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 NONINFRINGEMENT 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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

PART I

Introduction 1

CHAPTER 1

New and Changed Information 3

CHAPTER 2

Overview of Cisco Prime Collaboration Assurance 5

- Standard and Advanced Cisco Prime Collaboration Assurance 5
- Cisco Prime Collaboration Assurance—Standard Features 13
  - Device Inventory Management in Standard 13
  - Monitor and Fault Management in Standard 13
- Cisco Prime Collaboration Assurance—Advanced Features 14
  - Voice and Video Unified Dashboard 14
  - Device Inventory Management 15
  - Voice and Video Endpoint Monitoring 15
  - Diagnostics 16
  - Fault Management 16
  - Reports 17
- Cisco Prime Collaboration Assurance Support for IPv6 17

Overview of Cisco Prime Collaboration Assurance—MSP Mode 19

Differences Between the Enterprise Mode and the MSP Mode 22

Cisco Prime Collaboration Assurance NBI 23

Cisco Prime Collaboration Geo-Redundancy 23

What's New in Cisco Prime Collaboration Assurance 11.0—Advanced 23

CHAPTER 3

Concepts 27

- Event 27
- Alarm 28
- Event Creation 29
- Alarm Creation 29
Event and Alarm Association 30
Event and Alarm Correlation 30
Event Aggregation 31
Event Masking 31
Alarm Status 31
Event Severity 32
Event and Alarm Database 33
Alarm Notifications 33

CHAPTER 4  Get Started with Cisco Prime Collaboration Assurance 35
Get Started with Cisco Prime Collaboration Assurance 35

PART II  Set Up the Server 41

CHAPTER 5  Enable Third-Party CA Signed Certificate 43
Install CA Signed Certificate for Secure Data Transmission 43
Install CA Signed Certificate 44

CHAPTER 6  Manage Licenses 47
Cisco Prime Collaboration Assurance Licensing 47
Cisco Prime Collaboration Analytics Licensing 48
Enable and Disable Analytics 48
Cisco Prime Collaboration Contact Center Assurance Licensing 49
License Count 50
Phone Count in Cisco Prime Collaboration Assurance 50
View License Details 50
Add and Delete a License File 51
Switch Between the Standard and Advanced Modes in Cisco Prime Collaboration 52

CHAPTER 7  Manage Users 55
Cisco Prime Collaboration Assurance-Advanced User Roles 56
Single Sign-On for Cisco Prime Collaboration 56
Default User Accounts 58
User Roles and Tasks 59
Add, Edit, and Delete a User 59
Modify User Roles 60
Configure an LDAP Server 61
LDAP Configuration Parameters 61
Reset Cisco Prime Collaboration Assurance Passwords 63
Change Passwords 64

CHAPTER 8  Manage Customers 65
Add Customers 65
Global Customer Selection 66

CHAPTER 9  Manage Assurance Domains 67
Manage Assurance Domains 67
Add Assurance Domains 67
Global Assurance Domain Selection 68

CHAPTER 10 Configure System Parameters 69
Configure System Parameters 69
Global System Parameters 70
Configure SMTP Server 71
Configure Cisco Prime Collaboration Assurance Server Time Zone 72

PART III  Manage Devices in Cisco Prime Collaboration Assurance 73

CHAPTER 11 Manage Device Credentials 75
Manage Device Credentials 75
Add a Device Credentials Profile 76
Credential Profiles Field Descriptions 76
SSL Certificate Authentication for Device Discovery 80
Modify Device Credentials 80
Verify Device Credentials 81
Credential Verification Error Messages 82
Delete a Device Credential Profile 84

CHAPTER 12 Set Up Clusters 85
Manage Cisco TelePresence Manager or Cisco TMS or Cisco TelePresence Exchange (CTX) clusters 85

CHAPTER 13
Discover Devices 87
Discover Devices 87
Discovery Life Cycle 87
Discovery Methods 90
Prerequisites and Recommendations 93
Automatic Discovery of Devices 99
Discovery Filters and Scheduling Options 101
Manual Discovery of Devices 102
Import Devices 103
Export Device Lists and Credentials 105
Discovery of Cisco Unified Computing System (UCS) 105
Unified CM Cluster Data Discovery 107
Schedule Cluster Data Discovery 108
Rediscover Devices 109
Rediscover Deleted Devices 110
Verify Discovery Status 110
Troubleshooting 111

CHAPTER 14
Manage Device Groups 113
About Device Groups 113
Create Groups 116
Add Devices to a Group 116
Remove Devices from a Group 117
Device Group Selector 117

CHAPTER 15
Manage Inventory 119
View Inventory Details 119
Inventory Pane 120
Device 360° View 124
Global Search Options for Cisco Prime Collaboration Assurance 127
Assurance Inventory Summary 130
Device-Specific Inventory Details 130
Update and Collect Inventory Details 143
   Update Inventory 143
   Job Schedule - Field Descriptions 145
   Inventory Details Collection 145
   IP Phone Discovery Schedule 146
   View and Add an IP Phone Collection Status 146
   Schedule IP Phone XML Discovery Schedule 147
Suspend and Resume Managed Devices 148
Delete Devices 149
Performance Graphs 149
Perform Device Search 155
SNMP Query 156

---

**CHAPTER 16**

**Poll Devices** 159
   Overview 159
   Polling Parameters— Settings 160
   View Polling Parameters 161
   Edit Polling Parameters 161

---

**PART IV**

**CHAPTER 17**

**Configure Notifications** 165
   Configure Notifications 165
   Notification Groups 166
   Notification Criteria 167
   Types of Notifications 167
   SNMP Trap Notifications 168
   Syslog Notifications 176
   Notifications Limited to Specific Alarms 177
   Add an Alarm Set 178
   Add a Device Notification Group 178
      General Information Field Descriptions 179
   Set up Destinations Field Descriptions 180
   Alarm & Event Setup 182
CHAPTER 18
Set Threshold Rules  183
Threshold Rules  183
Configure TelePresence Endpoint Thresholds—Global  185
Configure TelePresence Endpoint Threshold—Device Level  185
Enable Automatic Troubleshooting for TelePresence Endpoints  186
Overview of Device Pool Thresholds  186
Edit Device Pool Thresholds  187
Overview of Voice Call Grade Settings  188
Add Dynamic Syslogs  188
Correlation Rules  190
Create Custom Events  193
Custom Alert Parameters  193

CHAPTER 19
Monitor Alarms and Events  197
Alarms and Alarm Summary  197
Events  200
View Call Events  202

PART V
Monitor the Network  205

CHAPTER 20
Monitor Video Endpoints  207
Endpoint Diagnostics Dashboard  207
View User 360 Details  209

CHAPTER 21
Monitor Sessions  211
Monitor Sessions  211
Data Collection for Video Sessions  212
Import Sessions from CTS-Manager and Cisco TMS  215
Session Workflow and Scenarios  216
Session Diagnostics Dashboard  222
Realtime Visibility of an Endpoint  226
360° Session View  228
Session Topology  229
Endpoint Statistics  231
PART VI
Dashboards and Reports 233

CHAPTER 22
Cisco Prime Collaboration Dashboards 235
Cisco Prime Collaboration Dashboards 235
Ops View 237
Summary 240
Endpoint by Device Pool 241
Topology—Cisco Unified Communications Manager or Cisco TelePresence Video Communication Server Cluster 242
View Information in the Cluster 244
Search for Devices 246
Connected Devices 246
Performance 246
Route Pattern Summary 246
Device Search 247
Endpoint Registration Summary 247
Availability Summary 248
Service Experience/Call Quality 248
Top 5 Poor Voice Call Quality Locations 248
Top 5 Call Failure Locations 249
Top 10 TelePresence Endpoints with Call Quality Alarms 250
Session with Alarms 250
Alarm Dashboard 250
Top 10 Impacted TelePresence Endpoints with Alarms 250
Top 10 Devices with Alarms 250
Infrastructure Alarm Summary 250
Utilization Monitor 251
Trunk Utilization 251
Route Group Utilization 252
Trunk Group Utilization 253
Location CAC Bandwidth Usage 253
Conferencing Devices 254
Conductor Bridge Pool Utilization 254
TelePresence Endpoint 255

Cisco Prime Collaboration Assurance Guide - Advanced, 11.0
Contents

Top 10 Utilized TelePresence Endpoints 255  
Top 10 Utilized TelePresence Endpoint Models 256  
Top 10 No Show TelePresence Endpoints 256  
Least 10 Utilized TelePresence Endpoints 256  
Least 10 Utilized TelePresence Endpoint Models 256  
Number of TelePresence Session 256  
License Usage 257  
Prime License Manager 257  
VCS License Usage 257  
Customer Voice Portal License Usage 258  
Contact Center Enterprise License Usage 259  
TelePresence Exchange Dashboard 260  
Customer Summary Dashboard 261  
Contact Center Assurance Topology Dashboard 263  
Performance Dashboards 265  
Unified CM and Unity Connection 265  
System Summary 266  
Communications Manager Summary 266  
Call Activity 267  
Gateway Activity 267  
SDL Queue 268  
Cisco TFTP 269  
CPU and Memory 270  
Disk Usage 271  
CTI Manager 272  
Heartbeat 272  
SIP Activity 273  
Process 273  
Database Summary 275  
Phone Summary 276  
Device Summary 276  
IM and Presence Summary 277  
Cisco Jabber Summary 278  
Learned Patterns 278  
Port Monitor 279
View Historical Trends 280
Create Custom Performance Dashboards 280
Add a Customized Dashboard 282

CHAPTER 23
Cisco Prime Collaboration Reports 283
Prerequisites to Generate the Cisco Prime Collaboration Reports 283
Update CDR Data Source Credentials 284
  Add a Data Source Credential 284
  Add Multiple Data Source Credentials 285
Use Data Source Credentials to Troubleshoot Problems and Verify Credentials 285
Call Classification 286
  Understand OffNet and OnNet Calls 288
Call Category Creation 289
Dial Plan Addition 289
  Understand the Default Dial Plan 289
  Add a Dial Pattern to a Dial Plan 293
  Apply Dial Patterns to VG/Trunk-Outgoing, Internal, and OnNet Trunk Calls 294
Configure Gateway Codes 294
Configure SFTP Settings 295
  SFTP Settings Page - Field Descriptions 295
Administrative Reports 296
CDR & CMR Call Report 297
  Generate CDR & CMR Reports 303
  Troubleshoot 306
NAM & Sensor Report 307
  Understand Sensor Reports 312
  View Sensor Stream Correlation Data 312
Session Reports 316
  All Session Summary Report 316
  Session Detail Report 317
TelePresence Endpoint Reports 317
  Endpoint Utilization Report 317
  No Show Endpoint Summary Report 317
Launch CUCM Reports 318
Miscellaneous Reports 318
UCM/CME Phone Activity Reports 318
   Audio Phone Move Report 318
   Audio Phone Audit Report 318
   Removed IP Phones Report 319
   Extension Number Changes Report 319
   Suspect Phones Report 319
   Duplicate MAC/IP Address Report 320
   Video Phone Move Report 320
   Video Phone Audit Report 320
   Removed Video Phones Report 321
   Video Phone Extension Number Changes Report 321
   Export Audio Phones Report 321
   Export Video Phones Report 322
   Understand the Time Period Covered by Audio IP Phone Activity Reports 323
   Track Phone Status when Cisco Unified CM Is Down 324

Voice Call Quality Event History Reports 324

Other Reports 325
   CTI Applications Report 325
   ATA Devices Report 326
   Cisco 1040 Sensors Report 326
   Conferencing Device Video Port Utilization Report 326

Scheduled Reports 327
   Generate Scheduled Reports 328

Access Data for Reports that Contain More than 2,000 Records 328

Troubleshoot File Download Issues 329

---

PART VII

Perform Diagnostics 331

CHAPTER 24

Diagnostics for Voice Endpoints 333
   Phone Status Test 333
      Create a Phone Status Test 334
   Import Phone Status Test 335
      Format Phone Status Test Import File 335
   Synthetic Test 337
   Prerequisites for Synthetic Tests 338
Create an Emergency Call Synthetic Test 339
Create a Message-Waiting Indicator Synthetic Test 340
Create a TFTP Download Synthetic Test 341
Create an End-to-End Call Synthetic Test 341
Create Dial-Tone Synthetic Tests 343
Create a Phone Registration Test 344
Import Synthetic Tests 344
Format Synthetic Test Import Files 345
Manage Synthetic Tests 350
Synthetic Test Notes 351
IP SLA Voice Tests 352
Required Cisco IOS and IP SLA Versions 354
Create an IP SLA Voice Test 355
Import Multiple IP SLA Voice Tests 360
Format IP SLA Voice Test Import Files 361
Manage IP SLA Voice Tests 363
IP SLA Voice Test Data 364
Create a Batch Test 371
Format Batch Test Import Files 371
Manage Batch Tests 372
Phone Tests—Batch and On Demand Tests 374
Create a Phone Test on Demand 376
UC Phone Tests SummaryAudio Phone Features Test 378
Update the JTAPIJAR files in Cisco Prime Collaboration Assurance 380
CME Diagnostics 380

CHAPTER 25

Diagnostics for Video Endpoints 383
Features of the Troubleshooting Workflow 384
Features of the Troubleshooting Workflow for Sessions 386
Features of the Troubleshooting Workflow for Endpoints 386
Support Matrix for Troubleshooting Source and Destination Endpoints 387
Traceroute Command 388
Cisco Performance Monitor 389
Start a Troubleshooting Workflow 389
MSI-enabled Device Troubleshooting 391
Troubleshoot Data Analysis  392
  Troubleshooting  392
  Logs  395
  Medianet Path View  396
    CPU and Memory  396
    CPU and Packet Loss  396
    Video IP Bit Rate and Packet Loss  397
    Video Interarrival Jitter and Packet Loss  398
    IP DSCP and Packet Loss  399
    Medianet Enabled Network  399
    View All Flows  400
    Performance Monitor  400
  Path Assessment  402
    Test Result  403
  Export Troubleshooting Data  404
    Understand the Export Troubleshooting Report  405
  Cisco Mediatrace  406
    WSMA and SNMP Support in Mediatrace 3.0  407
    Cisco Mediatrace on Switches  407
    Cisco Mediatrace Diagnostics  407
  Cisco Prime Infrastructure Cross-Launch  408
    Cross-Launch Cisco Prime Infrastructure  409
      Cisco Prime Infrastructure Pane - Field Descriptions  409

_______________________________
CHAPTER 26  411

Media Path Analysis  411
  Analyze Media Paths Using VSAA  411
    VSA Agent Assessment Results  412
  Manage a Video Test Call  414

_______________________________
CHAPTER 27  417

Collect Logs  417
  Log Collection Center  418
  Set the Trace Levels  420
  Log Collection Template  421
  Collect Call Logs  421
Overview of Cisco Prime NAM/vNAM 453
Perform Initial Configuration in Cisco Prime Collaboration 454
  Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files 454
  Add and Delete a TFTP Server 454
  Set Up the Cisco 1040 Sensor Default Configuration 455
  Cisco 1040 Sensor/NAM Setup Page—Graphical User Interface Elements 456
Configure Cisco 1040 Sensors in Cisco Prime Collaboration 456
  Cisco 1040 Sensor Details 457
  Add a Cisco 1040 Sensor 458
    Cisco 1040 Sensor/NAM Dialog Box—Graphical User Interface Elements
      Description 459
Edit Configurations for Multiple Cisco 1040s 459
  Cisco 1040 Management - Field Descriptions 460
  Reset Cisco 1040s 460
  Delete a Cisco 1040 Sensor 461
  View Diagnostic Information on a Cisco 1040 461

APPENDIX C

User Interface 463
  Overview 463
  Filters 464
  Launch the Advanced Filter and Save Filter Criteria 465
  Quick View 465
  View About Details 465
PART

Introduction

- New and Changed Information, page 3
- Overview of Cisco Prime Collaboration Assurance, page 5
- Concepts, page 27
- Get Started with Cisco Prime Collaboration Assurance, page 35
New and Changed Information

The following table describes the information that has been added or changed since the initial release of this guide.

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 14, 2015</td>
<td>Initial version</td>
<td>—</td>
</tr>
</tbody>
</table>
Overview of Cisco Prime Collaboration Assurance

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

- Standard and Advanced Cisco Prime Collaboration Assurance, page 5
- Cisco Prime Collaboration Assurance—Standard Features, page 13
- Cisco Prime Collaboration Assurance—Advanced Features, page 14
- Overview of Cisco Prime Collaboration Assurance—MSP Mode, page 19
- Differences Between the Enterprise Mode and the MSP Mode, page 22
- Cisco Prime Collaboration Assurance NBI, page 23
- Cisco Prime Collaboration Geo-Redundancy, page 23

Standard and Advanced Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance is available in the following modes:

- Cisco Prime Collaboration Assurance Standard—Enterprise mode
- Cisco Prime Collaboration Assurance Advanced—Enterprise and MSP mode

Cisco Prime Collaboration Assurance Standard is a simplified version of Cisco Prime Collaboration Assurance Advanced. It provides basic assurance features that help you manage Unified Communications 9.x and later and Cisco TelePresence components. You can monitor only one cluster per product for a single installation of Cisco Prime Collaboration-Standard.

