any uncompression utility such as 7-Zip.



PART **X**

Unified Communication Operations Dashboard

- [Getting Started with Unified Communication Operations Dashboard, on page 587](#)
- [Threshold Settings, on page 591](#)
- [System Settings, on page 593](#)
- [Responder Settings, on page 597](#)



CHAPTER 35

Getting Started with Unified Communication Operations Dashboard

This chapter explains the following:

- [Unified Communication Operations Dashboard, on page 587](#)

Unified Communication Operations Dashboard

This section provides information on the following:

Introduction to Unified Communication Operations Dashboard

Unified Communication Operations Dashboard (UCOD) collects all the unified cluster information from more than one PCA node. It supports a maximum of 10 responders. UCOD collects cluster information like critical alerts etc., from different PCA servers, registered to one particular master. So, each PCA is a **Responder** which is communicating with one node called the **Master**.

Install master in a PCA node, and you may or may not install the responder in the same PCA node. The master shows cluster information from one or more responder(s) registered to the corresponding master.

Install Responder in PCA

Install Responder in PCA to see the **UC Operations Dashboard** menu. You can install **Master** and **Responder** (optional) in the same PCA server or install only **Responders** on the other PCA nodes.

Click on **UC Operations Dashboard** tab to find the following submenus.

- UCOD Landing page - The Landing page appears only after you register the master successfully. An appropriate error message notifies the user if the master is not registered.
 - Responder Settings page - Register the Master with the Responder.
-

What to do next

[Launch UC Operations Dashboard, on page 588](#)

Launch UC Operations Dashboard

Register the Master IP Address to navigate to the UCOD Landing page sub menu from the UC Operations Dashboard tab.



Note

If you do not register the Master IP Address, an error message notifies 'UC Operations Dashboard Master IP Address is not registered properly. Please register the Master with the Responder in the Responder Settings Page'.

Register the Master IP Address

Log in to **PCA**.

Go to **UC Operations Dashboard** → click Responder Settings.

Enter the Master IP address in **UCOD Master Node** field.

Check **Enable** and click **Apply**.

Once you register, access the Responder Settings page to register the Master with the Responder.

Procedure

- Click on **UC Operations Dashboard** (first submenu) tab, which leads you to **UCOD Login** page.
- Enter the User Name as **globaladmin** (lowercase letters) and enter the same Password as your PCA's password, which leads you to the UCOD Landing Page.
- No other user name except **globaladmin** is allowed. An error message notifies 'Invalid Username or Password. Please try again'.

What to do next

Unified Communication Operations Dashboard Landing page

Unified Communication Operations Landing page

This page consists of Unified Communication Manager Cluster Information, which displays following fields.

Field	Description
UCM Cluster	Name of the Cisco Unified CM Cluster (VCS Clusters are not supported).
Critical Alerts	Shows the Critical Alert count for the specified cluster
CPU Usage (Avg, Peak)	Shows the CPU Usage information based on the average and peak CPU Usage respectively of all the nodes that are part of the specified cluster.
Virtual Memory (Avg, Peak)	Shows the Virtual Memory information based on the average and peak Virtual Machine usage respectively of all the nodes that are part of the specified cluster based on the severity.

Field	Description
Disk Usage (Avg, Peak)	Shows the Disk Usage information of all the nodes that are part of the specified cluster based on the average and peak Disk Usage, respectively.
Calls (Attempted + Completed)	Shows the consolidated number of Attempted and Completed Calls for the specified cluster.
Unregistered Endpoints (% , Actual)	Shows the consolidated number of unregistered hard and soft endpoints for the specified cluster in percentage and the actual number of unregistered endpoints in this cluster . The symbols against the values represent the severity.
Unregistered Gateways (% , Actual)	Shows the number of Unregistered MGCP gateways for the specified cluster in percentage and actual number of unregistered endpoints in this cluster. The symbols against the values represent the severity.
Unregistered Media Resources (% , Actual)	Shows the number of Unregistered Media Resources for the specified cluster in percentage and actual number of unregistered endpoints in this cluster. The symbols against the values represent the severity.

**Note**

CPU Usage (Avg, Peak), Virtual Memory (Avg, Peak) and Disk Usage (Avg, Peak) have symbols against the values, and these values are sorted based on severity.

All the above fields have a few symbols against the values, and they represent the **severity**.

Hover over these symbols to read the respective Threshold Criteria as well.

These hover message change accordingly based on any changes done to the [Threshold Settings](#)

The symbols and hover messages are explained below-

Symbols

1. Red cross-Critical
2. Yellow triangle - Warning
3. Green circle check - Information

Hover Messages

1. Threshold between 0 and 50% (inclusive)
2. Threshold between 50 and 70% (inclusive)
3. Threshold above 70%

How to access the submenus below settings on the UCOD Landing page

Click **Settings** icon on the top right corner of the **UCOD Landing** page to see the submenus below.

1. [Threshold Settings](#)
2. [System Settings](#)



CHAPTER 36

Threshold Settings

This chapter explains the following:

- [Introduction to Threshold Settings, on page 591](#)

Introduction to Threshold Settings

The Threshold Settings page shows the criteria of threshold parameters like **CPU Usage**, **Virtual Memory**, **Disk Usage**, **Unregistered Endpoints**, **Unregistered Gateways**, and **Unregistered Media Resources** in percentile.

Threshold settings in the table shows default values. You can choose to override these default values and define critical parameters. The data you set here reflects on the dashboard.

Threshold Settings

You can set the severity levels for the threshold parameters

Step 1 Click **Reset to Default** below the table to restore the default threshold parameter values.

Step 2 Click **Save** to save the Settings.

After saving successfully, navigate to the landing page to find the columns showing criticality updated, based on these threshold values saved.

Note **Save** button appears disabled if you provide any invalid data and the relevant error message appears against each field. Error message is different for each column.

Threshold Parameters

The threshold parameters have three severity levels -

1. Critical
2. Warning
3. Information

You can view the rules below. When you enter an invalid data, the severity appears in the field.