For installing Standard and 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, troubleshooting, 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 assurance 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 sections Overview of Cisco Prime Collaboration Assurance—MSP Mode and Differences Between the Enterprise Mode and the MSP Mode.

The following table lists the features available in Cisco Prime Collaboration Assurance—Standard and Advanced.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Modes</td>
<td>It supports Enterprise mode only.</td>
<td>It supports both the Enterprise and MSP modes.</td>
<td>For more information on Advanced features, see the sections Overview of Cisco Prime Collaboration Assurance—MSP Mode and Differences Between the Enterprise Mode and the MSP Mode.</td>
</tr>
<tr>
<td>License Requirement</td>
<td>Does not require a license.</td>
<td>Requires license after evaluation expiry.</td>
<td>For more information on Advanced features, see the section Manage Licenses.</td>
</tr>
</tbody>
</table>
| Role Based Access Control| Supports Super Administrator role only.       | Supports five roles to provide multiple levels of authorization:  
  • Super Administrator  
  • System Administrator  
  • Network Administrator  
  • Operator  
  • Helpdesk            | For more information on Advanced features, see the section Manage Users.                                              |
| Single Sign-On Support   | Yes                                           | Yes                                           | For more information on Advanced features, see the section Manage Users.                                                |
| Cluster Management       | Manages only one cluster of Cisco Unified CM, one cluster of Cisco Unity and Cisco IM and Presence. | Manages multiple clusters with mixes of cluster revisions and cluster associations.                                         | For more information on Advanced features, see the section Set Up Clusters.                                              |
For more information on Advanced features, see the section *Discover Devices*.

| Discovery | • You can discover and manage endpoints that are registered to Cisco TMS and Cisco VCS.  
• You can add and manage Cisco Unified CM (including Cisco Unified IM and Presence) 9.x and later and Cisco Unity Connection 9.x and later applications.  
| Inventory Management | • You can discover and manage all endpoints that are registered to Cisco Unified CM (phones and TelePresence), Cisco VCS (TelePresence), CTS-Manager (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. |
| Provides multiple discovery modes such as Auto Discovery, Import, and Add Device features. |
| Provides a concise summary information for a device through the Device 360 view.  
Provides exhaustive Inventory details. |
<p>| Provides limited inventory information by using the Current Inventory Table. |
| For more information on Advanced features, see the section <em>Manage Inventory</em>. |</p>
<table>
<thead>
<tr>
<th>Fault Management</th>
<th>Provides an Alarms and Events browser.</th>
<th>Support for initiating troubleshooting by using quick views.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supports setting up email notifications for Alarm Sets.</td>
<td>Supports Alarm Correlation rules.</td>
</tr>
<tr>
<td></td>
<td>Supports creation of custom events for Unified Communications Performance Counters.</td>
<td>Supports customization of events at the device, and global level.</td>
</tr>
<tr>
<td></td>
<td>Supports set up of custom alerts based on selected metrics and corresponding thresholds. Once a threshold is violated, an alert is seen in the alarm browser.</td>
<td>Provides configuration of thresholds for:</td>
</tr>
<tr>
<td></td>
<td>• TelePresence Endpoints</td>
<td>• Infrastructure Device</td>
</tr>
<tr>
<td></td>
<td>• Call Quality</td>
<td>• Device Pool</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Voice and video Reports</th>
<th>NA</th>
<th>Provides the following predefined reports and customizable reports:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Administrative Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Communications Manager Reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Interactive Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Scheduled Reports</td>
</tr>
</tbody>
</table>

For more information on Advanced features, see the section Monitor Alarms and Events.

For more information on Advanced features, see the section Dashboards and Reports.
### Dashboards

- Provides predefined dashboards for Cisco Unified CM, IM and Presence, and Cisco Unity Connection.
- Supports creation of custom dashboards based on the desired performance counters for Cisco Unified CM, IM and Presence, and Cisco Unity Connection.

<table>
<thead>
<tr>
<th>Dashboards</th>
<th>Provides the following dashboards:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ops View - Provides high-level information about the Cisco Unified CM and VCS Clusters.</td>
<td></td>
</tr>
<tr>
<td>• Service Experience - Provides information about quality of service.</td>
<td></td>
</tr>
<tr>
<td>• Alarm - Provides information about alarm summaries.</td>
<td></td>
</tr>
<tr>
<td>• Performance - Provides details on critical performance metrics of each managed element.</td>
<td></td>
</tr>
<tr>
<td>• Contact Center Topology - Provides information about.</td>
<td></td>
</tr>
</tbody>
</table>

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.

For more information on Advanced features, see the section *Dashboards and Reports*. 
For more information on Advanced features, see the section *Perform Diagnostics*.

### Voice and Video Endpoint Diagnostics

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
</table>
| NA | - Provides a detailed analysis of the end-to-end mediapath, including specifics about endpoints, service infrastructure, and network-related issues.  
- Uses Cisco Mediant 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 |

### Job Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables you to view job status.</td>
<td>Enables you to view, schedule, and delete jobs.</td>
</tr>
</tbody>
</table>

### Cross Launch to UC Application

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device Search</td>
<td>UC Cluster Components Search and Status Capability - Enables you to define the search criteria to select specific cluster components, such as phones, H.323 gateways, Computer Telephony Integration (CTI) devices, voice mail devices, media resources, SIP trunks, or hunt lists that are associated with a Cisco Unified CM cluster.</td>
</tr>
</tbody>
</table>
| Cisco Prime Collaboration Analytics | NA | 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:
  - Technology Adoption
  - Asset Usage
  - Traffic Analysis
  - Capacity Analysis
  - Service Experience
  - UC System Performance
  - Scheduled Reports
  - Video Conferences
  - Custom Report Generator |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>See <a href="#">Cisco Prime Collaboration Analytics Guide</a>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Prime Collaboration Analytics is a licensed software, which has to be purchased separately with Cisco Prime Collaboration Assurance. Cisco Prime Collaboration Analytics is not supported in MSP mode deployment.

| NB API | NA | NB API is supported for the following:
  - Managing devices
  - Viewing and deleting device credentials
  - Listing all video sessions
  - Troubleshooting video sessions |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server with the administrator privilege and enter <a href="http://pc-server-ip/emsam/nbi/nbiDocumentation">http://pc-server-ip/emsam/nbi/nbiDocumentation</a> in the browser URL; where, pc-server-ip is the Cisco Prime Collaboration Assurance server IP address.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco Prime Collaboration Assurance—Standard Features

Cisco Prime Collaboration—Standard mode provides basic Assurance features that help you manage Unified Communications 9.x and later and Cisco TelePresence components. You can monitor only one Unified Communications Manager and one Video Communications Server (VCS) Expressway cluster per product for a single installation of Cisco Prime Collaboration—Standard. The features include:

- Support for Unified Communications 9.x and later components including Unified CM, Cisco Unity Connection, and Cisco IM and Presence
- Fault monitoring for core Unified Communications 9.x and later components (Unified CM 9.x and later, Cisco Unity Connection 9.x and later)
- Precanned and customizable performance metrics dashboards that display term trends for core Unified Communications 9.x and later components
- Contextual cross launch of serviceability pages of Unified Communications 9.x and later components
- Supports Super Administrator role only (Role Based Access Control is not applicable).
- Support for Single Sign-On

Device Inventory Management in Standard

You can add and monitor Cisco Unified Communications Manager (phones and TelePresence), Cisco VCS (TelePresence), CTS-Manager (TelePresence), and Cisco TMS (TelePresence).

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

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

- Add or remove Cisco Unified CM or Cisco Unity Connection
- Manage device credentials. This applies to Cisco TMS and associated devices only
- Discover devices. This applies to Cisco TMS and associated devices only

Monitor and Fault Management in Standard

Service operators must quickly isolate the source of any service degradation in the network for all voice and video sessions in an enterprise. Cisco Prime Collaboration provides a detailed analysis of the service infrastructure, and network-related issues.

Cisco Prime Collaboration periodically imports information from the managed devices based on the polling parameters you configure.

The Home page includes several preconfigured dashlets that help you monitor system performance, device status, device discovery, CTI applications, and voice messaging ports. These dashlets enable you to monitor a set of predefined management objects that monitor the health of the system. From the dashlets, you can launch contextual serviceability pages.
Cisco Prime Collaboration ensures near real-time quick and accurate fault detection. Cisco Prime Collaboration allows to monitor the events that are of importance to you. You can set up Cisco Prime Collaboration to send email notifications for alarms.

In addition to the faults that are present in the Cisco TelePresence Management System and Unified Communications applications, it also displays the custom tickets that are raised on Cisco TMS.

You can view the alarms and events in the system by using the Alarm browser. You can also configure Cisco Prime Collaboration to send email fault notifications. You can also view call connection or disconnection details related to the Cisco TMS applications, in the Call Events user interface.

Cisco Prime Collaboration 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 Call Signaling Analyzer feature for Unified CM to further zoom in on the collected calls and isolate faults in the messages. It also helps you to trace the issue as you can view the call ladder diagram that indicates faults in the call messages.

**Cisco Prime Collaboration Assurance—Advanced Features**

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

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
<th>Cisco Prime Collaboration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Experience</td>
<td>Information about quality of service.</td>
<td>Cisco Prime Collaboration Assurance Advanced</td>
</tr>
<tr>
<td>Alarm</td>
<td>Information about Alarm summaries.</td>
<td>Cisco Prime Collaboration</td>
</tr>
<tr>
<td>Contact Center Topology</td>
<td>Information about the Unified Contact Center Topology View.</td>
<td>Cisco Prime Collaboration Contact Center Assurance</td>
</tr>
</tbody>
</table>

See [Cisco Prime Collaboration Dashboards](#) to learn how the dashlets are populated after deploying the Cisco Prime Collaboration servers.
Device Inventory Management

You can discover and manage all endpoints that are registered to Cisco Unified Communications Manager (phones and TelePresence), Cisco Expressway (TelePresence), CTS-Manager (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 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 sessions in an enterprise.

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

- In-progress
- Scheduled
- Completed
- No Show

Cisco Prime Collaboration periodically imports information from:

- The management applications (CTS-Manager and Cisco TMS) and conferencing devices (CTMS, Cisco MCU, and Cisco TS) on the scheduled sessions.
- The call and sessions control devices (Cisco Unified CM and Cisco Expressway) shown on the registration and call status of the endpoints.
In addition, Cisco Prime Collaboration 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 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 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 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 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 server to IP phones.

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

Cisco Prime Collaboration 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, based on the severity.

Cisco Prime Collaboration 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 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 monitors faults.
Reports

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

- **CDR & CMR Reports**—Provides call details such as call category type, call class, call duration, termination type, call release code, and so on.
- **NAM & Sensor Reports**—Provides call details collected from Sensor or NAM such as MOS, jitter, time stamp, and so on.
- **Session Reports**—Provides the All Sessions Summary Report and Session Detail Report.
- **TelePresence Endpoint Reports**—Provides details on completed and in-progress session, 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 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 a 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*

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Notes or Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Inventory/Inventory - Credential Profile</td>
<td>Creation of IPv6 credential profiles.</td>
<td>—</td>
</tr>
<tr>
<td>Features</td>
<td>Supported</td>
<td>Notes or Limitations</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Device Inventory/Inventory - Discovery | • 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. | • 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. | — |
| Session Diagnostics | Endpoint Statistics (System and Session Information) shows IPv6 addresses.  
Endpoints Quick View shows IPv6 addresses. | — |
| 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. | — |
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.

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 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 with Public IP address also referred to as the Managed IP Address.

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

Cisco Unified Communications Manager cannot be shared, and must always be configured with the private IP address of the endpoints.
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 then the public domain.

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

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

**Figure 1: Cisco Prime Collaboration Deployment Scenarios**

**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
- Sessions 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 Management

For HCS-specific discovery details, see the HCS documents.

You can view and manage each customer's device 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), CTS-Manager (TelePresence), Cisco TMS (Cisco TelePresence) and Cisco TelePresence Exchange. 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 database.

Voice and Video Endpoint Monitoring

For video endpoints, Cisco Prime Collaboration enables you to monitor all point-to-point, multipoint, and multipoint video collaboration sessions for individual customers. These sessions 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 sessions diagnostics is only supported for endpoints with Public IP addresses.

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, 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 22 for more information on the Enterprise and the MSP modes.

Differences Between the Enterprise Mode and the MSP Mode

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

<table>
<thead>
<tr>
<th>Managed Service Provider (MSP) Mode</th>
<th>Enterprise Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comes with Advanced mode only.</td>
<td>Comes with both Advanced and Standard modes.</td>
</tr>
<tr>
<td>Enables you to create customers and add specific devices to them.</td>
<td>Enables you to create logical units in your enterprise called assurance domains. This is an optional feature in the Advanced mode. <strong>Note</strong> This feature is not available in the Standard mode.</td>
</tr>
<tr>
<td>Filters information, by customer, Inventory Management, phone inventory reports, session diagnostics, and endpoint diagnostics.</td>
<td>Filters information, by assurance domains, in the inventory table, Inventory Management, session diagnostics, and endpoint diagnostics.</td>
</tr>
<tr>
<td>Provides dashboards and dashlets on Cisco TelePresence Exchange (CTX) and Customer Summary.</td>
<td>Does not provide dashboards and dashlets on Cisco TelePresence Exchange (CTX) and Customer Summary.</td>
</tr>
<tr>
<td>IP SLA testing can be performed for a specific customer's routers and switches also.</td>
<td>IP SLA testing is available all for IP SLA-enabled routers and switches.</td>
</tr>
<tr>
<td>Provides support for CTX clusters and meeting types supported by CTX.</td>
<td>Does not support CTX.</td>
</tr>
<tr>
<td>Provides Role Based Access Control (RBAC) for customer groups.</td>
<td>Provides Role Based Access Control (RBAC) for assurance device pools and endpoints.</td>
</tr>
<tr>
<td>Supports Static NAT.</td>
<td>Does not support NAT.</td>
</tr>
<tr>
<td>Supports CTX manageability for both hosted and non-hosted deployment models.</td>
<td>Does not support CTX.</td>
</tr>
<tr>
<td>RTP-based diagnostics tests (for example, Synthetic tests) are only supported in a non-NAT environment.</td>
<td>All functionalities are supported.</td>
</tr>
<tr>
<td>In a NAT environment, for phones, the data from Phone XML discovery is not available. Video session stats and session information will not be available for phones even if they are set to full visibility.</td>
<td>All functionalities are supported.</td>
</tr>
<tr>
<td>Sensor-based call quality reports are not available.</td>
<td>All reports are available.</td>
</tr>
</tbody>
</table>
### Managed Service Provider (MSP) Mode vs. Enterprise Mode

<table>
<thead>
<tr>
<th>Function</th>
<th>MSP Mode</th>
<th>Enterprise Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>TelePresence endpoint health monitoring</td>
<td>Only supported for endpoints with Public IP addresses.</td>
<td>All functionality is supported.</td>
</tr>
<tr>
<td>Video session diagnostics</td>
<td>Only supported for endpoints with Public IP addresses.</td>
<td>All features of video session diagnostics are supported.</td>
</tr>
<tr>
<td>Auto Discovery</td>
<td>Not supported.</td>
<td>Auto Discovery is supported.</td>
</tr>
<tr>
<td>Medianet</td>
<td>Only supported for endpoints with Public IP addresses.</td>
<td>All features of Medianet are supported.</td>
</tr>
</tbody>
</table>

### 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.

To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server with the administrator privilege and enter `http://<pc-server-ip>/emsam/nbi/nbiDocumentation` in the browser URL. The pc-server-ip is the Cisco Prime Collaboration Assurance server IP address.

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. See the *Configure Alarm and Event Notification* section in the Cisco Prime Collaboration Assurance Guide - Standard for more information.

### Cisco Prime Collaboration 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 license to configure Geo-Redundancy. For more information on Geo-Redundancy, see Geo-Redundancy for Cisco Prime Collaboration Assurance and Analytics.

### What's New in Cisco Prime Collaboration Assurance 11.0—Advanced

Cisco Prime Collaboration Assurance provides the following new features:
User Interface Changes

Cisco Prime Collaboration Assurance has a new user interface to give you a simplified user experience and includes the following:

- You can click the **Toggle Navigation** icon to view a list of dashlets and reports.
- 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.
- You can click the pin icon at the top left to hide or display the left pane.
- Upgrade icon on the global toolbar is changed to Get Advanced icon.
- Getting Started popup is moved to the left pane of the menu bar.

Dashboards

- You can view Customer Voice Portal License Usage dashlet under License Usage dashboard to view license usage for CVP call servers. See *Customer Voice Portal License Usage*, on page 258.
- You can view Contact Center Enterprise License Usage dashlet under License Usage dashboard to view the list of devices, capability of the device, and the number of agents logged on to the devices. See *Contact Center Enterprise License Usage*, on page 259.
- You can view Severely Conceal Seconds Ratio, Conceal Seconds Ratio, Conceal Seconds, and Severely Conceal Seconds values in Call Details pane of Call Quality Troubleshooting page. See *Overview of Voice Call Grade Settings*, on page 188.
- The OpsView dashlet is enhanced to display the hard and soft unregistered endpoints count as a separate entity. See *Ops View*, on page 237.
- Conductor Bridge Pool Utilization dashlet is added as a tab on the Utilization Monitor page. The dashlet provides information about the cumulative utilization of the conference bridges for each conductor pool in your network. See *Conductor Bridge Pool Utilization*, on page 254.
- You can view a new set of performance counters loaded for Cisco SocialMiner devices till version 11.0.

Reports

- Voice call quality grading is performed based on the Severely Conceal Seconds Ratio (SCSR) (%) value in the following reports:
  - CDR & CMR Reports
  - NAM & Sensor Reports
  - Voice Call Quality Event History Reports

See *Overview of Voice Call Grade Settings*, on page 188.

- CDR & CMR Report is simplified to enhance the user experience. You can filter the CDR & CMR Report by using the **Display** filter panel. See *CDR & CMR Call Report*, on page 297.
• Monitoring and Diagnostics

  • Session monitoring is supported for Collaboration Edge meetings and includes topology construction of MRA endpoints for Point-to-point, Multipoint, and Multisite sessions. See Session Workflow and Scenarios, on page 216.

  • Cascading of Cisco TelePresence Servers allows you to monitor TelePresence servers during ad hoc conference calls over Cisco TelePresence Conductor. See Session Diagnostics Dashboard, on page 222.

  • The following new alarm is generated - CDRNotReceived. See the Supported Alarms and Events for Cisco Prime Collaboration.

  • The Cisco Integrated Management Controller Hardware Fault trap is generated to troubleshoot any fault in the hardware components of Cisco Integrated Management Controller device.

  • The VXML Server alert trap is supported from CVP devices. For more information, see the Supported Alarms and Events for Cisco Prime Collaboration.

  • You can cross launch to CMR report from Last Call Quality column under 360 User View.

  • You can cross-launch Cisco Prime Infrastructure features for devices that are managed in both Cisco Prime Infrastructure and Cisco Prime Collaboration applications to perform network diagnosis and troubleshooting for a session. See Cisco Prime Infrastructure Cross-Launch, on page 408 for more information.

• General

  • Cisco Prime Collaboration Assurance licensing is simplified, and based on the number of endpoints only. The endpoint type or category does not affect the number of licenses required.

  • Cisco SocialMiner and Cisco Integrated Management Controller (CIMC) devices are supported for this release. See Supported Devices for Cisco Prime Collaboration Assurance.

  Note

  Cisco Prime Collaboration supports only Cisco Integrated Management Controller (CIMC) traps for this release. You must manually add the device on the Inventory Management page.

  • CDR Report now reports the following video codecs: H.264 and H.265.

  • Log Collection Center and Call Signaling Analyzer features are now supported in MSP mode also.

  • The Cisco Prime Collaboration ordering structure and pricing model is reduced and simplified to make ordering easier. From 11.0 release, all tiers and voice and video endpoint classification product numbers are removed. You now order Cisco Prime Collaboration 11.0 by specifying the number of endpoints managed, regardless of the type of endpoint. See the Cisco Prime Collaboration 11 Ordering Guide for more information.

  • Cisco Prime Collaboration supports Geo-Redundancy from this release. See Cisco Prime Collaboration Geo-Redundancy, on page 23 for more information.

• Features or Devices Not Supported From This Release

  The following features or devices are not supported from 11.0 release:

  • The IP SLA Video Operations test for video endpoints is not supported.
Note  IP SLA Voice Test feature is still supported.

* Cisco Unity devices are not supported.
* Survivable Remote Site Telephony (SRST) Test is not supported
* The integration of Cisco Deployment Manager with Cisco Prime Collaboration Assurance is not supported.
* The convergence of Cisco Prime Collaboration Provisioning and Cisco Prime Collaboration Assurance applications is no longer supported. Hence, the attach and detach functions are not supported.
* Most Impacted Endpoints by Sensor/NAM, Most Impacted Endpoints by CDR, and Export Most Impacted Endpoints reports are not supported. However, you can view these reports by typing the hidden URLs in the address bar of the browser.
* Contacting Cisco Technical Assistance Center (TAC) by using the user interface is not supported.
CHAPTER 3

Concepts

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

Some of the concepts like alarm correlation rules are not applicable to Cisco Prime Collaboration Standard.

- Event, page 27
- Alarm, page 28
- Event Creation, page 29
- Alarm Creation, page 29
- Event and Alarm Association, page 30
- Event and Alarm Correlation, page 30
- Event Aggregation, page 31
- Event Masking, page 31
- Alarm Status, page 31
- Event Severity, page 32
- Event and Alarm Database, page 33
- Alarm Notifications, page 33

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:

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

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, the preset period is 60 minutes.

Event and Alarm Association

Cisco Prime Collaboration maintains a catalog of events and alarms. The catalog contains the list of events managed by Cisco Prime Collaboration, 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 compares an incoming notification against the event and alarm catalog.

2 Cisco Prime Collaboration decides whether an event has to be raised.

3 If an event is raised, Cisco Prime Collaboration 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 to create alarms for these events, you must change the severity of these events.

---

Event and Alarm Correlation

Event correlation is the process of relating one event to other events.

Cisco Prime Collaboration distinguishes two event relationship types:

• An event sequence. Events that have the same type and the same source are considered part of an event sequence, or an alarm. An alarm represents the complete lifecycle of a fault.
• An event sequence hierarchy (alarms), representing causality.

Cisco Prime Collaboration associates a new event to an existing alarm if the existing alarm has the same event type and source as the new event.

Cisco Prime Collaboration raises an alarm, if the number of related events received (by fault management system) from the device element exceeds a specified threshold in a specified unit of time, based on predefined correlation rules.

Example use cases:

• Call Manager location goes out-of-resource for more than five times over the last one hour.

• CPU usage of a device is over 80% for the last 15 minutes.

You can modify these rules and configure the number of event occurrences to set the trigger. This can vary from two to 100. You can also set the time interval. You can modify these rules at Assurance Administration > Event Customization > Correlation Rules.

If an administrator does not specify a time interval, maximum time period, or a count for a specific alarm, the default values for the time interval, maximum time period, and count is attached on an alarm, device type, or device class basis.

Event Aggregation

If the number of same event received from a set of elements exceeds a specified threshold, Cisco Prime Collaboration 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 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 masks all its component (such as powersupply, interface, fan) events.

• When a switch card goes down, Cisco Prime Collaboration masks all the contained port level events.

Alarm Status

The following are the supported statuses for an alarm:
### Table 2: Alarm Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Acknowledged</td>
<td>When an event triggers a new alarm or an event is associated with an existing alarm.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>When you acknowledge an alarm, the status changes from Not Acknowledged to Acknowledged</td>
</tr>
<tr>
<td>Cleared</td>
<td><strong>System-clear from the device</strong>—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. <strong>Alarms are also triggered during the session</strong> because of packet loss, jitter, and latency. These alarms are auto-cleared after the session ends. <strong>Manual-clear from Cisco Prime Collaboration users</strong>: 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. <strong>If the fault continues to exist in the network</strong>, a new event and alarm are created subsequently based on the polling. <strong>Auto-clear from the Cisco Prime Collaboration server</strong>—Cisco Prime Collaboration clears all session-related alarms, when the session ends. If there are no updates to an active alarm for 24 hours, Cisco Prime Collaboration automatically clears the alarm.</td>
</tr>
</tbody>
</table>

**Note** Certain alarms might get cleared automatically before 24 hours. See [Supported Events and Alarms for Prime Collaboration](#).

---

### Event Severity

Each event has an assigned severity, and can be identified by its color in Cisco Prime Collaboration. 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 allows you to customize the settings and severity of an event. The events that are of importance to you can be given higher severity. For more information on how to customize the event settings, see *Customize Alarms and Events* section in the [Cisco Prime Collaboration Assurance Guide - Standard](#).

The event settings and severity predefined in the Cisco Prime Collaboration 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 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.

---

**Note**

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

---

**Alarm Notifications**

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

For more information on how to configure the notifications, see the *Configure Alarm and Event Notification* section in the *Cisco Prime Collaboration Assurance- Standard*. 
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

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task and Description</th>
<th>Navigation in Cisco Prime Collaboration Assurance Application</th>
<th>Document to be referred</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Add a new license file. This step is applicable only if you have purchased Assurance Advanced and/or Analytics license.</td>
<td>System Administration &gt; License Management</td>
<td>Cisco Prime Collaboration Assurance Guide - Advanced</td>
</tr>
<tr>
<td>Step 2</td>
<td>Manage Users and Roles Add a new user</td>
<td>System Administration &gt; User Management</td>
<td>Cisco Prime Collaboration Assurance Guide - Advanced</td>
</tr>
</tbody>
</table>
### Task and Description

#### Step 3
Define credentials. Enter the required device credentials to manage devices in Cisco Prime Collaboration. For more details, see Setting up Devices for Prime Collaboration.

#### Navigation in Cisco Prime Collaboration Assurance Application
In Advanced mode, **Device Inventory > Inventory Management > Auto Discovery > Manage Credentials**
In Standard mode, **Device Inventory > Current Inventory**

#### Document to be referred
Cisco Prime Collaboration Assurance Guide - Advanced

---

#### Step 4
**Standard mode**
- Discover Cisco Unified Communications Manager (including Cisco Unified IM and Presence) 10.x and Cisco Unity Connection 10.x applications.
- Discover Cisco TMS
- Discover Cisco Expressway

**Note** In standard mode, CTS-Manager discovery is not applicable. The Cisco Expressway, Cisco MCU, Cisco Profile and Codec, default gateway, and switches are discovered along with Cisco TMS.
Cisco TelePresence Conductor is not auto discovered through TMS. The Cisco TelePresence Conductor need to be discovered separately.

**Navigation in Cisco Prime Collaboration Assurance Application**
**Device Inventory > Current Inventory**

**Document to be referred**
Cisco Prime Collaboration Assurance Guide - Standard
<table>
<thead>
<tr>
<th>Task and Description</th>
<th>Navigation in Cisco Prime Collaboration Assurance Application</th>
<th>Document to be referred</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Inventory &gt; Inventory Management &gt; Auto Discovery &gt; Devices Discovery</td>
<td></td>
<td>Cisco Prime Collaboration Assurance Guide - Advanced</td>
</tr>
</tbody>
</table>
### Advanced mode
- Discover CTS-Manager
- Discover Cisco TMS
- Discover CUCM
- Discover Cisco Expressway
- Discover VCS
- Discover Expressway-Core
- Discover CVP OAMP

The Cisco Unified CM, Cisco TelePresence Multipoint Switch, Cisco TelePresence System, default gateway, and switches are discovered along with CTS-Manager. The Cisco Expressway, Cisco MCU, Cisco Profile and Codec, default gateway, and switches are discovered along with Cisco TMS.

Cisco TelePresence Conductor is not auto discovered through CTS-Manager/TMS. The Cisco TelePresence Conductor need to be discovered separately.

The CVP Call Server, Reporting Server, VXML Server, Cisco Unified IC, Cisco Unified CCE (ICM), Cisco Packaged Contact Center Enterprise (PCCE), Gateways (IOS and VXML) also get discovered along with CVP OAMP, provided they have been added in CVP OAMP.

The other Contact Center
<table>
<thead>
<tr>
<th>Task and Description</th>
<th>Navigation in Cisco Prime Collaboration Assurance Application</th>
<th>Document to be referred</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assurance devices, such as MediaSence, Finesse, and so on get discovered only if you have added the devices to Cisco Prime Collaboration Assurance Advanced. <strong>Note</strong> CVP OAMP discovery is applicable only in the Enterprise mode. To discover Contact Center Assurance devices in the MSP mode, you need to manually add the devices to Cisco Prime Collaboration Assurance Advanced.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> Verify Inventory <strong>Note</strong> This step is applicable only if you have purchased Advanced and/or Analytics license. Verify whether all discovered devices are in the Managed state.</td>
<td><strong>Device Inventory &gt; Inventory Management</strong></td>
<td><strong>Cisco Prime Collaboration Assurance Guide - Advanced</strong></td>
</tr>
</tbody>
</table>

Get Started with Cisco Prime Collaboration Assurance
<table>
<thead>
<tr>
<th>Step 6</th>
<th>Task and Description</th>
<th>Navigation in Cisco Prime Collaboration Assurance Application</th>
<th>Document to be referred</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Import Sessions</td>
<td>Diagnose &gt; Session Diagnostics</td>
<td>Cisco Prime Collaboration Assurance Guide - Advanced</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This step is applicable only if you have purchased Advanced and/or Analytics license. Import the video collaboration sessions from CTS-Manager, Cisco TMS, and Cisco TelePresence Multipoint Switch to monitor the sessions. To periodically import sessions from CTS-Manager, Cisco TMS, and Cisco TelePresence Multipoint Switch, define the polling interval based on your business needs, using <strong>Diagnose &gt; Session Diagnostics &gt; Import Session</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify Sessions</td>
<td>Diagnose &gt; Session Diagnostics</td>
<td>Cisco Prime Collaboration Assurance Guide - Advanced</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This step is applicable only if you have purchased Advanced and/or Analytics license. Verify whether all session details have been imported from CTS-Manager, Cisco TMS, and Cisco TelePresence Multipoint Switch. Cisco Prime Collaboration collects scheduled sessions data for five days (for the past one day, for the current day, and for three days ahead).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PART II

Set Up the Server

- Enable Third-Party CA Signed Certificate, page 43
- Manage Licenses, page 47
- Manage Users, page 55
- Manage Customers, page 65
- Manage Assurance Domains, page 67
- Configure System Parameters, page 69
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 for Secure Data Transmission, page 43

Install CA Signed Certificate for Secure Data Transmission

To install CA signed certificate for secure data transmission, perform the following tasks:

- Generate Certificate Signing Request (CSR)
- Install CA signed Certificate

To generate CSR:

Procedure

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the following details:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name</td>
<td>You must enter the name of your country in alphabets with 2 characters. Special characters, numbers, and space are not allowed. Example: GB, IN, US, SG, and so on.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>You must enter the name of your state or province in alphabets with minimum of one character. Special characters and numbers are not allowed.</td>
</tr>
<tr>
<td>Locality Name</td>
<td>You must enter the name of your locality in alphabets with minimum of one character. Special characters and numbers are not allowed.</td>
</tr>
</tbody>
</table>
You must enter the name of your organization in alphabets with minimum of one character. Special characters and numbers are not allowed. Example: Cisco System Inc

You must enter the name of your organizational unit in alphabets with minimum of one character. Special characters and numbers are not allowed. Example: XL Cisco

You must enter the server's IP address or hostname. Common Name (IPAddress or Host/FQDN)

Step 3 Click Generate CSR.
Step 4 Click Download CSR and save the file on your local system.
Step 5 Send the generated CSR to the CA for signing.
Step 6 After the CSR is signed by CA, download it on your local system in PKCS#7 format. For information on how to install the downloaded certificate, see section Install CA Signed Certificate.

Note: We recommended you to use the certificates only in PKCS#7 (.p7b) format as PEM/DER (.pem, .cer, .der, .key, and so on) formats are not supported.

### Install CA Signed Certificate

To install CA signed certificate:

**Procedure**

Step 2 Click Import Certificates and browse through the CA signed Certificate (in PKCS7 format) from your local system.
Step 3 Click Import. A warning message is displayed, stating that the services will be restarted.
Step 4 Click Continue on receiving the warning message. The certificates are successfully imported on the server and the services are restarted. 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.
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.

We recommend you to use the certificates in PKCS#7 (.p7b) format as PEM/DER (.pem, .cer, .der, .key, and so on) formats are not supported.

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

<table>
<thead>
<tr>
<th>Browser</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>Choose <strong>Tools &gt; Internet Options &gt; Content &gt; Certificates &gt; Trusted root certification authorities &gt; Import</strong></td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Choose <strong>Tools &gt; Options &gt; Advanced &gt; Certificates &gt; View certificates &gt; Import</strong></td>
</tr>
<tr>
<td>Chrome</td>
<td>Choose <strong>Settings &gt; Advanced settings &gt; HTTP/SSL Manage certificates &gt; Trusted root certification authorities &gt; Import</strong></td>
</tr>
</tbody>
</table>
Install CA Signed Certificate for Secure Data Transmission
Manage Licenses

The Cisco Prime Collaboration license enables the endpoint quantities for the Cisco Prime Collaboration 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 either Standard or Advanced mode. Cisco Prime Collaboration Assurance in Standard mode does not require a license.