Severity	Description
Critical	Critical Min threshold should be greater than or equal to Warning Max threshold.
Information	Information Max threshold should be less than Warning Min threshold.
Warning-Max Threshold	Warning Max threshold should be less than Critical Max threshold and greater than Warning Min threshold.
Warning-Min Threshold	Warning Min threshold should be greater than or equal to Information Min threshold and less than Warning Max threshold.

The table lists the default Threshold Criteria.

Criteria	Range
Critical	Greater than or equal to 70% and less than 100%
Warning	Greater than or equal to 50% and less than 70%
Information	Greater than or equal to 0% and less than 50%



Note

You must specify continuous custom ranges which do not overlap with one another. For example, Critical range - 80 to 100 and Warning range - 60 to 70 is not valid.

1. Click on **Settings** on the top-most right corner of the **UCOD Landing** page.
2. Click on **System Settings** from the drop-down list. The **System Settings** page appears.



CHAPTER 37

System Settings

This chapter explains the following:

- [System Settings, on page 593](#)

System Settings

In **System Settings** page configure the Master application. In this page, you can add the responders (PCA nodes) that you wish to monitor.

- Click Yes to Enable Master Node.
- Click No to Disable Master Node. A message notifies ‘Do you want to disable the UC Operations Dashboard Master Node?’
- Click YES to confirm deleting the Master Node.



Note

The default Enable Master State is ‘Yes’. On disabling master, no communication takes place between the master and the associated responders.

Add or Delete Associated Responders

The table provides a list of associated responders.

Field	Description
Host Name	Hostname of the Responder Node.
IP Address	IP Address of the Responder Node.
Number of Managed Clusters	Number of clusters managed in the associated Responder Node.
Responder Status	Shows the status of the Responder registration with the Master.
Registered At	The date and time at which the Responder is Registered/Unregistered with the Master.

Field	Description
Status Reason	<p>Shows the status reasons of the respective Responder registration with the Master. The following are the different reasons shown.</p> <ol style="list-style-type: none"> 1. Registration Rejected Reason - Master IP is not authorized at the Responder 2. Registered Successfully 3. Responder is in Suspended mode 4. Unable to Contact the Responder 5. Responder initiated deregistration 6. Data not received over the past two cycles

To Add or Delete an Associated Responder

1. Click **Add** to add an associated responder.

Enter either comma separated Master IP Address(es) or Host Names you want to add in the **Responder IP** field that pops up.

2. Check the box against the responder(s) you want to delete.

A message notifies 'Do you want to delete the selected Responder(s)'.

Click **Yes** to delete the selected Responder(s).

Click **No** to retain the added Responder(s).



Note

Deleting the responder in **System Settings** page deletes the corresponding cluster data as well.

Set the Job Frequency

Set the job frequency of the cluster summary using the drop-down box of 'Cluster Summary Job Frequency' as 1, 3, 5 or 10 minutes as per your preference.



Note

The default time interval is **5** minutes.

Click **Apply**.



Note

1. The job frequency is applicable for all Responders. For every chosen respective time intervals, the responder will send the aggregated cluster summary information to the Master.
2. For mega cluster, the bigger the interval (>5 minutes) better is the accuracy. Smaller frequency should be applicable for small clusters (number of nodes - 3 to 5) and less number of PCAs (<= 5).

Set the Shared Secret Key

Procedure

- Enter the same Shared Secret Key that was set earlier in the Responder settings page while setting up for the Master.
- You must provide the same key for both Master and associated Responder(s).
- Click 'Apply' once every field in System Settings page.



CHAPTER 38

Responder Settings

This chapter explains the following:

- [Introduction to Responder Settings, on page 597](#)

Introduction to Responder Settings

This page contains complete information on **Responder Settings**.

Once you install the responder, it is in the default **Suspend** state. So, the Responder will not collect/send any data. In this state, the Master IP Address and Shared Secret Key are in the default **Disable** state.

Enable Responder

- Step 1** Click **Enable** to select Responder State manually, in the **Responder Settings** page.
- Step 2** Enter either the Host Name or Master IP Address in **UCOD Master Node** field.
-

Set the Shared Secret Key

Once you enable the Responder state and enter the UCOD Master Node, set the **Shared Secret Key**. This is optional, but highly recommended to secure the data. It secures the communication between the Master and the Responder.



Note You must provide the same key for both Master and associated Responder(s).

Set the Shared Secret Key based on the key policy provided below.

Key policy:

1. Alphanumeric (case sensitive)
2. Must be between 8 and 24 characters in length
3. No special characters allowed

Registration Status

Step 1 Click **Apply** to successfully register the Responder Settings.

Once you set the shared secret key, the Registration Status changes accordingly.

Step 2 Check for the respective reasons below.

a. Registered: Registration successful with the Master.

b. Pending: When Responder is suspended or Master is not available for Registration (Default state).

c. Unregistered: Responder IP is not available in the Master authorized list.

d. Suspended: Responder is in suspended state. However, the Master has this Responder IP in its authorized list.

Based on successful validation of the Master IP Address/Shared Secret Key, the responder is successfully registered to the Master.

Note If you do not provide the correct Master IP Address(es)/Host Names, **Apply** button in the **Responder Settings** page is disabled.



APPENDIX

References

This section provides information on Synthetic Test Worksheet, Cisco 1040 Sensor Management, and the user interface.

- [Synthetic Test Worksheet, on page 601](#)
- [Cisco 1040 Sensor Management, on page 605](#)
- [Troubleshooting Secure JTAPI Connection, on page 615](#)
- [TLS Configuration for Jetty and Tomcat Server, on page 617](#)
- [User Interface, on page 621](#)



APPENDIX A

Synthetic Test Worksheet

This section explains the following:

- [Synthetic Test Worksheet, on page 601](#)

Synthetic Test Worksheet

The number of phones you must create in a Cisco Unified Communications Manager for use in synthetic tests depends on:

- The number of synthetic tests you want to configure.
- The type of tests you want to run.

The following table provides a worksheet for determining how many phones you need. Fill in the number of tests and calculate the total phones needed using the information provided in the table:

Table 105: Number of Phones Required for Synthetic Tests

Number of Tests	Type of Test	Phones Needed for Test	Total Phones Needed
	Phone Registration	1 (synthetic phone)	
	Dial-Tone	1 (synthetic phone)	
	End-to-End Call with real phones	2 (1 synthetic phone and 1 real phone)	
	End-to-End Call with synthetic phones	2 (synthetic phones)	
	TFTP Download	0	
	For Cisco Prime Collaboration Release 11.6 and later HTTP Download	0	

Number of Tests	Type of Test	Phones Needed for Test	Total Phones Needed
	Emergency Call (without On Site Alert Number)	2 (synthetic phones)	
	Emergency Call (with On Site Alert Number)	3 (synthetic phones)	
	Message-Waiting Indicator	2 (synthetic phones)	

As you configure phones on each Unified CM, use the following worksheets to simplify data entry into Cisco Prime Collaboration Assurance.

The dashes in the table indicate that data is not required for the MAC Address, Destination Phone Extension Number, or Destination Phone Cisco Unified Communications Manager.

Table 106: Cisco Unified Communications Manager

Synthetic Test	MAC Address	Destination Phone Extension Number	Destination Phone Cisco Unified Communications Manager
Phone Registration		-	-
Dial-Tone		-	-
End-to-End Call-source phone		-	-
End-to-End Call-destination phone (synthetic phone)			
End-to-End Call-destination phone (real phone)	-		-
Phone Registration		-	-
Dial-Tone		-	-
End-to-End Call-source phone		-	-
End-to-End Call-destination phone (synthetic phone)			
End-to-End Call-destination phone (real phone)	-		-
Phone Registration		-	-
Dial-Tone		-	-
End-to-End Call-source phone		-	-
End-to-End Call-destination phone (synthetic phone)			
End-to-End Call-destination phone (real phone)	-		-

Table 107: Cisco Emergency Responder

Parameter	Name or Number
Source	
Cisco Unified Communications Manager	
MAC address	
Destination	
Emergency number	
Public Safety Answering Point	
Cisco Unified Communications Manager	
MAC address	
On Site Alert	
Cisco Unified Communications Manager	
MAC address	

Table 108: Cisco Unity

Parameter	Name or Number
Caller	
Cisco Unified Communications Manager	
MAC address	
Recipient	
Cisco Unified Communications Manager	
MAC address	
Phone extension number	
Voice mail	
Password	



APPENDIX **B**

Cisco 1040 Sensor Management

This section explains the following:

- [Cisco 1040 Sensor Management, on page 605](#)

Cisco 1040 Sensor Management

Cisco Prime Collaboration Assurance uses the data that it receives from Cisco 1040 Sensors to determine the voice transmission quality in your network.

For the Cisco 1040 Sensor to operate as desired, the switch connected to Cisco 1040 must be managed and configured in Cisco Prime Collaboration Assurance. For more details, see the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#):



Note The Cisco 1040 Sensor management is not applicable if you have installed Cisco Prime Collaboration Assurance in MSP mode.

This section contains the following:

Overview of Cisco Prime NAM/vNAM

Cisco 1040 Sensor is now end of sale. For more information, see [End-of-Sale and End-of-Life Announcement for the Cisco 1040 Sensor](#) page.

The Cisco Prime NAM/vNAM replaces the Cisco 1040 Sensor and fills the missing capabilities gap. You can use Cisco Prime Network Analysis Module (NAM) and Cisco Prime Collaboration Assurance together to monitor and troubleshoot voice and other network-related issues. For more information, see the [Using Cisco Prime Virtual Network Analysis Module and Cisco Prime Collaboration to Monitor and Troubleshoot Voice and Video](#) white paper.

To know about what information you can get from the NAM reports, see [NAM & Sensor Report, on page 408](#).

Perform Initial Configuration in Cisco Prime Collaboration Assurance

For initial configuration of Cisco 1040 Sensors, do the following:

-
- Step 1** Add one or more TFTP servers for Cisco Prime Collaboration Assurance and Cisco 1040 Sensors to use. See [Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files](#).
- Step 2** Create a default configuration file. See [Set Up the Cisco 1040 Sensor Default Configuration](#).
- When a Cisco 1040 connects to the network, it downloads a configuration file from a TFTP server before registering to Cisco Prime Collaboration Assurance.
-

Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files

Cisco Prime Collaboration Assurance uses one or more TFTP servers to provide configuration files and binary image files for Cisco 1040s. You must define at least one TFTP server for Cisco Prime Collaboration Assurance to use. You can configure additional TFTP servers if you either want a backup server or have more than one DHCP scope.

You can use the configuration files that Cisco Prime Collaboration Assurance keeps on the server to recover if there is a write failure on the TFTP server. In this case, you can manually copy configuration files from Cisco Prime Collaboration Assurance to each TFTP server that is configured for Cisco Prime Collaboration Assurance.

Add and Delete a TFTP Server

To enable Cisco 1040s to register with Cisco Prime Collaboration Assurance, you must define at least one TFTP server where Cisco Prime Collaboration Assurance can provide Cisco 1040 configuration files (and the binary image file).



Note

- Using Cisco Prime Collaboration Assurance as a TFTP server is not supported. Additionally, we recommend disabling the CWCS TFTP service on the Cisco Prime Collaboration Assurance server.
 - If you plan to use Unified CM as a TFTP server, consider that:
 - You must manually copy configuration and image files from Cisco Prime Collaboration Assurance to the root location on the Unified CM TFTP server.
 - After you update files and copy them to the TFTP server, you might also need to restart the Cisco TFTP service (on Unified CM) for Cisco 1040s to be able to download the files.
-

-
- Step 1** Choose **Alarm & Report Administration > 1040 Sensor Setup > TFTP Servers**. The TFTP Server Setup page is displayed.
- Step 2** Click **Add**. The TFTP Server Settings dialog box is displayed.
- Step 3** Enter data in the following fields:
- TFTP Server — IP address or DNS name.
 - Port Number — The customary port number is 69.