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 can be extended from the initial period of 60 days. You need to contact the Cisco licensing team to extend the evaluation period. 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.

- Cisco Prime Collaboration Assurance Licensing, page 47
- Cisco Prime Collaboration Analytics Licensing, page 48
- Cisco Prime Collaboration Contact Center Assurance Licensing, page 49
- License Count, page 50
- View License Details, page 50
- Add and Delete a License File, page 51
- Switch Between the Standard and Advanced Modes in Cisco Prime Collaboration, page 52

Cisco Prime Collaboration Assurance Licensing

Cisco Prime Collaboration—Standard does not require a license. After you install the Standard version, you can activate the Evaluation mode from within Cisco Prime Collaboration by using the Activate Advanced Features link in the Getting Started popup window. After the evaluation expires, it comes back to Standard
mode. If you need to continue in Advanced mode after evaluation expires, you need to obtain license for Cisco Prime Collaboration—Advanced.

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 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.

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.

When you switch over from the Standard to the Advanced mode in Cisco Prime Collaboration Assurance, the Cisco Prime Collaboration Analytics is installed in the Evaluation 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.

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.

Procedure

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 server as admin user using CLI.

Enter the following commands to restart the processes and for the changes to take effect:
```
application stop cpcm
```
Wait approximately 10 to 15 minutes for all the processes to stop, after which you will receive a message indicating the successful completion of the command. To confirm if the processes have stopped, run the command `show application status cpcm`

```
application start cpcm
```
Wait approximately 10 to 15 minutes for all the processes to start. To confirm if the processes have started, run the command `show application status cpcm`.

**Note** For very large deployment, you must run the above commands on Cisco Prime Collaboration Assurance application and database servers.

Step 5 Enter the following command to restart the processes and for the changes to take effect:
```
application stop cpcm
```
Wait approximately 10 to 15 minutes for all the processes to stop, after which you will receive a message indicating the successful completion of the command. To confirm if the processes have stopped, run the command `show application status cpcm`.

```
application start cpcm
```
Wait approximately 10 to 15 minutes for all the processes to start. To confirm if the processes have started, run the command `show application status cpcm`.

**Note** For very large deployment, you must run the above commands on Cisco Prime Collaboration Assurance application and database servers.

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 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 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. After the evaluation period for Cisco Prime Collaboration Assurance Advanced expires, you can access Cisco Prime Collaboration Assurance Standard mode only.

Upon license expiry, the Unified Contact Center infrastructure devices are not displayed in the UC Performance dashboard, Threshold Rules, and Correlation Rules windows. Call Signaling 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 Assurance, the license count is updated after a discovery task is performed. For example, the license count for Managed endpoints is updated a few minutes (approximately five minutes) after device discovery. Cisco Prime Collaboration only counts endpoints that are in Managed state (registered or unregistered).

⚠️ Caution

If the number of endpoints exceeds the license count, endpoints are randomly managed in the Cisco Prime Collaboration Assurance server.

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

Phone 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

From 11.0 release, each endpoint is counted; and Jabber and IP Phones are now counted separately.

The Prime License Manager dashlet (in the Infrastructure dashboard) displays the license usage for all collaboration applications. The VCS License Usage dashlet provides information about Video Communication Server license usage. For more information about these dashlets, see License Usage.

View License Details

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

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. In Standard mode, the usage is shown as zero percentage. 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:

<table>
<thead>
<tr>
<th>Enterprise Mode</th>
<th>Managed Service Provider (MSP) Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics:</td>
<td></td>
</tr>
<tr>
<td>• Licenses Installed</td>
<td></td>
</tr>
<tr>
<td>• License Expiration Date</td>
<td></td>
</tr>
<tr>
<td>Contact Center Assurance:</td>
<td></td>
</tr>
<tr>
<td>• Licenses Installed</td>
<td></td>
</tr>
<tr>
<td>• License Expiration Date</td>
<td></td>
</tr>
</tbody>
</table>

**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.

## 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:

**Procedure**

**Step 1** Choose **System Administration** > **License Management**.
The **License Management** page is displayed.

**Step 2** Under **License Files**, click **Add**.
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” in *Cisco Prime Collaboration Assurance Guide-Advanced*.

---

### Switch Between the Standard and Advanced Modes in Cisco Prime Collaboration

Cisco Prime Collaboration allows you to switch from the Standard mode to the Advanced mode in Cisco Prime Collaboration Assurance.  
The following table captures the different scenarios of switching:
Table 3: Switch from the Standard Mode to the Advanced Mode in Cisco Prime Collaboration Assurance

<table>
<thead>
<tr>
<th>Installation Modes</th>
<th>Standard to Advanced Evaluation</th>
<th>Standard to Advanced (Purchase license)</th>
<th>Advanced Evaluation to Advanced (Purchase license)</th>
<th>Advanced Evaluation to Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Prime Collaboration Assurance</td>
<td>Yes. (Click the Get Advanced icon at the top right corner of the User Interface and click Start Evaluation.)</td>
<td>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.)</td>
<td>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.)</td>
<td>Yes. After the evaluation expiry, you are prompted with a message to either downgrade to the standard mode or to purchase a license file for advanced mode. If you choose to downgrade, the Cluster for Standard Mode dialog box pops-up. Select a cluster from the Unified Communications Manager drop-down, device type from the Cisco Unity Connection drop-down list and click Select.</td>
</tr>
</tbody>
</table>
Manage Users

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

In Cisco Prime Collaboration, you can create users and assign roles to the users. In Cisco Prime Collaboration Assurance-Standard, a user is assigned the Super Administrator role. Cisco Prime Collaboration Assurance-Advanced supports several user roles.

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 specific customers (if you have deployed Cisco Prime Collaboration in MSP mode) or assurance domains (if you have deployed Cisco Prime Collaboration in Enterprise mode). Typically, a user with Operator role, is granted access to certain customers or assurance domains only.

For creating and managing customer groups in your network, see Manage Customers. For creating and managing assurance domains in your network, see Manage Assurance Domains.

- Cisco Prime Collaboration Assurance-Advanced User Roles, page 56
- Single Sign-On for Cisco Prime Collaboration, page 56
- Default User Accounts, page 58
- User Roles and Tasks, page 59
- Add, Edit, and Delete a User, page 59
- Modify User Roles, page 60
- Configure an LDAP Server, page 61
- LDAP Configuration Parameters, page 61
- Reset Cisco Prime Collaboration Assurance Passwords, page 63
- Change Passwords, page 64
Cisco Prime Collaboration Assurance-Advanced User Roles

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

A user can be assigned one of the following roles:

- **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 network data collection. Cannot perform any Inventory Management operations such as adding, discovering, or importing devices. Also, an operator will not be able to 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 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.

The roles selected for a user, will determine the access to data of other users. For example a user with Super Admin role can view all other users, however a user with 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 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 in ENT Mode, you can look at assurance domains belonging to another user of the same role, only if you are associated with the assurance domain(s).

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

1. Helpdesk
2. Operator

Single Sign-On for Cisco Prime Collaboration


Cisco Prime Collaboration 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:

Procedure

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.
   a) Locate the IdP metadata file from your local system and click Import IdP Metadata.
   b) Click Download Trust Metadata file.
   c) 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.
   d) 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 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 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 server while enabling SSO, it is recommended that you close the browser and re-launch the Cisco Prime Collaboration application. Because, though your session expires in Cisco Prime Collaboration server, the IdP server session might still be active.

• While enabling SSO, ensure that the hostname for Cisco Prime Collaboration 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>/ssosp/local/login.

• Disable Single Sign-On from CMD Utility.

To disable SSO from CMD utility in Cisco Prime Collaboration 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:

<table>
<thead>
<tr>
<th>Operations can be ..</th>
<th>Values can be ..</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-To get the Single Sign-On status</td>
<td>Not applicable</td>
</tr>
<tr>
<td>2-To get the recovery URL status</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
| 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

By default, the recovery URL is enabled. If you want to disable it for security reasons, set it as False.

Default User Accounts

Cisco Prime Collaboration 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 web client for the first time.

Cisco Prime Collaboration Assurance server supports the CLI user: admin.

You cannot create CLI users using the web client user interface. CLI users are created during OVA configuration. By default, the username is admin; the password is specified during OVA configuration and is used to log into the CLI to check the application status and perform backup and restore.
We recommend that you write down the root password as it cannot be retrieved.

- The users defined in the Cisco Prime Collaboration web client are different from the users defined on the Cisco Prime Collaboration server (CLI).
  - CLI users are not listed on the Cisco Prime Collaboration User Management page.
  - globaladmin and root follow same set of password validation rules, but the rules for admin are different. See the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide for password validation rules for these users.

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

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/emsam/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 Assurance tasks. See Manage Device Credentials, on page 75 to perform device management tasks using the Cisco Prime Collaboration Assurance application.

User Roles and Tasks

The User Roles and Tasks wiki page lists the Cisco Prime Collaboration Assurance user roles and tasks they are mapped to.

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

Add, Edit, and Delete a User

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

To add a user:
Procedure

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. 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  If you have deployed the Managed Service Provider (MSP) version of Cisco Prime Collaboration, select a customer from the **Customer** drop-down list. If you have deployed the Enterprise version of Cisco Prime Collaboration, you can select an Assurance Domain from the **Assurance Domain** drop-down list, however it is not mandatory.

**Note**

- In MSP mode, you must create multiple customers, and associate the customers to a user. If you create only one customer and assign it to a user, the user is added to "All My Customers" in Cisco Prime Collaboration.

- In Enterprise mode, you must create multiple Assurance domains, and associate the domains to a user. If you create only one Assurance domain and assign it to a user, the user is added to "Enterprise" in Cisco Prime Collaboration.

Step 5  Select the appropriate Cisco Prime Collaboration Assurance roles.

Step 6  Click **Save**.

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

As part of your regular system administration tasks, you sometimes must delete users from the Cisco Prime Collaboration database. However, you cannot delete the Cisco Prime Collaboration 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 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.

As part of your regular system administration tasks, you sometimes must delete users from the Cisco Prime Collaboration database. However, you cannot delete the Cisco Prime Collaboration 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 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, Edit, and Delete a User and to edit or delete a user, see Modify User Roles.

Cisco Prime Collaboration supports one primary LDAP server and one backup LDAP server. If you have deployed Cisco Prime Collaboration in MSP mode, the LDAP server configured must be a provider LDAP. This provider LDAP server has all the resellers, customers, and admin users. You can configure only one LDAP server. Multiple LDAP server configuration is not supported.

To configure LDAP server:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose System Administration &gt; LDAP Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the LDAP Settings page, enter values for all the fields. See LDAP Configuration Parameters for the field descriptions.</td>
</tr>
<tr>
<td>Note</td>
<td>If Cisco Prime Collaboration must use SSL encryption, check the Use SSL check box and specify port 636.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Test Connection to check the connectivity to the LDAP server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Upon successful connection, click Apply Settings and restart Cisco Prime Collaboration Assurance server to log in using LDAP. The application stop cpcm command takes 10 minutes to complete execution and application start cpcm takes 10 to 15 minutes to complete execution.</td>
</tr>
</tbody>
</table>

LDAP Configuration Parameters
### Table 4: LDAP Server Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP address</td>
<td>Enter the LDAP server name or IP address. Optionally enter the Backup LDAP server IP address.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Enter the Port number on which the LDAP requests for the server is received.</td>
</tr>
<tr>
<td></td>
<td>Non-secure port: 389</td>
</tr>
<tr>
<td></td>
<td>Secure SSL port: 636</td>
</tr>
<tr>
<td></td>
<td>Optionally enter the Backup LDAP server Port number.</td>
</tr>
<tr>
<td>Note</td>
<td>If the LDAP server is configured to use a non-standard port, that port should be entered here as well.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Admin Distinguished Name | Admin Distinguished Name is the distinguished name to use.  
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:  
• CN = John Doe  
• OU = Campus  
• OU = AdminBLR  
• OU = ABC  
• DC = eta  
• DC = com                                                                                                                                                                                                                                                                   |
| Admin Password      | Enter the password for the LDAP server authentication and reconfirm the password.  
**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 (#).                                                                                                           |
| LDAP User Search Base | Enter the user search base. LDAP server searches for users under this base.  
Search Base is as follows:  
• DC = eta  
• DC = com  
**Note** LDAP authentication fails if you enter special characters in the search base.                                                                                                                                          |

---

**Reset Cisco Prime Collaboration Assurance Passwords**

As a super administrator, system administrator or network operator, you can reset the password for other Cisco Prime Collaboration users.

**Prerequisite** - Root access feature is mandatory to perform this task, hence you should raise a TAC case to obtain root access.

You can reset the Cisco Prime Collaboration Assurance web client globaladmin password using the following procedure.

To reset the Cisco Prime Collaboration Assurance globaladmin password:
Procedure

Step 1  Log in as a root user.
Step 2  Execute the following:
        # cd /opt/emms/emsam/bin/
        # ./resetGlobalAdminPassword.sh
Step 3  Enter a new password for the globaladmin when prompted, and also confirm the new password, when prompted. A message notifies that the globaladmin passwords has been successfully reset.

Change Passwords

To change your own password, go to System Administration > User Management, click Reset Password, and make the necessary changes.
Manage Customers

This section applies only if you have deployed Cisco Prime Collaboration 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. 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 Automatic Discovery of Devices.

You can assign multiple customers to a user. For more information on creating a user, see Add, Edit, and Delete a User.

- Add Customers, page 65
- Global Customer Selection, page 66

Add Customers

To add a customer:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Assurance Administration &gt; Customer Management</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the Customer Management page, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the General Info page, enter the required details, and click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Devices/Device Group page, select the appropriate devices, and click <strong>Save</strong>. 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 <strong>Assign Registered Endpoints also</strong> check box. A message notifies that the devices are associated with the customer.</td>
</tr>
</tbody>
</table>
Global Customer Selection

On the Cisco Prime Collaboration 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 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 as a user associated with particular customers in Cisco Prime Collaboration, 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 as a user or globaladmin associated with all customers available in Cisco Prime Collaboration, 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 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 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.*
Manage Assurance Domains

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

Add Assurance Domains

To add an assurance domain:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Assurance Administration &gt; Domain Setup.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the Domain Setup page, click Add. You can associate device pools or devices to a domain.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Create Assurance Domain page, enter the required details, and click Save. All endpoints or subscribers registered to a publisher inherit the assurance domain name from the publisher, if the publisher has been discovered with association to a single domain.</td>
</tr>
</tbody>
</table>

Note: You cannot associate multiple domains to a device.

Click Edit to unassign an assurance 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 Assurance Domain Selection

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

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

The Cisco Prime Collaboration user interface filters and shows only the information for the selected assurance 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 10

Configure System Parameters

This section includes the following:

- Configure System Parameters, page 69
- Configure SMTP Server, page 71
- Configure Cisco Prime Collaboration Assurance Server Time Zone, page 72

Configure System Parameters

Cisco Prime Collaboration allows you to configure system parameters for Cisco Prime Collaboration Assurance. The following are the system configuration parameters for Cisco Prime Collaboration Assurance.

If you have deployed Cisco Prime Collaboration in MSP mode, the cluster (data) is displayed for a selected customer (selected from the global selection drop-down list).

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

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

- **IP Phone Inventory Collection Settings**—To configure this parameter under Device Inventory > Inventory Schedule > IP Phone Inventory Schedule, see Update and Collect Inventory Details.
• IP Phone XML Inventory Collection Settings—You can use the Phone XML Collection to schedule the phone discovery. To configure this parameter under Device Inventory > Inventory Schedule > IP Phone Inventory Schedule, see Update and Collect Inventory Details.

• Cluster Data Discovery Settings—Allows Cisco Prime Collaboration to consolidate the inventory and the device registration information it collects from Unified CM. To configure this parameter under Device Inventory > Inventory Schedule > Cluster Data Discovery Schedule, see Unified CM Cluster Data Discovery.