Step 4 Click **OK**.

Note To delete, select the TFTP server and click Delete.

Set Up the Cisco 1040 Sensor Default Configuration

Use this procedure to:

- Enable or disable call metrics archiving — Cisco Prime Collaboration Assurance saves MOS data in the database. Optionally, you can also save the data to files.
- View the directory path for the archive data file and the Cisco 1040 image file.
- Create the default configuration file — QOVDefault.CNF specifies the primary Cisco Prime Collaboration Assurance to which a Cisco 1040 can register.



Note If you are using Unified CM software version 4.2 or later as a TFTP server, you must manually copy the default configuration file from the image file directory on the Cisco Prime Collaboration Assurance server to the root location on the Unified CM TFTP server. For more information, see step 3, in the following procedure.

To set up the Cisco 1040 sensor:

Step 1 Select **Alarm & Report Administration > 1040 Sensor Setup**

The Setup page is displayed.

Step 2 Update data described in the following table.

Step 3 Click **OK**. Cisco Prime Collaboration Assurance stores the configuration file locally and copies it to the TFTP servers that are added to Cisco Prime Collaboration Assurance.

Cisco 1040 Sensor/NAM Setup Page—Graphical User Interface Elements

Table 109: Cisco 1040 Sensor/NAM Setup Page—Graphical User Interface Elements

Graphical User Interface Element	Description
Call Metrics Archiving	Select one of the following: <ul style="list-style-type: none">• Enable — After analysis, Cisco Prime Collaboration Assurance saves data from sensors to disk files.• Disable — After analysis, Cisco Prime Collaboration Assurance discards data. Default: Disable.

Graphical User Interface Element	Description
Data File Directory	Directory where files are stored if call metrics archiving is enabled. You cannot edit this field.
Image File Directory	Directory where Cisco 1040 binary image file and configuration files are stored locally. You cannot edit this field.
Send traps every n minutes per endpoint	Enter a number greater than or equal to 5. Cisco 1040s send data to Cisco Prime Collaboration Assurance every 60 seconds. Cisco Prime Collaboration Assurance determines whether a violation has occurred and can potentially send a trap-a-minute for each endpoint. Use this setting to reduce the number of traps that Cisco Prime Collaboration Assurance sends for each endpoint. For a given endpoint, a trap is sent every n minutes and additional traps during that time are suppressed (not sent).
Default Configuration to TFTP Server	
Image Filename	Enter the image file name if you are using a new image (for example, after a product upgrade).
Primary Prime Collaboration	IP address or DNS name for the primary Cisco Prime Collaboration Assurance.

Configure Cisco 1040 Sensors in Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance analyzes data that it receives from Cisco 1040 Sensors installed in your voice network. Cisco Prime Collaboration Assurance manages multiple Cisco 1040 Sensors.

This section contains the following:

Cisco 1040 Sensor Details

To see Cisco 1040 Sensor details, choose **Alarm & Report Administration > 1040 Sensor Setup > Management**. The Cisco 1040 Sensor Details page displays information listed in the following table:

Graphical User Interface Element	Description
	Exports data from the Cisco 1040 Sensor/NAM Details page to a CSV or PDF file.
	Opens a printer-friendly version of the data in another window; for printing from a browser window.
Check box column	Select Cisco 1040s that you want to edit, reset, or delete.
Name column	Click the name link to view details of the Cisco 1040 configuration.

Graphical User Interface Element	Description
Cisco 1040 Address columns	Displays MAC and IP addresses for Cisco 1040. Click the MAC address link to launch an HTML page on the Cisco 1040.
Prime Collaboration columns	Displays the following: <ul style="list-style-type: none"> • Primary — IP address or hostname of the primary Cisco Prime Collaboration Assurance defined for the Cisco 1040. • Registered with — Displays one of the following: <ul style="list-style-type: none"> • IP address or hostname of the Cisco Prime Collaboration Assurance to which the Cisco 1040 is currently sending data. • Waiting — The Cisco 1040 is not yet registered. • Older Image—The binary image on the Cisco 1040 is not supported.
Reset Time column	The last date and time that Cisco Prime Collaboration Assurance sent a reset command to the Cisco 1040.
Buttons	
Add	See Add a Cisco 1040 Sensor .
Edit	See Edit Configurations for Multiple Cisco 1040s .
Delete	See Delete a Cisco 1040 Sensor .
Reset	See Reset Cisco 1040s .
Refresh	Refresh the Cisco 1040 Sensor Details page.

Restart Processes to Update Cisco 1040 Registration Information in Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance might show a Cisco 1040 Sensors waiting to register while receiving and processing syslogs from it; this problem can occur after a user does one of the following:

- Uses **pdterm** to stop the QOVR process, and, in quick succession, uses **pdexec** to start it again. To prevent this problem, wait at least 5 minutes between stopping and starting the QOVR process. To correct this problem:

From the command line, stop the QOVR process again, by entering this command:

```
pdterm QOVR
```

Wait at least 5 minutes.

Enter this command:

```
pdexec QOVR
```

- Changes the time on the system where Cisco Prime Collaboration Assurance is installed without subsequently stopping and restarting the daemon manager. To correct this problem, login as admin and execute the following commands:

```
<hostname>/admin#application stop cpcm
<hostname>/admin#application start cpcm
```

Add a Cisco 1040 Sensor

To add a Cisco 1040 Sensor to Cisco Prime Collaboration Assurance, perform the following procedure.