Global System Parameters

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

Table 5: System Parameters

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Navigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Single Sign-On.</td>
<td>System Administration &gt; Single Sign-On</td>
</tr>
<tr>
<td>Add a license file.</td>
<td>System Administration &gt; License Management</td>
</tr>
<tr>
<td>Configuring SMTP server</td>
<td>Assurance Administration &gt; E-mail Setup for Alarms &amp; Events</td>
</tr>
<tr>
<td>Configure SSL Certificate Authentication for Device Discovery.</td>
<td>System Administration &gt; Certificate Management</td>
</tr>
<tr>
<td>Configure LDAP server to access user details.</td>
<td>System Administration &gt; LDAP Settings</td>
</tr>
<tr>
<td>Change the log levels, the default value is “Error”.</td>
<td>System Administration &gt; Log Management</td>
</tr>
<tr>
<td>Configure SFTP parameters to monitor calls from Unified CM.</td>
<td>Assurance Administration &gt; CDR Source Settings &gt; CUCM SFTP Credentials</td>
</tr>
<tr>
<td>Configure parameters to collect information about the phones and clusters that are managed in Cisco Prime Collaboration Assurance inventory database.</td>
<td>Device Inventory &gt; Inventory Schedule &gt; IP Phone Inventory Schedule</td>
</tr>
<tr>
<td>Configure parameters to collect information from IP phone XML.</td>
<td>Device Inventory &gt; Inventory Schedule &gt; IP Phone Inventory Schedule</td>
</tr>
<tr>
<td>Configure parameters to consolidate the inventory and the device registration information from Unified CM.</td>
<td>Device Inventory &gt; Inventory Schedule &gt; Cluster Data Discovery Schedule</td>
</tr>
<tr>
<td>Poll parameters for Cisco TelePresence monitoring settings</td>
<td>Assurance Administration &gt; Session Path Threshold Settings</td>
</tr>
<tr>
<td>Tasks</td>
<td>Navigation</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>Add a dial plan.</td>
<td>Assurance Administration &gt; CDR Analysis Settings &gt; Dial Plan Configuration</td>
</tr>
<tr>
<td>Create a call category.</td>
<td>Assurance Administration &gt; CDR Analysis Settings &gt; Call Category Configuration</td>
</tr>
<tr>
<td>Configure parameters to poll devices.</td>
<td>Assurance Administration &gt; Polling Settings</td>
</tr>
<tr>
<td>Customize the syslog rules to monitor faults.</td>
<td>Assurance Administration &gt; Event Customization &gt; Syslog Rules</td>
</tr>
<tr>
<td>Customize the correlation rules to monitor faults.</td>
<td>Assurance Administration &gt; Event Customization &gt; Correlation Rules</td>
</tr>
<tr>
<td>Configure alarm notification (e-mail, syslog, or trap)</td>
<td>Assurance Administration &gt; Notification Setup &gt; Custom Notification</td>
</tr>
<tr>
<td>Configure threshold parameters for network devices and Medianet Configuration.</td>
<td>Assurance Administration &gt; Session Path Threshold Settings</td>
</tr>
<tr>
<td>Configure MOS parameters (poor and acceptable).</td>
<td>Administration &gt; Alarm &amp; Event Setup &gt; Threshold Settings &gt; Global Call Quality Settings</td>
</tr>
<tr>
<td>Configure MOS parameters (poor and acceptable).</td>
<td>Assurance Administration &gt; Alarm &amp; Event Setup &gt; Threshold Settings &gt; Global Call Quality Settings</td>
</tr>
<tr>
<td>Configure Voice Call Grade Settings (Good, Acceptable, Poor)</td>
<td>Assurance Administration &gt; CDR Analysis Settings &gt; Configure Voice Call Grade</td>
</tr>
<tr>
<td>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.</td>
<td>Assurance Reports &gt; Miscellaneous Reports &gt; UCM/CME Phone Activity Reports &gt; Export Audio Phones</td>
</tr>
<tr>
<td>Configure video phones report export parameters, such as video phone reports (video phone audit, move, remove video phones), file format, export file location, and notification e-mail.</td>
<td>Assurance Reports &gt; Miscellaneous Reports &gt; UCM/CME Phone Activity Reports &gt; Export Audio Phones</td>
</tr>
<tr>
<td>Schedule regular backups.</td>
<td>System Administration &gt; Backup Settings</td>
</tr>
</tbody>
</table>

**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.
Configure Cisco Prime Collaboration Assurance Server Time Zone

To configure the Cisco Prime Collaboration Assurance server time zone:

**Procedure**

**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:

`cm/admin# show timezones`

**Step 3** Enter the following commands to set the time zone for the Cisco Prime Collaboration Assurance server:

`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:

`cm/admin# write memory`

**Step 5** Enter the following command to restart the Cisco Prime Collaboration Assurance server:

`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:

`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 time zone 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, page 75
- Set Up Clusters, page 85
- Discover Devices, page 87
- Manage Device Groups, page 113
- Manage Inventory, page 119
- Poll Devices, page 159
Manage Device Credentials

You need to configure device credentials for all devices that are managed using Cisco Prime Collaboration. 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, you must create two separate credentials profiles.

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.
- CLI credentials are required to troubleshoot sessions involving endpoints and network devices.
- JTAPI credentials are mandatory for Unified CM for session 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 Unified Contact Center Enterprise (Unified CCE), and Cisco MediaSense.
- 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), and Cisco MediaSense.
• Enter HTTP credentials for Contact Center Enterprise in the following format: domain\administrator. 
  For example hcsde2\administrator.

• Enter HTTP credentials for Cisco Unified Customer Voice Portal (CVP) which have the 
  ServiceabilityAdministrationUserRole privileges. The default username wsmadmin has this privilege.

• JTAPI credentials are not required for Cisco Prime Collaboration Assurance Standard mode .

• Credentials are not required for the phones, Cisco Cius, Cisco Jabber, and Cisco Jabber Video for 
  TelePresence (Movii) 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.

---

You must review the Setting up Devices for Prime Collaboration Assurance document to understand the 
required protocols to manage devices in Cisco Prime Collaboration.

---

**Add a Device Credentials Profile**

To add or clone a credential profile:

**Procedure**

**Step 1** Choose Device Inventory > Inventory Management from the Toggle Navigation pane.
  The Inventory Management page is displayed.

**Step 2** In the Inventory Management page, click Manage Credentials.

**Step 3** In the Credentials Profile page, click Add and enter the necessary information described in the Credential 
  Profiles Field Descriptions table.

**Step 4** Click Save.
  In your network, you may have configured the same SNMP credentials for all devices, but different CLI 
  credentials. 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 database.
The following table describes the fields on the Credential Profiles page.

**Table 6: Credential Profiles Field Descriptions**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Name of the credential profiles.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>• CTS_MAN</td>
</tr>
<tr>
<td></td>
<td>• CUCM</td>
</tr>
<tr>
<td></td>
<td>• router_switches</td>
</tr>
<tr>
<td>Device Type</td>
<td>(Optional) The credential fields (such as SNMP, HTTP, CLI) are displayed,</td>
</tr>
<tr>
<td></td>
<td>based on the device type that you have selected.</td>
</tr>
<tr>
<td></td>
<td>To reduce rediscovery time, we recommend that you select the device type</td>
</tr>
<tr>
<td></td>
<td>when you create the credential profiles.</td>
</tr>
<tr>
<td></td>
<td>The default device type is &quot;Any&quot;, if you do not select a device type while</td>
</tr>
<tr>
<td></td>
<td>creating a credential profile.</td>
</tr>
<tr>
<td></td>
<td>See cisco.com for the list of device types.</td>
</tr>
<tr>
<td></td>
<td>For EX series, MX series, SX series, bare Codec devices, and all profiles</td>
</tr>
<tr>
<td></td>
<td>with Codec, select the device type as Codec.</td>
</tr>
<tr>
<td></td>
<td>For MSE devices, select Cisco MCU as the device type.</td>
</tr>
<tr>
<td></td>
<td>You can enter any credentials (SNMP, HTTP, CLI, JTAPI, MSI) to create</td>
</tr>
<tr>
<td></td>
<td>an “Any” credential profile. You must create an “Any” credential profile</td>
</tr>
<tr>
<td></td>
<td>to run auto-discovery (Ping Sweep and CDP discovery). However, you</td>
</tr>
<tr>
<td></td>
<td>can run logical discovery also.</td>
</tr>
<tr>
<td></td>
<td>If your network has multiple subnets, then create an “Any” profile for each</td>
</tr>
<tr>
<td></td>
<td>subnet.</td>
</tr>
<tr>
<td>IP Version</td>
<td>The IP address is version 4 or version 6.</td>
</tr>
</tbody>
</table>
### Field Name: IP Address Pattern

**Description:** IP address of the devices for which the credentials are provided. You must:

- Separate multiple IP addresses by the delimiter pipe (|).
- Not use 0.0.0.0 or 255.255.255.255.
- Not use question mark (?).

We recommend that you:

- Enter the exact IP address for CTS-Manager, Cisco Unified CM, and Cisco TMS.
- Enter the exact IP address for either CTS or network devices.
- Do not use many wildcard expressions in the address patterns.

For example:

- 100.5.10.*|100.5.11.*|100.5.20.*|100.5.21.*
- 200.5.1*.*|200.5.2*.*|200.5.3*.*
- 172.23.223.14
- 150.5.*.*

Avoid using patterns such as 150.*.*.*, 192.78.22.1?, 150.5.*.*/24.

If you are unable to find a common pattern for the devices, enter *.*.*.*.

Minimize the use of wildcard character (*), while defining the IP address patterns in the credential profiles **Device Inventory > Inventory management > Manage Credentials**.

Use of wildcard character may increase the discovery time.

See SNMPv2C to understand how the patterns are used.

### General SNMP Options

**SNMP Timeout** - The default is 10 seconds.

**SNMP Retries** - The default is 2.

**SNMP Version** - Selecting an SNMP version is mandatory.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| SNMPv2C         | SNMP Read Community String  
Used to discover and manage the device.  
You can provide either SNMPv2C or SNMPv3 credentials. We recommend that you use different SNMP credentials for Cisco TelePresence systems and network devices.  
Cisco Prime Collaboration searches the credential profiles, based on the IP address pattern. Cisco Prime Collaboration 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 chooses the profile that matches first.  
**Note**  
If multiple profiles have the same SNMP credentials but different CLI credentials, Cisco Prime Collaboration might choose a profile that contains the correct SNMP credentials but incorrect CLI credentials for the device. If this occurs, the troubleshooting workflow might not work. |
| SNMPv3          | SNMP Write Community String  
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. |
| CLI             | CLI Login Username and Password  
Used to access the device through CLI to discover media path for troubleshooting.  
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. |
| HTTP            | HTTP Username and Password  
Used to access the device through HTTP to poll system status and meeting information.  
Cisco Prime Collaboration first checks the access for HTTP. If the access attempt fails, then Cisco Prime Collaboration checks the access for HTTPS.  
If you log in to Cisco TMS using the <domain/username> format, then ensure that you add the same <domain/username> value in the HTTPS Username field. |
| JTAPI           | (Optional) JTAPI Username and Password.  
**Note**  
Password must not contain a semicolon (;) or equals (=).  
Used to retrieve the session status information from the Cisco Unified CM. |
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| MSI        | MSI Username and Password  
The MSI credentials are used during the troubleshooting workflow, to troubleshoot MSI enabled endpoints.  
MSI credentials remain the same as http credentials for TC 6.0 and TE 6.0 software versions. For TX 6.0 version, the default MSI username is msiuser and the password is cisco. |

SSL Certificate Authentication for Device Discovery

In Cisco Prime Collaboration, 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 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 trust-store to access the device.

Cisco Prime Collaboration 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.

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

To enable the SSL certificate authentication:

**Procedure**

The Certificate Management page is displayed.
2. In the Device Certificate Management tab, check the Enable SSL certificate authentication for device discovery check box.
3. Click the Import Certificates button.
4. Restart the Cisco Prime Collaboration 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 application, you must modify the relevant credential profiles in the Cisco Prime Collaboration database.
If the credentials are incorrect, a major event—Device is inaccessible—is triggered from Cisco Prime Collaboration (Monitor > Alarms & Events > Events).

To edit a credential profile:

**Procedure**

1. **Step 1** Choose Device Inventory > Inventory Management.
2. **Step 2** From the Inventory Management page, select a device and click Modify Credentials.
3. **Step 3** Update the credentials and click Rediscover.
   - Cisco Prime Collaboration 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 uses the updated credentials in the next polling job.

---

### Verify Device Credentials

If device discovery fails because of incorrect credentials, you can test the credentials for the failed devices and rediscover those devices. Choose Device 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:

**Procedure**

1. **Step 1** Choose Device Inventory > Inventory Management. The Inventory Management page is displayed.
2. **Step 2** In the Inventory Management page, choose Manage Credentials. The Manage Credential page is displayed.
3. **Step 3** From the Credential Profiles page, select the profile name to use for testing the credentials, and click Verify.
4. **Step 4** 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.
5. **Step 5** 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.

**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 database in the current Inventory table. To know more about the inventory table, see the View Inventory Details section in the Cisco Prime Collaboration Assurance Guide Advanced.
Credential Verification Error Messages

The credential verification error messages are tabulated below.

Table 7: Credential Verification Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Conditions</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMPv2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Request: Received no response</td>
<td>Failed for one of the following reasons:</td>
<td>• Verify the device connectivity.</td>
</tr>
<tr>
<td>from IP Address.</td>
<td>• Device response time is slow.</td>
<td>• Update the credential profile with the correct community strings.</td>
</tr>
<tr>
<td></td>
<td>• Device is unreachable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Incorrect community string entered in the credential profile.</td>
<td></td>
</tr>
<tr>
<td><strong>SNMP timeout.</strong></td>
<td>Either the device response time is slow or the device is unreachable.</td>
<td>• Verify the device connectivity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Increase the SNMP Timeout and Retries values in the credential profile.</td>
</tr>
<tr>
<td>Failed to fetch table due to:</td>
<td>Either the device response time is slow or the device is unreachable.</td>
<td>Increase the SNMP Timeout and Retries values in the credential profile.</td>
</tr>
<tr>
<td>Request timed out.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SNMPv3</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The configured SNMPv3 security level</td>
<td>Device does not support the configured SNMPv3 security level.</td>
<td>Change the SNMPv3 security level to the supported security level in the credential</td>
</tr>
<tr>
<td>is not supported on the device.</td>
<td></td>
<td>profile.</td>
</tr>
<tr>
<td>The SNMPv3 response was not received</td>
<td>Either the device response time is slow or the device is unreachable.</td>
<td>Verify the device connectivity.</td>
</tr>
<tr>
<td>within the stipulated time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMPv3 Engine ID is wrong.</td>
<td>Incorrect engine ID entered in the credential profile.</td>
<td>Enter the correct SNMPv3 engine ID in the credential profile.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Conditions</td>
<td>Possible Solutions</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMPv3 message digest is wrong.</td>
<td>Failed for one of the following reasons:</td>
<td>• Verify that the correct SNMPv3 authentication algorithm and device password are set in the credential profile.</td>
</tr>
<tr>
<td></td>
<td>• Either the SNMPv3 authentication algorithm or the device password is incorrect.</td>
<td>• Check for network errors.</td>
</tr>
<tr>
<td></td>
<td>• Network password.</td>
<td></td>
</tr>
<tr>
<td>SNMPv3 message decryption error.</td>
<td>Cannot decrypt the SNMPv3 message.</td>
<td>• Verify that the correct SNMPv3 authentication algorithm is entered in the credential profile.</td>
</tr>
<tr>
<td>Unknown SNMPv3 Context.</td>
<td>The configured SNMPv3 context in the credential profile does not exist on the device.</td>
<td>• Verify that the configured SNMPv3 context is correct in the credential profile.</td>
</tr>
<tr>
<td>Unknown SNMPv3 security name.</td>
<td>Either the SNMPv3 username is incorrect in the credential profile or the SNMPv3 username is not configured on the device.</td>
<td>• Verify that the correct SNMPv3 username is set in the credential profile and on the device.</td>
</tr>
<tr>
<td>CLI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login authentication failed.</td>
<td>Incorrect credentials entered in the credential profile.</td>
<td>• Verify and reenter the device CLI credentials in the credential profile.</td>
</tr>
<tr>
<td>Connection refused.</td>
<td>Either SSH or Telnet service may not be running on the device.</td>
<td>1 Verify the device connectivity for the supported CLI (port).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Verify whether the SSH or Telnet service is running on the device.</td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server returned HTTP response code: 401 for URL.</td>
<td>Either the HTTP service is not running or the URL is invalid.</td>
<td>• Verify whether the HTTP or HTTPS service is running on the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Verify whether the URL is valid on the server.</td>
</tr>
<tr>
<td>Connection refused.</td>
<td>The HTTP or HTTPS service is not running.</td>
<td>• Verify whether the HTTP or HTTPS service is running on the device.</td>
</tr>
<tr>
<td>HTTP check failed.</td>
<td>Incorrect HTTP credentials entered in the credential profile.</td>
<td>• Verify and reenter the device HTTP credentials in the credential profile.</td>
</tr>
</tbody>
</table>
## 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 application.

To delete a credential profile:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Device Inventory &gt; Inventory Management.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Inventory Management page, click Manage Credentials. By default, the credentials for a device that appears first on the list are displayed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select the profile name and click Delete.</td>
</tr>
</tbody>
</table>
Set Up Clusters

Cisco Prime Collaboration manages the following clusters:

- Cisco TelePresence Manager
- Cisco TMS
- Cisco VCS
- Cisco Unified CM
- Cisco TelePresence Exchange - MSP mode only

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

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

For CTS-Manager, or TMS clusters, the session details are imported from the primary CTS-Manager, or Cisco TMS as defined on the Manage Clusters page.