-
- Step 1** Select **Alarm & Report Administration > 1040 Sensor Setup > Management**.
The Cisco 1040 Sensor/NAM Details page is displayed.
- Step 2** Click **Add**.
The Add a Cisco 1040 Sensor dialog box is displayed.
- Step 3** Enter data listed in the following table:
- Step 4** Click **OK**. The configuration file is saved on the server where Cisco Prime Collaboration Assurance is installed and is copied to all TFTP servers. (See [Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files](#).) The configuration file is named QOV<MAC address>.CNF, where <MAC address> is the MAC address for the Cisco 1040. Similarly, for updating the configuration, select one or more check boxes and click **Edit**.
-



Note

- Select a Cisco 1040 Sensor to edit the name or description.
 - Do not edit a Cisco 1040 configuration file using a text editor.
-

Cisco 1040 Sensor/NAM Dialog Box—Graphical User Interface Elements Description

Graphical User Interface Element	Description
Sensor Name	<p>Enter up to 20 characters. This name is used to identify the sensor on Cisco Prime Collaboration Assurance windows, such as reports.</p> <p>Note Cisco 1040 names must be unique. Cisco 1040s that register to Cisco Prime Collaboration Assurance using the default configuration file use the name Cisco 1040 + <last 6 digits from MAC address>.</p>
Image File Name	<p>Enter the binary image file name. The filename format is SvcMonAB2_<nnn>.img where <nnn> is a revision number.</p>

Graphical User Interface Element	Description
MAC Address	Enter the MAC address for the Cisco 1040 that you are adding.
Primary Prime Collaboration	Enter an IP address or DNS name of a host where Cisco Prime Collaboration Assurance is installed.
Description	(Optional) Enter up to 80 characters.

Edit Configurations for Multiple Cisco 1040s

- If you use Unified CM as a TFTP server, you must manually upload the updated configuration file from the image file directory on the Cisco Prime Collaboration Assurance server to the root location on Unified CM TFTP server. Afterward, you must reset the Cisco 1040. (The image file directory is *NMSROOT/ImageDir*. *NMSROOT* is the directory where Cisco Prime Collaboration Assurance is installed; its default location is C:\Program Files\CSCOpX.) If the Cisco 1040 does not register or does not load the latest files, restart the TFTP Server.
- Do not edit a Cisco 1040 configuration file using a text editor. Edit a Cisco 1040 configuration file using this procedure only.

To edit configurations for multiple Cisco 1040s:

-
- Step 1** Select **Alarm & Report Administration > 1040 Sensor Setup > Management**.
- Step 2** Select check boxes for more than one Cisco 1040 and click **Edit**.
- Step 3** Update any of the fields.
- Step 4** Click **OK**.
- Cisco Prime Collaboration Assurance saves the configuration files on the local server copies it to all TFTP servers. Then Cisco Prime Collaboration Assurance resets the Cisco 1040s, so that they load the updated configuration.
-

Cisco 1040 Management - Field Descriptions

Table 110: Cisco 1040 Management - Field Descriptions

Fields	
Image File Name	Enter the binary image filename. The filename format is SvcMonAB2_ <i>nnn</i> .img where <i>nnn</i> is a revision number. For the name of the most recently supported binary image file, see Cisco Prime Unified Service Monitor 2.3 Compatibility Matrix .
Primary Prime Collaboration	Enter an IP address or DNS name of a host where Cisco Prime Collaboration Assurance is installed. The Cisco 1040 sends data to this Cisco Prime Collaboration Assurance unless it becomes unreachable.

Fields	
Secondary Prime Collaboration	(Optional) Enter an IP address or DNS name of a host where Cisco Prime Collaboration Assurance is installed. The Cisco 1040 sends data to this Cisco Prime Collaboration Assurance only if the primary Cisco Prime Collaboration Assurance becomes unreachable.

Reset Cisco 1040s

Use this procedure to boot one or more Cisco 1040s. After a Cisco 1040 boots, it first uses DHCP to obtain the IP address of the TFTP server. Cisco 1040 obtains a configuration file from the TFTP server. If the configuration file specifies a binary image file that is different from the currently installed image, the Cisco 1040 obtains the binary image file from the TFTP server.

-
- Step 1** Select **Alarm & Report Administration > 1040 Sensor Setup > Management**.
- Step 2** Select check boxes for the Cisco 1040s that you want to reset.
- Step 3** Click **Reset**. The Cisco 1040 will take a few minutes to complete the startup sequence, reconfigure (if necessary), and register with Cisco Prime Collaboration Assurance.

Note If you use Unified CM as a TFTP server, the Cisco 1040 Sensor does not register or does not load the most recent image file after reset. You must restart the TFTP Service on Cisco Prime Unified Communications Manager.

When you reset a Cisco 1040, Cisco Prime Collaboration Assurance sends the most recent time to the sensor. The Cisco 1040 resets its clock as needed.

Delete a Cisco 1040 Sensor

Before you delete a Cisco 1040 Sensor from Cisco Prime Collaboration Assurance, you must shut the switch port that physically connects to the 10/100-1 Fast Ethernet port on the Cisco 1040:

-
- Step 1** To identify the port, get the switch IP address and the switch port from the Cisco 1040 web interface.
- Step 2** To shut the port, use the CLI on the switch.

Note Do not delete the Cisco 1040 from Cisco Prime Collaboration Assurance until you shut the switch port.

You should also either shut or reconfigure the SPAN or RSPAN destination port on the switch. For information about configuring SPAN and RSPAN on Cisco Catalyst switches and modules, see http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml.

After you delete a Cisco 1040, it cannot automatically register again to the Cisco Prime Collaboration Assurance from which it has been deleted. To enable such a Cisco 1040 to register with this Cisco Prime Collaboration Assurance again, you must add the Cisco 1040 Sensor manually. See [Add a Cisco 1040 Sensor](#).

To delete, select **Alarm & Report Administration > 1040 Sensor Setup > Management**. Select check boxes for the Cisco 1040s that you want to delete from the Cisco 1040 Sensor Details page and click Delete.

Note Delete a Cisco 1040 Sensor from any sensor threshold groups, before you delete the Cisco 1040 Sensor.