If you have deployed Cisco Prime Collaboration in MSP mode, you can manage a CTX cluster also. Cisco Prime Collaboration 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 or Cisco TelePresence Exchange (CTX) clusters, page 85

Manage Cisco TelePresence Manager or Cisco TMS or Cisco TelePresence Exchange (CTX) clusters

Before discovering Cisco TelePresence Manager, Cisco TMS, or Cisco TelePresence Exchange (CTX) 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 uses the cluster details, along with the device credentials (Device Inventory > Inventory Management > Manage Credentials) and discovers the management applications.
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 wiki](#).

To manage Cisco TelePresence Manager, Cisco TMS or Cisco TelePresence Exchange (CTX) clusters:

**Procedure**

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

**Step 2** From the Inventory Management page, click Manage CTS-MAN/TMS Cluster.
If you have deployed Cisco Prime Collaboration in MSP mode, click Manage CTS-MAN/TMS Cluster.

**Step 3** In the Manage Clusters window, enter the cluster name and choose an item from the cluster type drop-down list.

**Step 4** For a CTS-MAN cluster: Enter the IP addresses of the primary, secondary, hot standby, and the load-balancer servers. (The Primary Server IP address and hot standby or secondary are mandatory; only load-balancer server is optional.)
For a TMS cluster: Enter the IP address of the primary active server, and the secondary active or passive server.
For a CTX cluster: Enter the IP address of the primary and secondary admin server.

**Step 5** A new cluster is added when you click Add.
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.
CTX clusters (for MSP deployment mode only): You must enter both the primary and secondary admin server IP addresses.
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 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 75 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 75 for information on required device credentials.

- Inventory discovery—Cisco Prime Collaboration polls MIB-II and other device MIBs to collect information on the device inventory, neighboring switches, and default gateway. It also verifies whether the polled device is supported in Cisco Prime Collaboration.

- Path trace discovery—Cisco Prime Collaboration 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 database.
Cisco Prime Collaboration 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 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**

![Device Discovery Lifecycle Diagram]

Cisco Prime Collaboration displays the following device states:

**Table 8: Discovery States**

<table>
<thead>
<tr>
<th>Discovery States</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>This is the preliminary state, when the device is first added. This is a transient state.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Cisco Prime Collaboration is unable to ping the device using ICMP. If ICMP is not enabled on the device, the device is moved to the Unreachable state.</td>
</tr>
<tr>
<td>Unsupported</td>
<td>Cisco Prime Collaboration 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. For a list of devices supported by Cisco Prime Collaboration 11.0, see <a href="#">Supported Devices for Prime Collaboration Assurance</a>.</td>
</tr>
<tr>
<td>Accessible</td>
<td>Cisco Prime Collaboration 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.</td>
</tr>
<tr>
<td>Discovery States</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inaccessible</td>
<td>Cisco Prime Collaboration is not able to access the device through any of the mandated credentials (see Add a Device Credentials Profile). You must check the credentials and discover the devices.</td>
</tr>
<tr>
<td>Deleted</td>
<td>The device is hidden from the Inventory Management. However, the device is in the Cisco Prime Collaboration database and can be discovered.</td>
</tr>
<tr>
<td>Inventory Collected</td>
<td>Cisco Prime Collaboration 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.</td>
</tr>
<tr>
<td>Undiscoverable</td>
<td>Cisco Prime Collaboration is not able to collect the required data using the mandated data collectors. The device state can be undiscoverable when:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Prime Collaboration collects the endpoint data from CTS-Manager. If data is not collected, CTS-Manager is moved to Undiscovered state. There is no mandated data collection for Cisco Unified CM, CTS, CTMS, and other network devices.</td>
</tr>
<tr>
<td></td>
<td>• 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 faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery.</td>
</tr>
<tr>
<td>Managed</td>
<td>Cisco Prime Collaboration has successfully imported the required device data to the inventory database. All session, endpoints, and inventory data are available for devices in this state.</td>
</tr>
<tr>
<td></td>
<td>You can troubleshoot a device only if it is in this state.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Cisco Prime Collaboration supports third-party devices whose manageability depends on MIB-II support.</td>
</tr>
<tr>
<td></td>
<td>If the Cisco Prime Collaboration inventory exceeds your device limit, you will see a warning message. For information on how many devices Cisco Prime Collaboration can manage, see the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide.</td>
</tr>
<tr>
<td>Suspended</td>
<td>User has suspended monitoring of the device. Session and endpoint data are not displayed for devices in this state. Periodic polling is also not performed for devices in this state. To do so, you will need to perform Resume Management. See Suspend and Resume Managed Devices for details on suspended devices.</td>
</tr>
</tbody>
</table>
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.

Discovery Methods

Choose one of the following discovery methods to manage devices in Cisco Prime Collaboration Assurance:
<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Discovery Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto discovery | Logical Discovery | - Discovers management applications, conferencing devices, and call processors such as CTS-Manager, Cisco TMS, Cisco VCS, and Cisco Unified CM.  
- All endpoints and infrastructure devices registered with CTS-Manager, Cisco TMS, Cisco Unified CM, and Cisco VCS are discovered automatically during logical discovery.  
  - Logical discovery of CTS-Manager discovers Cisco TMS, Cisco Unified CM, CTS, Cisco Cius, IP phones, routers, and switches.  
  - Logical discovery of CTS-Manager discovers the first-hop router and switch for Cisco 500, 1000 and 3000 series TelePresence systems.  
  - For Cisco C and Ex series TelePresence systems, Cisco Prime Collaboration 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 PCA. 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. |
**Discovery Type** | **Discovery Method** | **Description**
--- | --- | ---
Auto discovery | CDP | • 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.

Auto discovery | Ping Sweep | • 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.
**Discover Devices**

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Discovery Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| -              | Add Devices      | • 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           | Use this option to add:  
                 |                  | • 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.

**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 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 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.

- CDP must be enabled on all CTS endpoints, 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 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 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 CTS-Manager, 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 109 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 only during the inventory collection process. Therefore, any changes to a device’s configuration will not be shown by Cisco Prime Collaboration until the next inventory collection after the configuration change.

- To periodically update inventory, and synchronize the inventory with the Cisco Prime Collaboration database, you must perform inventory update. For more information, see Update and Collect Inventory Details.
Cisco Unified CM

- Cisco Prime Collaboration 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 server IP address.

- Cisco Prime Collaboration 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 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, so that the configured ELM or PLM gets discovered and managed when a Unified Communications Manager publisher is added to Cisco Prime Collaboration using auto discovery User Interface.

- 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 rediscover Unified CM Publisher node to add them to Cisco Prime Collaboration. See Rediscover Devices, on page 109 for information on rediscovering devices.

Note

We recommend that you should not add a subscribe node manually.
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 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 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>
session protocol sipv2
session 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 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 session 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 detects the IP address change automatically.

- If the Cisco VCS Expressway is configured within the DMZ, Cisco Prime Collaboration 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 for Cisco Prime Collaboration Assurance 11.0, see the Setting up Devices for Prime Collaboration Assurance 11.0 wiki page.

CTS-Manager

- If you have installed a licensed version of Cisco Prime Collaboration, it is mandatory to configure the CTS-Manager Reporting API. If this feature is not configured on the CTS-Manager 1.7, 1.8, or 1.9, Cisco Prime Collaboration will not manage the CTS-Manager. See Cisco TelePresence Manager Reporting API Developer's Guide for more information.

- Cisco Prime Collaboration 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 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.

CTX Cluster

- Cisco Prime Collaboration 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 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. See the Setting Up Devices for Prime Collaboration Assurance wiki page for more information.

- Before performing the discovery, enter the IP address of the primary and secondary admin server details in Device Inventory > Inventory Management > Manage CTS-MAN/TMS Cluster.
Cisco TelePresence Conductor

Cisco Prime Collaboration 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 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. 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.

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


- 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 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, see the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page for Cisco Prime Collaboration Assurance 11.0
Cisco SocialMiner
You must configure SNMP. For more information, see the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page for Cisco Prime Collaboration Assurance 11.0.

Cisco Finesse
You must configure SNMP. See the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page for Cisco Prime Collaboration Assurance 11.0,

Cisco Integrated Management Controller (CIMC)

- Cisco Prime Collaboration 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.

- You must configure the SNMP. For more information on setting up devices for Cisco Prime Collaboration Assurance 11.0, see the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page and for Cisco Prime Collaboration Assurance 11.5, see Configure Devices for Prime Collaboration Assurance 11.5.

- The CIMC device will be in managed state only when you enter the correct IP address and SNMP credentials.

### Automatic Discovery of Devices

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

- 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 may not be able to automatically discover this endpoint. This is applicable to all Cisco TelePresence systems registered with Cisco Unified CM.

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.

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.
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 CTS-Manager, or Cisco TMS and CTX clusters, you need to enter specific application details.

**Procedure**

**Step 1** 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.

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

- 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 Ping Sweep 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 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 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.

**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** Schedule a periodic discovery job (see Discovery Filters and Scheduling Options for field descriptions) or run the discovery job immediately by following Automatic Discovery of Devices.

**Step 8** 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, click Job Progress in the message confirmation window to verify discovery status. See Verify Discovery Status for more information.

**Discovery Filters and Scheduling Options**

**Discovery Filters**

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

**Table 9: Discovery Filters**

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• To include all devices in the 172.20.57/24 subnet, enter an include filter of 172.20.57.*.</td>
</tr>
<tr>
<td></td>
<td>• 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].</td>
</tr>
<tr>
<td></td>
<td>You can use both wildcard types in the same range; for example, 172.20.[55-57].<em>.</em>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Advanced Filters</td>
<td></td>
</tr>
<tr>
<td>DNS Domain</td>
<td>Comma-separated DNS domain names for included or excluded devices. An asterisk (*) wildcard matches, up to an arbitrary length, any combination of alphanumeric characters, hyphen (-), and underscore (<em>). A question mark (?) wildcard matches a single alphanumeric character, hyphen (-), or underscore (</em>). 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.</td>
</tr>
</tbody>
</table>
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.

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.

A question mark (?) wildcard matches a single alphanumeric character, hyphen (-), underscore (_), or white space (space or tab).

**Schedule Options**

The following table describes the scheduling options that are available.

**Table 10: Schedule Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Click Start Time to enter the start date and time in the yyyy/MM/dd and hh:mm AM/PM formats, respectively. 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.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Click None, Hourly, Daily, Weekly, or Monthly to specify the job period.</td>
</tr>
<tr>
<td>Settings</td>
<td>Specify the details of the job period.</td>
</tr>
<tr>
<td>End Time</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Manual Discovery of Devices**

You can add single or multiple devices to Cisco Prime Collaboration 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.

**Procedure**

**Step 1** Choose **Device 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 Assurance 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 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. See **Verify Discovery Status** for more information.

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.

---

**Import Devices**

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

If you have deployed Cisco Prime Collaboration 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 devices 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 host name of the devices.

If you have deployed Cisco Prime Collaboration in MSP mode, you must provide Host Name 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.

**Procedure**

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

**Step 2** Click **Import**.

**Step 3** In the Import dialog box, browse to the file with the list of devices and credentials that you want to import. (Only 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 rediscovery of the seed device to get the complete registration and association details.

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 in 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 Assurance Inventory 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:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Device Inventory &gt; Inventory Management &gt; Export.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Device list and Credentials, and enter a name for the output file. (Only CSV and XML file format is supported.)</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Export. This file contains encrypted credentials only.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the dialog box that appears, do one of the following:</td>
</tr>
</tbody>
</table>

- 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.

Discovery of Cisco Unified Computing System (UCS)

**Prerequisites**

- 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.
- VMware Tools must be installed on the VMs before performing the discovery. This ensures the tools are discovered during the VMware ESX server discovery.
- Check the Event and Alarm correlation rules with UCS blades by configuring vCenter as follows:

  1. **Configure SNMP on vCenter**: Log in to vCenter by using vSphere and navigate to Administration > vCenter Server Settings. Select SNMP menu on the left of the page to configure the SNMP settings.

  2. **Configure the triggers and alarms on vCenter**:

     1. Select a virtual machine and navigate to Alarms > Definition. Click the vCenter name and select the alarm to configure the settings.

     2. 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 Prime Collaboration Assurance. Select the state as ”Alert” and click OK. Click Actions and then select Repeat for all the following cases: “Normal->Warning”, “Warning->Error”, “Error->Warning”, and “Warning->Normal”. Click OK.
• 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. For more information about the fields and their configuration options, see Cisco UCS Manager GUI Configuration Guide.

• Ensure that the vCenter, ESX, and UCS Manager devices are added to Cisco Prime Collaboration Assurance:

1. Login to Cisco Prime Collaboration Assurance server and navigate to Device Inventory > Inventory Management.
2. Click the Manage Credentials button to create credential profiles for the following:
   • VMware ESX Server (ESX):
     • The HTTP credentials for the VMware ESX Server credential profile must be the same as the VMware ESX Server device login credentials.
     • Configure SNMP credentials on the VMware ESX Server. See the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page for Cisco Prime Collaboration Assurance 11.0
   • Cisco UCS Manager (UCS Manager):
     • 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.
   • VMware vCenter Server (vCenter): The HTTP credentials for the vCenter credential profile must be the same as the vCenter device admin login credentials.

Note: The Virtual Machines are supported both in a NAT and non-NAT deployment.

• Perform logical discovery of the following:

1. ESX Logical Discovery - Use the ESX Server IP address as the seed device to discover all the VMs running on it.
2. 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.
3. 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.

To discover the Cisco UCS and associated Virtual Machine(s) in a non-NAT deployment, perform the following tasks:
• Choose **Device Inventory > Inventory Management > Auto Discovery**, and then select Logical Discovery in the Discovery Methods 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.

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

• (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.

To discover Cisco UCS in a NAT deployment, you must use the Add Device or Import feature to discover the vCenter, ESX or UCS Manager individually. Ensure that you use the Rediscover feature, and select the **Enable Logical Discovery** check box to get the association between ESX and VM/UC applications.

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.

---

**Unified CM Cluster Data Discovery**

After the Unified CM publisher is managed in Cisco Prime Collaboration, 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 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.

**Schedule Cluster Data 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 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 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.
Procedure

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

Rediscover Devices

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

Perform rediscovery when:

- A deleted device must be 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.

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. (For Cisco Prime Collaboration Release 10.6) Now, rediscover (Operate > Device Work Center) 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.

Rediscover Deleted Devices

To rediscover deleted devices:

Procedure

Step 1 Choose Device Inventory > Inventory Management.
Step 2 From the Inventory Management page, choose the Deleted quick filter to get a list of devices that are in the Deleted state in the Current Inventory table.
Step 3 Select the devices you want to rediscover. Click Rediscover. If you want to perform logical discovery (discovery of all registered devices) select the Enable Logical Discovery check box, else deselected it.
Step 4 In the confirmation message box that appears, click OK.
Step 5 From the Inventory Management page, click the Discovery Jobs button to check the progress and the status of the job in the Job Management page. For more information, see Verify Discovery Status.

Note Deleted endpoints are not discovered as part of Unified CM, Cisco VCS, and CTS-MAN seed device discovery.

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:

Procedure

Step 1 Choose Device 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, do one or more of the following:

  • For any devices that were not discovered because of incorrect credentials, verify the credentials for those devices (see Verify Discovery Status, on page 110), and run the discovery again.

  • For CTS-Manager discovery failure with the error UNDISCOVERABLE Exception:: null, perform the discovery again. (This issue occurs if multiple users are accessing CTS-Manager at the same time.)

  • 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.

   **Note**: Logical Discovery is not supported in MSP mode.

   Rediscover the TMS with selection of the Enable Logical discovery option. Ensure that the credentials are added for all the associated devices.

3 **Issue**: DX80/Phones are not discovered successfully.

   **Recommended Action**: DX 80 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 inventory only after the Cluster Data Discovery.

   You should not discover the DX 80 device separately by adding DX IP address.

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

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

5 **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. See the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page for Cisco Prime Collaboration Assurance 11.0

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

**Recommended Action:** The endpoint name of an endpoint belonging to a cluster is updated only after performing the Cluster Data Discovery.

**7 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 in the **Inventory Management** page.

- Verify that the service is running by typing the following URL on a browser:
  

**8 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 in the **Inventory Management** page.

- Verify that the service is running by typing the following URL in a browser:
  
Manage Device Groups

- About Device Groups, page 113
- Create Groups, page 116
- Add Devices to a Group, page 116
- Remove Devices from a Group, page 117
- Device Group Selector, page 117

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 Device Inventory, Session 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, and to monitor sessions, endpoints, alarms, and events. 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 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
- Sessions on the Session 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 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 11: Quick View Details for User-Defined Groups

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the device.</td>
</tr>
<tr>
<td>Group Type</td>
<td>Displays the group type: Dynamic or static.</td>
</tr>
<tr>
<td>Number of Members</td>
<td>Displays the total number of members in the group.</td>
</tr>
<tr>
<td>Number of SubGroups</td>
<td>Displays the number of subgroups (children) in the group. You can add any</td>
</tr>
<tr>
<td></td>
<td>number of subgroups to a group.</td>
</tr>
<tr>
<td>Number of Rules</td>
<td>Displays the number of rules set for the group.</td>
</tr>
<tr>
<td>Note</td>
<td>To know the details of the rules, hover the mouse over Number of Rules and</td>
</tr>
<tr>
<td></td>
<td>click on the quick view icon.</td>
</tr>
</tbody>
</table>

#### Add SubGroup

1. Click Add SubGroup.
2. In the Create SubGroup window, enter details for the sub group.
3. Click Save.

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.

For dynamic groups, when you create a dynamic subgroup, it automatically inherits the parent group rule.

#### Edit Group

1. Click Edit Group.
2. In the Edit Group window, edit the required fields.
3. Click Save.

You can edit the group name and description, and select a parent group.

#### Delete Group

1. Click Delete Group.
2. In the confirmation message box, click OK.
Create Groups

To create a group:

Procedure

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:

Procedure

Step 1 Choose Device 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:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Device Inventory &gt; Inventory Management.</td>
</tr>
<tr>
<td>2</td>
<td>From the Inventory Management page, select the managed devices from the Current Inventory table.</td>
</tr>
<tr>
<td>3</td>
<td>Click the right arrow on the Current Inventory pane.</td>
</tr>
<tr>
<td>4</td>
<td>Select Remove From Group.</td>
</tr>
<tr>
<td>5</td>
<td>From the confirmation message box, click OK.</td>
</tr>
</tbody>
</table>

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.
Device Group Selector
Manage Inventory

- View Inventory Details, page 119
- Device-Specific Inventory Details, page 130
- Update and Collect Inventory Details, page 143
- Suspend and Resume Managed Devices, page 148
- Delete Devices, page 149
- Performance Graphs, page 149
- Perform Device Search, page 155
- SNMP Query, page 156

View Inventory Details

Cisco Prime Collaboration performs continuous, real-time discovery of device 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 database. The Cisco Prime Collaboration inventory reflects every addition, deletion, and modification that occurs in the network after update.

In Cisco Prime Collaboration, devices are grouped based on the device type. The Device Group pane is available in the Inventory Management, Session 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, and to monitor sessions, endpoints, alarms, and events.

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.

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 Device Inventory page.

Each device that is managed by Cisco Prime Collaboration 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.

You can change the visibility settings of the devices by using the Edit option. This is enabled only for endpoints, predefined groups and user-defined groups. The visibility settings of the device can be changed only if the device is in the Managed state. Any change in visibility settings appear in the Session Diagnostics page. For more information, see Session Diagnostics Dashboard, on page 222.

If you have deployed Cisco Prime Collaboration 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.

You can edit the Jitter, Average Period Latency, and Rx Packet Loss threshold settings of all devices except infrastructure devices using the Threshold Settings option.

---

**Note**

You can add decimal values also. You can set the value of Rx Packet Loss to as low as 0.1.

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.

There are options such as Quick Filters, Advanced Filters to filter devices based on the device criteria. See Manage Device Groups.

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.
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 12: Field Descriptions for the Current Inventory Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Name</td>
<td>Name assigned to the endpoint for ease of identification.</td>
</tr>
<tr>
<td>Extension</td>
<td>Directory Number of endpoints. This number helps to identify a device uniquely.</td>
</tr>
<tr>
<td>Phone Description</td>
<td>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).</td>
</tr>
<tr>
<td>Host Name</td>
<td>Name assigned to the device for ease of identification.</td>
</tr>
<tr>
<td>Model</td>
<td>Device model, such as Catalyst3506G48PS.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used for managing the device. Click on the IP address to log into the device. Click on the quick view icon to launch the Device 360 Degree View for that device. If that device is an endpoint the Endpoint 360 Degree View appears. If these devices are discovered by logical discovery then the IP Address and Private IP address will be same. For routers and switches, you must associate a terminal client application, such as Putty, to log into the device.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>MAC Address of the devices.</td>
</tr>
<tr>
<td>NAT Status</td>
<td>If you have deployed Cisco Prime Collaboration in MSP mode, you will see if NAT is enabled or disabled.</td>
</tr>
<tr>
<td>Private IP Address</td>
<td>If you have deployed Cisco Prime Collaboration in MSP mode in a NAT environment, you will see the Private IP address of the device. The Private IP address is populated using the Add Device or Import feature.</td>
</tr>
<tr>
<td>Private Host Name</td>
<td>If you have deployed Cisco Prime Collaboration in MSP mode in a NAT environment, you will see the host name of the device.</td>
</tr>
<tr>
<td>Customer</td>
<td>If you have deployed Cisco Prime Collaboration in MSP mode, you can see the customer to which the device belongs to.</td>
</tr>
<tr>
<td>Software Type</td>
<td>Software running on the device, such as IOS, CatOS.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Software version running on the device.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Only for CUCM registered devices.</td>
</tr>
<tr>
<td>Partition</td>
<td>Only for CUCM registered endpoints.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Applicable only for endpoints.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the device.</td>
</tr>
<tr>
<td>Status Reason</td>
<td>Reason for the device status.</td>
</tr>
<tr>
<td>Type</td>
<td>The most applicable role or service of the device.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>All other roles or services of the device.</td>
</tr>
<tr>
<td>Last Discovered</td>
<td>Date and time when the device was last discovered. The time will be according to the time zone set in the Cisco Prime Collaboration server.</td>
</tr>
<tr>
<td>Visibility</td>
<td>• Not Applicable—Realtime visibility is not supported for this device.</td>
</tr>
<tr>
<td></td>
<td>• Limited or Full visibility—Displayed only for endpoints, based on the visibility settings.</td>
</tr>
<tr>
<td>Customized Events</td>
<td>• Green check mark displayed—Event settings are customized for the device using Customize Events tab.</td>
</tr>
<tr>
<td></td>
<td>• Green check mark not displayed—Event settings are not customized for the device. The device uses global settings.</td>
</tr>
<tr>
<td>Mediatrace Role</td>
<td>• Unsupported—Device does not support Cisco Mediatrace.</td>
</tr>
<tr>
<td></td>
<td>• Transparent—Device supports Cisco Mediatrace but profile is not configured.</td>
</tr>
<tr>
<td></td>
<td>• Responder—Cisco Mediatrace responder profile is enabled on the device. Enable this profile if you want to monitor and collect information on Cisco Mediatrace.</td>
</tr>
<tr>
<td></td>
<td>• Initiator—Cisco Mediatrace initiator profile is enabled on the device. Enable this profile if you want to initiate Cisco Mediatrace session or polls.</td>
</tr>
<tr>
<td></td>
<td>• Initiator/Responder—Cisco Mediatrace initiator and responder profiles are enabled on the device.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IP SLA Role           | • 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. |
| Performance Monitor   | • 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. For more information on Cluster Data Discovery, see [Unified CM Cluster Data Discovery](#), on page 107.

• 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'.
  * Restart Cisco Prime Collaboration Assurance Server by logging in as admin user and execute the following commands:
    * `application stop cpcm`
    * `application start cpcm`
  * 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 the IP Address is shown as NA.
Device 360° View is available for MRA clients.

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 13: Field/Buttons and their Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>You can hover on the State icon to know the state of the device. Different colors of the icon represent different states.</td>
</tr>
<tr>
<td>Status Reason</td>
<td>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.</td>
</tr>
<tr>
<td>Host Name</td>
<td>—</td>
</tr>
<tr>
<td>Host IP /Global IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Descriptions</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>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.</td>
</tr>
<tr>
<td>Host Name</td>
<td>If you have deployed Cisco Prime Collaboration in MSP mode in a NAT environment, you will see the hostname of the device.</td>
</tr>
<tr>
<td>Customer</td>
<td>If you have deployed Cisco Prime Collaboration in MSP mode, you can see the customer to which the device belongs to.</td>
</tr>
<tr>
<td>Version</td>
<td>Software version of the device.</td>
</tr>
<tr>
<td>Last discovered</td>
<td>Time stamp of last successful discovery.</td>
</tr>
<tr>
<td>Cluster ID</td>
<td>Cluster ID of the cluster the device belongs to. You can click on the cluster ID to launch the Cluster Details page.</td>
</tr>
</tbody>
</table>

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. You can go to the support pages of other devices, and also visit the support community page of Cisco Prime Collaboration. To visit the Cisco Prime Collaboration 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**. 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.

For business impacting technical issues, we recommend that you open a service request with Cisco TAC for timely support.

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).

Click the tasks icon, and select from the drop-down list to perform multiple tasks such as launching performance graphs and managing thresholds.

**Note** The options available depend on the device you have selected.
Other device-specific information is as follows:

**Table 14: Device 360° View - Tabs Description**

<table>
<thead>
<tr>
<th>Tabs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>It includes the following:</td>
</tr>
<tr>
<td></td>
<td>• Severity—Severity of the alarm</td>
</tr>
<tr>
<td></td>
<td>• Status—Status of the alarm</td>
</tr>
<tr>
<td></td>
<td>• Name—Name of the device</td>
</tr>
<tr>
<td></td>
<td>• Component—Name of the component that has alarms</td>
</tr>
<tr>
<td></td>
<td>• Last Updated—Time stamp of the last alarm generation.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Operation Status—Operational state of the device</td>
</tr>
<tr>
<td></td>
<td>• Admin Status—Administrative status of the interface</td>
</tr>
<tr>
<td></td>
<td>• Name—Description of the device</td>
</tr>
<tr>
<td></td>
<td>• Address—Physical address of the device</td>
</tr>
<tr>
<td></td>
<td>• Type—Device type</td>
</tr>
<tr>
<td>Card/Services</td>
<td>It includes the following:</td>
</tr>
<tr>
<td></td>
<td>• Name—Description of the voice/service</td>
</tr>
<tr>
<td></td>
<td>• Version—Version of the card/service</td>
</tr>
<tr>
<td></td>
<td>• Status—Status of the card/service</td>
</tr>
<tr>
<td>Port</td>
<td>—</td>
</tr>
<tr>
<td>Environment</td>
<td>It includes:</td>
</tr>
<tr>
<td></td>
<td>• Power supply</td>
</tr>
<tr>
<td></td>
<td>• Fan</td>
</tr>
<tr>
<td></td>
<td>• Temperature sensor</td>
</tr>
<tr>
<td></td>
<td>• Voltage sensor</td>
</tr>
<tr>
<td>Device-specific details</td>
<td>—</td>
</tr>
</tbody>
</table>
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 device.

Choose **Device 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.

You can view the status of the CVP VXML server and its associated application; launch the Device 360 view, and click the VXML Server tab. The applications that are running on the VXML server are displayed in this tab. The status of the application is also appropriately displayed. For example, if an application is not running, an alarm is generated in the Alarms & Events page and the corresponding status is displayed in the Status column.

---

**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](#), on page 280.

### 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 poling 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**

The following table describes the Global Search options for Cisco Prime Collaboration Assurance.
## Table 15: Global Search Options for Cisco Prime Collaboration Assurance

<table>
<thead>
<tr>
<th>Search</th>
<th>Variable</th>
<th>Sample String Format</th>
<th>Exceptions and Allowed Search Strings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>DN</td>
<td>10002[1000*]</td>
<td>100*</td>
</tr>
<tr>
<td></td>
<td>IP</td>
<td>10.64.101.162</td>
<td>10.64.101.*</td>
</tr>
<tr>
<td></td>
<td>MAC</td>
<td>00260bd75cf8</td>
<td>00260bd75cf*</td>
</tr>
<tr>
<td>Phone Description</td>
<td>San Jose</td>
<td>-</td>
<td>If the domain name is not resolvable, the IP address is displayed in the search results.</td>
</tr>
<tr>
<td>Device</td>
<td>IP</td>
<td>10.78.22.129</td>
<td>10.78.22.*</td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>cussmtest15.cisco.com</td>
<td>If the domain name is not resolvable, the IP address is displayed in the search results.</td>
</tr>
<tr>
<td>Location</td>
<td>Name</td>
<td>US-Texas</td>
<td>US*</td>
</tr>
<tr>
<td>TelePresence</td>
<td>IP</td>
<td>10.78.22.77</td>
<td>10.78.22.*</td>
</tr>
<tr>
<td>User</td>
<td>First Name or Last Name</td>
<td>HS John</td>
<td>Alphanumeric characters, dash, underscore and blank space are not allowed.</td>
</tr>
</tbody>
</table>

### Search Results

<table>
<thead>
<tr>
<th>Search Parameter</th>
<th>Search Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>TelePresence</td>
<td>Host Name, Device Type, Model, Software Type, Software Version, and State. You can click on the icon next to the device name to launch the Endpoint 360 View for that Cisco TelePresence endpoint.</td>
</tr>
<tr>
<td>Phone</td>
<td>IP Address, IPv6 Address, MAC Address, Load ID, Description, and Model. You can click on the icon next to the device name to launch the Endpoint 360 View for that phone.</td>
</tr>
</tbody>
</table>
Device | Name, IP Address, Status, and Device Type. When you perform a device search, all phones and Cisco TelePresence endpoints are also included in this 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.

Location | Cluster ID, Call Failure Troubleshooting, and Call Quality Troubleshooting. You can click [Call Failure Troubleshooting](#) to launch the Call Failure Troubleshooting page. You can click [Call Quality Troubleshooting](#) to launch the Call Quality Troubleshooting page.

User | First Name, and Last 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 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.

**Note**

- The devices in deleted state do not appear in the search results.
- Phone search shows audio phones only. Cisco TelePresence endpoints are not displayed as part of phone search.
- E20 devices are shown as Cisco TelePresence search results only.
- When you search for phones using the MAC address in the global search option, do not use colon or hyphen or dots in between.
- The global search option is not available in Cisco Prime Collaboration Assurance - Standard.

### Search Use Cases

You can perform a search based on the following use cases.

**Table 16: Search Use Cases**

<table>
<thead>
<tr>
<th>To search for...</th>
<th>Perform/Use</th>
</tr>
</thead>
</table>
| 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 | Phone Search |
| E20 | TelePresence Search |
Device-Specific Inventory Details

The following tables provide field descriptions for additional inventory details for:

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Endpoints</td>
<td>Total number of unknown endpoints. You can click on this number to launch the filtered list of unknown endpoints in the Endpoint Diagnostics page.</td>
</tr>
<tr>
<td>Partially Managed</td>
<td>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 session monitoring or 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.</td>
</tr>
</tbody>
</table>

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.

Assurance 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 Assurance 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 Assurance Inventory Summary data is refreshed every 30 seconds.

Table 17: Assurance Inventory Summary - Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure devices</td>
<td>Device Search - For example search with a string such as 10.*</td>
</tr>
</tbody>
</table>
| IP address of a device with a partial IP address. | 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 *.
| List of all users associated with a particular customer. |                                                                                                                                               |
Table 18: CTS, Cisco Codec, MX, E20, MXP, and Polycom
Table 19: Cisco TelePresence Movi
Table 20: Cisco Unified IP Phone 8900 and 9900 Series, and Cisco Cius
Table 21: CTMS
Table 22: CTS-Manager and Cisco TMS
Table 23: Cisco Unified CM
Table 24: Cisco MCU and MSE
Table 25: Cisco VCS
Table 26: Cisco TelePresence Conductor
### Table 18: CTS, Cisco Codec, MX, E20, MXP, and Polycom

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TelePresence Endpoint</td>
<td>Name assigned to the endpoint for ease of identification.</td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>IP phone details as defined in the endpoint.</td>
</tr>
<tr>
<td>Directory Number</td>
<td>Hostname or IP address of the Cisco Unified CM server where the endpoint is registered.</td>
</tr>
<tr>
<td>Call Controller</td>
<td>Identification of the Cisco Unified CM cluster where the Cisco Unified CM server is registered.</td>
</tr>
<tr>
<td>CUCM Address</td>
<td>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.</td>
</tr>
<tr>
<td>CUCM Cluster ID</td>
<td>H.323 ID configured on the Cisco Codec device.</td>
</tr>
<tr>
<td>VCS Address</td>
<td>E164 number configured on the Cisco Codec device.</td>
</tr>
<tr>
<td>VCS Cluster ID</td>
<td>Network address of the gatekeeper to which the Cisco Codec device is registered.</td>
</tr>
<tr>
<td>Registration Status</td>
<td>Registered SIP URI on the Cisco Codec device.</td>
</tr>
<tr>
<td>H323 Gatekeeper Address</td>
<td>SIP proxy address that is configured manually on the Cisco Codec device.</td>
</tr>
<tr>
<td>SIP URI</td>
<td>Application Manager</td>
</tr>
<tr>
<td>CTSMAN</td>
<td>Hostname or IP address of the application manager where the CTS is integrated.</td>
</tr>
<tr>
<td>TMS</td>
<td>Hostname or IP address of the application manager where the Cisco Codec device is integrated.</td>
</tr>
<tr>
<td>Connected To Switch</td>
<td>Details of the switch to which the endpoint is connected.</td>
</tr>
<tr>
<td>Port Connected</td>
<td>Details of the switch port to which the endpoint is connected.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Peripherals | Name<br>Peripheral type, such as uplink, phone, camera, display, touch screen monitor, microphone.<br>Note <br>CTS systems support TelePresence Touch Screen monitoring.<br>Position<br>Position of the peripheral, such as front_center for a microphone.<br>MAC Address<br>MAC address of the peripheral.<br>Software Version<br>Software version running on the peripheral.<br>Model<br>Model of the peripheral.<br>Serial<br>Serial number of the peripheral.<br>Make<br>Manufacturer's details for the peripheral.<br>Firmware Version<br>Firmware version of the peripheral.<br>Hardware Version<br>Hardware version of the peripheral.<br>Midlet Version<br>Midlet version running on the peripheral.