Cisco Prime Collaboration Assurance sends a time synchronization message to each Cisco 1040 Sensor hourly. Cisco Prime Collaboration Assurance also sends a time synchronization message when a Cisco 1040 registers. A Cisco 1040 registers when it is added to the network and when it has been reset. The Cisco 1040 receives the time from Cisco Prime Collaboration Assurance and resets its clock as needed.

View Diagnostic Information on a Cisco 1040

To view the diagnostics stored on a Cisco 1040, enter `http://<IP address>/Diagnostics` in your browser, where IP address is the address of your Cisco 1040.

The Cisco 1040 web interface displays a Diagnostics Information window with the following information:

Field	Description
Current Time	Current time and date (HH:MM:SS MM/DD/YYYY).
Clock Drift	Seconds of drift and the last time and date that the clock was reset; for example, "1 second(s) updated at 9:23:37 03/16/2009".
Last Analysis Time	Time and date when the Cisco 1040 last ran an analysis.
Streams Analyzed	Number of RTP streams that were analyzed during the last interval.
Last Communication	Time and date when the sensor last received an ACK or timeSet message, or any supported message from the Cisco Prime Collaboration Assurance.
Last Successful Report Time	Time and date that the Cisco 1040 last sent data to Cisco Prime Collaboration Assurance.
Report Destination	Destination hostname or IP address and port number to which the report was sent.
Report Length (bytes)	Number of bytes in the last report record.
Received Packets	Number of packets that the Cisco 1040 received during the last interval.
Receive Errors	Number of errors received on the monitoring interface as reported by pcap.
Packets Dropped	Number of packets dropped on the monitoring interface as reported by pcap.
Buffer overruns	Number of buffer overruns on the monitoring interface as reported by pcap.

Field	Description
Framing Errors	Number of framing errors on the monitoring interface as reported by pcap.
Interface Promiscuous	Monitoring interface is in promiscuous mode (yes) or not (no).



APPENDIX C

Troubleshooting Secure JTAPI Connection

This section lists the possible errors along with the recommended actions to troubleshoot secure JTAPI connection.

- [Troubleshooting Secure JTAPI Connection](#) , on page 615

Troubleshooting Secure JTAPI Connection

1. Possible errors with setup of CUCM for Secure JTAPI.
 - a. Ensure to move CUCM to Mixed mode for Secure JTAPI connection to work.
 - b. Application User on CUCM do not have “Standard CTI Secure Connection” role associated.



Note

For non-secure connection “Standard CTI Secure Connection” role should not be present.

- c. Application User CAPF profile do not have “Certificate Operation as Install/Upgrade”.
 - d. CTI service/ Call Manager service/ CAPF service/ TFTP service is down on CUCM.
 - e. When CUCM/CAPF certificates are regenerated, make sure the CTL file is regenerated and all the required services are restarted, new CAPF Profile is created before CUCM rediscovery on Cisco Prime Collaboration Assurance.
2. Possible errors while using Cisco Prime Collaboration Assurance with Secure JTAPI in Session Monitoring.

Issue:

Sessions not coming up on Conference Diagnostics

Possible Reasons:

 - a. Access level for JTAPI may not be RO (read-only).
 - b. Endpoints may not have full visibility.
 - c. Endpoints may not be controlled by the JTAPI User.



APPENDIX D

TLS Configuration for Jetty and Tomcat Server

This section details steps to perform the following:

- [Enable Minimum TLS Version for Cisco Prime Collaboration Assurance Client Connections, on page 617](#)
- [Enable TLS Protocol for Jetty Server, on page 618](#)
- [Enable TLS Protocol for Tomcat Server, on page 618](#)

Enable Minimum TLS Version for Cisco Prime Collaboration Assurance Client Connections

Follow are the steps for Minimum TLS configuration for Cisco Prime Collaboration Assurance Client interfaces.

Before you begin



Note All HTTPS connections from Cisco Prime Collaboration Assurance to VOS based devices are controlled by the below settings.

-
- Step 1** Login as *root* user to edit the following file:
`/opt/emms/conf/connector.xml`
- Step 2** Edit `<minTLSProtocol>TLSv1</minTLSProtocol>` for particular connection type (HTTPS).
TLSv1 configured, TLSv1, TLSv1.1, TLSv1.2 enabled
TLSv1.1 configured, TLSv1.1, TLSv1.2 enabled
TLSv1.2 configured, TLSv1.2 enabled
- Step 3** Restart all Cisco Prime Collaboration Assurance services.
-

Enable TLS Protocol for Jetty Server



- Note**
1. Jetty server is configured to enable all the 3 protocols, by default.
 2. For example, to disable TLS v1 protocol and have only TLS v1.1 and TLS v1.2 enabled. Follow these steps:

Step 1 Edit the following file:

```
/opt/jetty/etc/jetty-ssl.xml
```

Step 2 Add the below entries under **sslContextFactory** tag. For example,

```
<Set name="IncludeProtocols">
  <Array type="String">
    <Item>TLSv1.1</Item>
    <Item>TLSv1.2</Item>
  </Array>
</Set>
<Set name="ExcludeProtocols">
  <Array type="String">
    <Item>TLSv1</Item>
  </Array>
</Set>
```

Step 3 Restart the Jetty server using the following command:

```
systemctl restart jetty
```

Enable TLS Protocol for Tomcat Server



- Note**
1. Tomcat server is configured to enable all the 3 protocols, by default.
 2. For example, to disable TLS v1 protocol and have only TLS v1.1 and TLS v1.2 enabled. Follow these steps:

Step 1 Edit the following file:

```
/opt/emms/apache-tomcat-8.5.11/conf/server.xml
```

Step 2 Replace **sslProtocols** parameter in **port 8443** connector tag with **protocols** parameter and mention the required protocols to be enabled.

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
```

```
maxThreads="150" scheme="https" secure="true"  
clientAuth="false" sslProtocols="TLSv1,TLSv1.1,TLSv1.2"  
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  
maxThreads="150" scheme="https" secure="true"  
clientAuth="false" protocols="TLSv1.1,TLSv1.2"
```

Step 3 Restart all processes on Cisco Prime Collaboration Assurance when the above configuration is complete.



APPENDIX E


User Interface

This section explains the following:

- [Overview, on page 621](#)
- [Filters, on page 622](#)
- [Launch the Advanced Filter and Save Filter Criteria, on page 623](#)
- [Quick View, on page 624](#)
- [View About Details, on page 624](#)

Overview

Cisco Prime Collaboration Assurance has a new user interface to give you a simplified user experience. The left pane displays vertical expandable **Navigation** tab, **Index** tab, **Favorites** tab, and **Search Menu** fields. The **Favorites** tab allows you to bookmark your preferred pages for future reference. Click the Toggle

Navigation icon  on the **Cisco Prime Collaboration** Assurance page to view a list of dashlets and reports. You can click the pin icon at the top left to hide or display the left pane.

For the navigation changes in Cisco Prime Collaboration Assurance user interface, see the *Navigation Changes in Cisco Prime Collaboration Assurance - Advanced User Interface* section in the [Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide](#)

Getting Started Page is the home page of Cisco Prime Collaboration Assurance user interface in Enterprise mode. For more information on Getting Started page in MSP mode, see [Get Started with Cisco Prime Collaboration Assurance, on page 45](#).

For Cisco Prime Collaboration Release 11.6 and later



Note The session times out if there is no activity for 15 minutes.

The following is a list of pages that never time out in Cisco Prime Collaboration Assurance server:

- **System View**
- **Customer Summary Dashboard (in MSP mode)**
- **Diagnostics Test pages (UC Application Synthetic Test, Audio Phone Features Test, Video Test, and Batch Test)**
- **Endpoint Diagnostics**
- **Performance dashboards**
- **Session Diagnostics**
- **All Topology pages**

For Cisco Prime Collaboration Release 11.5 and later




Note The conference times out if there is no activity for 15 minutes.

The following is a list of pages that never time out in Cisco Prime Collaboration Assurance server:

- **Network Health Overview**
 - **Customer Summary Dashboard (in MSP mode)**
 - **Diagnostics Test pages (UC Application Synthetic Test, Audio Phone Features Test, Video Test, and Batch Test)**
 - **Endpoint Diagnostics**
 - **Performance dashboards**
 - **Conference Diagnostics**
 - **All Topology pages**
-

Filters

You can use the Filter feature to display specific information on the Cisco Prime Collaboration Assurance user interface. The Filter icon  is provided wherever the data is displayed in a tabular format.

The following are the types of filters available on the Cisco Prime Collaboration Assurance client:

- Quick Filter
- Advanced Filter

The quick filter and advanced filter are case-insensitive. For these filters, you can also use the following wildcard expressions:

- Question mark(?) — Match any one character.
- Asterisk (*) — Match zero or more characters.

Quick Filter

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. The operator used with this filter is *Contains*. To apply different operators, use the Advanced Filter option.

To launch the quick filter, choose **Quick Filter** from the **Filter** drop-down menu.

To clear the quick filter, click **Filter**.

Advanced Filter

This filter allows you to narrow down the data in a table by applying a filter using multiple operators, such as Does not contain, Does not equal, Ends with, Is empty, and so on.

You choose the filter pattern (table column names) and operator from the drop-down menu. In addition, you must enter filter criteria based on data available in the Cisco Prime Collaboration Assurance database.

To launch the advanced filter, choose **Advanced Filter** from the **Filter** drop-down menu.

To clear the advanced filter, click **Filter**.

Launch the Advanced Filter and Save Filter Criteria

To launch the advanced filter, choose **Advanced Filter** from the Filter drop-down menu.

You can save the filter criteria used in the Advanced filter.

To save the filter criteria:

-
- Step 1** From the Filter drop-down menu, choose **Advanced Filter**.
 - Step 2** Enter advanced filter criteria.
 - Step 3** Click **Go** and then click the **Save** icon.
 - Step 4** In the Save Preset Filter page, enter a name for the Preset Filter and click **Save**.


To clear the Advanced Filter, click the **Filter** button.

Cisco Prime Collaboration Assurance provides predefined keywords to filter data. In addition, the saved advanced filter criteria are also listed in the Preset Filter drop-down list. See Advanced Filter in [Filters](#) for details on how to save the filter criteria.

This feature is available on some pages; for example, Device Management, Alarm browsers, and Event browsers. To launch a preset filter, choose the available values from the Show drop-down list.

Cisco Prime Collaboration Assurance provides a set of predefined filters that enable you to filter the data in a table.

Quick View

The quick view icon  is displayed when you hover your mouse pointer on a table, specific table columns, or a topology pane. You can use quick view to cross-launch a page that you want to view in detail. In Cisco Prime Collaboration Assurance, this option is not available for administrative tasks, reports, or diagnostic views.

View About Details

This page displays the About details for Cisco Prime Collaboration Assurance.

To launch this page in Essential mode, click **globaladmin - Essential** > **About** at the top right corner of the User Interface.

- Click System Information link to view the following system information details in a quick view.
 - Build Version
 - License Type
 - Expiration Date (displayed in red for the last 15 days before expiry)
 - IP Address
 - MAC Address
 - VM Capacity
- Click Licensing link to open the License Management page.



INDEX

A

- adding [207, 481, 610](#)
 - alarm set [207](#)
 - Cisco 1040 [610](#)
 - synthetic tests [481](#)
 - Message-Waiting Indicator test [481](#)
- Adding and Copying [86](#)
- Adding Devices [126](#)
- alarms [42](#)
 - status [42](#)
- analytics [34, 50, 60, 432, 433](#)
 - licensing [60](#)
 - usage scenarios [50](#)
 - user interface [432, 433](#)
 - detailed analysis [433](#)
 - global filter options [433](#)
 - quick view [433](#)
- applications, configuring for synthetic tests [479](#)
- asset usage [442](#)
- Assurance Licensing [59](#)
- Assurance user roles and tasks [69](#)

B

- backup [580](#)
 - history [580](#)
- Backup and Restore [575](#)
- batch tests [515](#)
 - phone tests, type of [515](#)

C

- capacity analysis [448, 449, 450, 452, 453, 461](#)
 - route group utilization [452](#)
 - top n busy-hour trunks [450, 453](#)
 - top n cac bandwidth locations [449](#)
 - top n conferencing devices [461](#)
 - utilized trunks [449](#)
- Cisco 1040 Sensor [605](#)
- Cisco 1040 Sensors [605](#)
- cluster device discovery [133](#)
- cluster device discovery, running for device pool thresholds [217](#)
- conferences [459, 460](#)
 - top n conference locations [460](#)

- conferences (*continued*)
 - video conference statistics [459](#)
- configure LDAP server [71](#)
- configuring [607](#)
 - Cisco 1040 [607](#)
 - primary Service Monitor [607](#)
- configuring gateway code [393](#)
- contact center [316, 320, 329, 337, 345](#)
 - dashboards [316, 320, 329, 337, 345](#)
 - CUIC [337](#)
 - CVP [320](#)
 - MediaSense [345](#)
 - UCCE [329](#)
- creating node-to-node tests [496](#)
- creating phone status tests [474](#)
- custom [373](#)
 - dashboards [373](#)
- Customer Voice Portal [463](#)

D

- data population [438](#)
- delete a user [70](#)
- Device Inventory Management [10](#)
- devices [178](#)
 - discovery [178](#)
- Diagnostics [12](#)
- dial plan [386](#)
 - default [386](#)
 - NANP [386](#)
- discovery [133](#)
 - cluster devices [133](#)
- DNS configuration [608](#)
 - and Cisco 1040s [608](#)
- DSP Utilization [454](#)

E

- e-mail [198](#)
 - notifications [198](#)
- edit user details [70](#)
- Emergency Call synthetic test [479](#)
 - adding [479](#)
- enabling [607](#)
 - call metrics archiving [607](#)

End-to-End Call synthetic test [482](#)
 adding [482](#)
 endpoint utilization report [418](#)
 event [43, 229](#)
 browser [229](#)
 severity [43](#)
 events [232, 233](#)
 call events [232, 233](#)

F

fault management [39, 40, 41](#)
 alarm creation [41](#)
 alarms [40](#)
 event creation [40](#)
 events [39](#)
 Fault Management [12](#)
 file, sensor-specific configuration [611](#)

G

globaladmin [69](#)
 group [142, 143](#)
 add devices [142](#)
 create [142](#)
 remove devices [143](#)
 group management [448](#)

I

importing phone status tests [475](#)
 interface components [622, 624](#)
 filters [622](#)
 quick view [624](#)
 inventory collection [133](#)
 cluster device discovery [133](#)
 IP SLA ping [473](#)

J

job [569, 571](#)
 cancel [571](#)
 schedule [569](#)
 Jobs [567](#)

L

least used endpoint types [443](#)
 license usage [462](#)

M

Managing [139](#)
 groups [139](#)

Message-Waiting Indicator synthetic test [481](#)
 failure, after Cisco Unified CallManager upgrade [481](#)

N

NANP [386](#)
 no show conference [443, 444](#)
 no show endpoints summary report [419](#)
 notifications [198](#)
 SNMP traps, sending as [198](#)

P

phone status tests [477](#)
 modifying [477](#)
 phone tests summary portlet [519](#)
 polling and thresholds [191](#)
 parameters, managing [191](#)
 viewing [191](#)

R

Recommendations for Device Discovery [115](#)
 Reports [12](#)
 resetting Cisco 1040 [612](#)
 roles and tasks, mapping [69](#)

S

scheduled reports [466](#)
 seed file format. See <Default Para Font> import file format [475](#)
 service experience [454, 455, 456, 457, 458](#)
 endpoints with service quality issues [456](#)
 service experience distribution [455](#)
 top n call failure locations [457, 458](#)
 users with service quality issues [458](#)
 session detail report [417](#)
 sessions [252, 258, 262, 265, 268, 530](#)
 360 degree session view [265](#)
 dashboard [258](#)
 statistics [268](#)
 topology [265](#)
 troubleshoot [530](#)
 visibility [262](#)
 workflow [252](#)
 SMTP server message [378](#)
 smuser password [394, 396](#)
 stopping [608](#)
 QOVR process [608](#)
 Super administrator [69](#)
 synthetic tests, working with [477, 478, 484](#)
 adding tests [484](#)
 Dial-Tone [484](#)
 Cisco Unity Message-Waiting Indicator test, about [478](#)

synthetic tests, working with (*continued*)

- Dial-Tone test [478](#)
 - about [478](#)
- Emergency Call test [478](#)
 - about [478](#)
- End-to-End Call test [478](#)
 - about [478](#)
- Phone Registration test [477](#)
 - about [477](#)
- TFTP Download test [478](#)
 - about [478](#)

syslog notifications [199](#)

T

- technology adoption [438, 439, 440, 441, 442](#)
 - endpoint model call distribution [440, 441](#)
 - endpoint model deployment distribution [439, 440](#)
 - endpoint type call distribution [441, 442](#)
- telepresence room utilization [443](#)
- TFTP Download synthetic tests [481](#)
 - adding [481](#)
- TFTP Server [606](#)
- traffic analysis [444, 445, 447](#)
 - call traffic analysis [447](#)

traffic analysis (*continued*)

- top n call traffic locations [447](#)
- top n callers [445](#)
- top n dialed numbers [445](#)
- top n off-net traffic locations [445](#)
- traps, SNMP [608](#)
 - from Cisco 1040s, suppressing [608](#)
- troubleshoot [533, 543](#)
 - report [543](#)
 - starting [533](#)

U

- uc system performance [462](#)
- UCCE [463](#)
- User Accounts [69](#)

V

- video collaboration dashboard [375](#)
 - Customizing [375](#)
- video conferences [459](#)
- Video Path Analysis [547](#)
- Voice and Video Endpoint Monitoring [11](#)