---

**Note**<br>Cisco Prime Collaboration does not support peripheral details for Cisco TelePresence 150 MXP.

---

### Table 19: Cisco TelePresence Movi

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Movi</td>
<td>Endpoint Name&lt;br&gt;Name assigned to the endpoint for ease of identification.</td>
</tr>
<tr>
<td>SIP URI</td>
<td>Registered SIP URI on the Cisco TelePresence Movi endpoint.</td>
</tr>
<tr>
<td>VCS Address</td>
<td>Hostname or IP address of the VCS where the endpoint is registered.</td>
</tr>
<tr>
<td>VCS Cluster ID</td>
<td>Identification of the VCS cluster where the VCS is registered.</td>
</tr>
</tbody>
</table>
Table 20: Cisco Unified IP Phone 8900 and 9900 Series, and Cisco Cius

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUCM Endpoint</td>
<td></td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>Name assigned to the endpoint for ease of identification.</td>
</tr>
<tr>
<td>Model</td>
<td>Model of the endpoint, such as CP-8945 or CP-9971.</td>
</tr>
<tr>
<td>Directory Number</td>
<td>IP phone details as defined in the endpoint.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the endpoint.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the endpoint as defined in the call processor.</td>
</tr>
<tr>
<td>Call Controller</td>
<td></td>
</tr>
<tr>
<td>CUCM Address</td>
<td>Hostname or IP address of the Cisco Unified CM server where the endpoint is registered.</td>
</tr>
<tr>
<td>CUCM Cluster ID</td>
<td>Identification of the Cisco Unified CM cluster where the Cisco Unified CM server is registered.</td>
</tr>
<tr>
<td>Registration Status</td>
<td>Registration status of the endpoint with call processor (Cisco Unified CM). If Cisco Unified CM is not managed, the information displayed is N/A.</td>
</tr>
<tr>
<td>Switch Details</td>
<td></td>
</tr>
<tr>
<td>Connected To Switch</td>
<td>Details of the switch to which the endpoint is connected.</td>
</tr>
<tr>
<td>Port Connected</td>
<td>Details of the switch port to which the endpoint is connected.</td>
</tr>
</tbody>
</table>
### Device-Specific Inventory Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Configuration</strong></td>
<td>Display the status of the wi-fi connection, such as connected or not connected.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>IP address used to manage the endpoint when connected using a wi-fi network.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>IP address of the default router to which the endpoint is connected.</td>
</tr>
<tr>
<td><strong>Default Router</strong></td>
<td>Name of the access point to which the endpoint is connected.</td>
</tr>
<tr>
<td><strong>Access Point Name</strong></td>
<td>Displays the status of the Ethernet connection, such as connected or not connected.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>IP address used to manage the endpoint when connected using Ethernet.</td>
</tr>
<tr>
<td><strong>Default Router</strong></td>
<td>IP address of the default router to which the endpoint is connected.</td>
</tr>
</tbody>
</table>

**Note**

For discovery of Cisco Cius and 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.

For Cisco Cius devices, the standard phone description available in the inventory is SEP and MAC address.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multipoint Switch</td>
<td>Timezone Time zone configured on the multipoint switch.</td>
</tr>
<tr>
<td>SKU</td>
<td>—</td>
</tr>
<tr>
<td>Hardware Model</td>
<td>Model number of the media convergence server on which the multipoint switch is running.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of multipoint switch administration software currently installed.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Operating System version.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname configured for the multipoint switch.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used to manage the multipoint switch.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used on the IP address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>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.</td>
</tr>
<tr>
<td>Switch Details</td>
<td></td>
</tr>
<tr>
<td>Connected To Switch</td>
<td>Details of the switch to which the multipoint switch is connected.</td>
</tr>
<tr>
<td>Port Connected</td>
<td>Details of the switch port to which the multipoint switch is connected.</td>
</tr>
<tr>
<td>Ad hoc Segments</td>
<td>Maximum number of segments that are available for impromptu meetings. The maximum number is 48.</td>
</tr>
<tr>
<td>Maximum Segments</td>
<td>Total number of segments (individual video displays) that this multipoint switch can handle. The maximum number is 48.</td>
</tr>
<tr>
<td>Schedulable</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 22: CTS-Manager and Cisco TMS

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Manager SKU</td>
<td>—</td>
</tr>
<tr>
<td>Hardware Model</td>
<td>Model number of the server on which the application manager is running.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of administration software currently installed.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Operating System version.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname configured for the application manager.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used to manage the application manager.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used on the IP address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address number supplied for the application manager.</td>
</tr>
</tbody>
</table>

System Connectivity (see note following this table) Exchange Server: Data displayed only if Calendaring service (Scheduling API mode) is configured in the CTS-Manager.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Whether the exchange server is running or down.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address assigned to the exchange server.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of software currently installed on the exchange server.</td>
</tr>
</tbody>
</table>

LDAP Server: Date displayed only if Active Directory is configured in CTS-Manager.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Whether the LDAP server is running or down.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address assigned to the LDAP server.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of software currently installed on the LDAP server.</td>
</tr>
</tbody>
</table>

Note

For CTS-Manager, the System Connectivity pane is visible only for versions 1.7 and 1.8. Also, the CTS-Manager user configured in the Cisco Prime Collaboration application must have administrative privileges in CTS-Manager.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Processor Cluster ID</td>
<td>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.</td>
</tr>
<tr>
<td>Publisher Hostname</td>
<td>Hostname configured for the cluster publisher.</td>
</tr>
<tr>
<td>Registered CTS Endpoints</td>
<td>Number of registered endpoints on the call processor.</td>
</tr>
<tr>
<td>Total CTS Endpoints</td>
<td>Total number of endpoints.</td>
</tr>
</tbody>
</table>
Table 24: Cisco MCU and MSE

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU or MSE Details</td>
<td>Model number of the media convergence server on which the multipoint switch is running.</td>
</tr>
<tr>
<td>Hardware Model</td>
<td>Serial Number of the Multipoint Control Unit (MCU).</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of multipoint switch administration software currently installed.</td>
</tr>
<tr>
<td>MCU Type/Device Type</td>
<td>Type of the MCU or device.</td>
</tr>
<tr>
<td>Build Version</td>
<td>Build version of the installed software.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Manufacturer’s name.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname configured in the device (MCU or Media Service Engine).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Local IP address of the MCU or Media Service Engine (MSE) network interface used to access the MCU or MSE web user interface.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used on the IP address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Fixed hardware MAC address of the Ethernet port.</td>
</tr>
<tr>
<td>Connected To Router</td>
<td>IP address of the router to which the MCU or MSE is connected.</td>
</tr>
<tr>
<td>Cluster Type</td>
<td>Whether the cluster is a master or slave. If the cluster is configured, Not Configured is displayed.</td>
</tr>
<tr>
<td>Total Video Ports</td>
<td>Number of video ports configured in MCU. (Data displayed only for MCU devices.)</td>
</tr>
<tr>
<td>Total Audio Ports</td>
<td>Number of audio ports configured in MCU. (Data displayed only for MCU devices.)</td>
</tr>
<tr>
<td>SIP (Data displayed only for MCU devices.)</td>
<td>Whether the SIP registration is enabled or disabled.</td>
</tr>
<tr>
<td>Status</td>
<td>Network address of the SIP proxy.</td>
</tr>
<tr>
<td>Domain</td>
<td>Network address of the SIP registrar to which the MCU has registered.</td>
</tr>
<tr>
<td>H.323 (Data displayed only for MCU devices.)</td>
<td>Whether the SIP registration is enabled or disabled.</td>
</tr>
</tbody>
</table>
### Device-Specific Inventory Details

#### Table 24: H.323 Gatekeeper Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Whether the H.323 gatekeeper registration is enabled or disabled.</td>
</tr>
<tr>
<td>Gatekeeper ID</td>
<td>Identifier used by the MCU to register with the H.323 gatekeeper.</td>
</tr>
<tr>
<td>Gatekeeper Address</td>
<td>Network address of the gatekeeper to which the MCU has registered.</td>
</tr>
</tbody>
</table>

#### MSE Blades (Data displayed only for MSE.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the blade.</td>
</tr>
<tr>
<td>Slot</td>
<td>Slot number. Slot 1 is MSE Supervisor; slots 2-10 are blades.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of the software used.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the blade: OK or absent.</td>
</tr>
<tr>
<td>Port A IP Address</td>
<td>IP address of Port A.</td>
</tr>
<tr>
<td>Port B IP Address</td>
<td>IP address of Port B.</td>
</tr>
</tbody>
</table>

#### Table 25: Cisco VCS

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Processor</td>
<td>Cluster ID</td>
</tr>
<tr>
<td>Master</td>
<td>Cluster Name that is used to identify one cluster of VCSs from another.</td>
</tr>
<tr>
<td>Registered Endpoints</td>
<td>Name of the VCS peer that is configured as the cluster master.</td>
</tr>
<tr>
<td>Peers</td>
<td>Number of endpoints registered to the VCS.</td>
</tr>
<tr>
<td></td>
<td>Number of VCS peers configured within the cluster.</td>
</tr>
</tbody>
</table>
## Device-Specific Inventory Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCS Configuration</td>
<td></td>
</tr>
<tr>
<td>Timezone</td>
<td>Time zone that is configured on the VCS.</td>
</tr>
<tr>
<td>Maximum Traversal Calls</td>
<td>Number of traversal call licenses available on the VCS.</td>
</tr>
<tr>
<td>Maximum Non-Traversal Calls</td>
<td>Number of non-traversal call licenses available on the VCS.</td>
</tr>
<tr>
<td>Maximum Registrations</td>
<td>Number of endpoints that can be registered with the VCS.</td>
</tr>
<tr>
<td>Expressway</td>
<td>Whether the VCS Expressway is configured.</td>
</tr>
<tr>
<td>Interworking</td>
<td>Whether the VCS is configured to allow H.323 systems to connect to SIP systems.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Whether AES encryption is available in the software build.</td>
</tr>
<tr>
<td>Find Me</td>
<td>Whether FindMe is enabled or disabled.</td>
</tr>
<tr>
<td>Device Provisioning</td>
<td>Whether the provisioning server is enabled on the VCS.</td>
</tr>
<tr>
<td>Dual Network Interface</td>
<td>Whether the LAN 2 interface on the VCS Expressway is enabled.</td>
</tr>
<tr>
<td>Starter Pack</td>
<td>Whether the Starter Pack option key is installed.</td>
</tr>
</tbody>
</table>

---

**Note**

Cisco Prime Collaboration manages both the Cisco VCS application and appliance.
### Table 26: Cisco TelePresence Conductor

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TelePresence Conductor</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Hostname configured for the conductor.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the conductor.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of software currently installed.</td>
</tr>
<tr>
<td>Cluster Master</td>
<td>Name of the conductor peer that is configured as the cluster master.</td>
</tr>
<tr>
<td>Cluster Peers</td>
<td>Number of conductor peers configured within the cluster.</td>
</tr>
<tr>
<td>Total Registered MCUs</td>
<td>Number of MCUs registered to the conductor.</td>
</tr>
<tr>
<td>Software ID</td>
<td>Identification of the software on the conductor.</td>
</tr>
<tr>
<td>Hardware Serial Number</td>
<td>Serial number of the conductor hardware.</td>
</tr>
<tr>
<td><strong>Registered MCUs</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the MCU registered to the conductor.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the MCU registered to the conductor.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the MCU registered to the conductor.</td>
</tr>
<tr>
<td>Pool</td>
<td>MCU pool to which the MCU belongs.</td>
</tr>
<tr>
<td>Blacklisted</td>
<td>Listed MCUs are not used by the conductor.</td>
</tr>
<tr>
<td>Blacklisted Reason</td>
<td>Reason why the MCUs are not used by the conductor.</td>
</tr>
<tr>
<td>Media Load: Allocated/In Use/ Max Available</td>
<td>Media load allocated and in use, and the maximum available load.</td>
</tr>
<tr>
<td>Signalled Load: Allocated/In Use/ Max Available</td>
<td>Signalled load allocated and in use, and the maximum available load.</td>
</tr>
</tbody>
</table>

**Note**

Only Cisco TelePresence Conductor-controlled MCU cascading is supported.
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 27: Recommendations to Update Inventory**

<table>
<thead>
<tr>
<th>Description</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have both voice and video endpoints deployed in your network, and want to collect data on both.</td>
<td>Perform Update Inventory (choose <strong>Device Inventory &gt; Inventory Management &gt; Update Inventory</strong>). For more information, see <strong>Update Inventory</strong>.</td>
</tr>
<tr>
<td>If you have both voice and video endpoints deployed in your network, and you want to collect data on video endpoints only.</td>
<td>Perform Update Inventory (choose <strong>Device Inventory &gt; Inventory Management &gt; Update Inventory</strong>). For more information, see <strong>Update Inventory</strong>.</td>
</tr>
<tr>
<td>If you have both voice and video endpoints deployed in your network, and you want to collect data on voice endpoints only.</td>
<td>Perform IP Phone Inventory Collection and Cluster Data Discovery (choose <strong>Assurance Administration</strong>). For more information, see <strong>Inventory Details Collection</strong>.</td>
</tr>
<tr>
<td>If you have only a voice network</td>
<td>Perform IP Phone Inventory Collection and Cluster Data Discovery (choose <strong>Assurance Administration</strong>). For more information, see <strong>Inventory Details Collection</strong>.</td>
</tr>
<tr>
<td>If you have only a video network</td>
<td>Perform Update Inventory (choose <strong>Device Inventory &gt; Inventory Management &gt; Update Inventory</strong>). For more information, see <strong>Update Inventory</strong>.</td>
</tr>
</tbody>
</table>

**Update Inventory**

The Update Inventory task helps you to synchronize the Cisco Prime Collaboration 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 database up-to-date.
- There are any changes in the network devices' interfaces.
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 database up-to-date.

To update inventory:

**Procedure**

**Step 1** Choose Device 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 Update Inventory. To run the job immediately, go to Update Inventory.

**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** Check the status of your job by doing one of the following:
- If you clicked 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 28: Job Schedule - Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Select Start Time to enter the start date and time in the <code>yyyy/MM/dd</code> and <code>hh:mm AM/PM</code> 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.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Select None, Hourly, Daily, Weekly, or Monthly to specify the job period.</td>
</tr>
<tr>
<td>Settings</td>
<td>Details of the job period.</td>
</tr>
<tr>
<td>End Time</td>
<td>If you do not want to specify an end date/time, click <strong>No End Date/Time</strong>. Click End at to enter the end date and time in the <code>yyyy/MM/dd</code> and <code>hh:mm AM/PM</code> format respectively.</td>
</tr>
</tbody>
</table>

Inventory Details Collection

Cisco Prime Collaboration 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 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 (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 an overview of inventory collection tasks, see the following table.
Table 29: Overview of Inventory Collection Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule inventory collection of IP Phones</td>
<td>Choose Device Inventory &gt; Inventory Schedule &gt; IP Phone Inventory Schedule to add, edit, or delete the IP phone discovery schedules. (For more information, see IP Phone Discovery Schedule.)</td>
</tr>
<tr>
<td>Schedule inventory collection of Phone XML</td>
<td>Choose Device Inventory &gt; Inventory Schedule &gt; IP Phone XML Inventory Schedule to add, edit, or delete the IP phone discovery schedules. (For more information, see IP Phone Discovery Schedule.)</td>
</tr>
<tr>
<td>Schedule inventory collection of cluster devices</td>
<td>Choose Device Inventory &gt; Inventory Schedule &gt; Cluster Data Discovery Schedule to add, edit, or delete the cluster device discovery schedules. (For more information, see Unified CM Cluster Data Discovery.)</td>
</tr>
</tbody>
</table>

IP Phone Discovery Schedule

When you choose Device Inventory > Inventory Schedule > IP Phone Inventory Schedule, you can perform the following tasks:

*View and Add an IP Phone Collection Status*

To view IP phone collection status, choose Device Inventory > Inventory Schedule > IP Phone Inventory Schedule.

The IP Phone Collection Status pane displays the information mentioned in the following table.

Table 30: IP Phone Collection Status - Field Descriptions

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
</table>
| Collection Status | Displays the status of the discovery process. The status could be any one of the following:  
  - In progress—When you start PIFSver for the first time or restart it, discovery takes place automatically and the status appears as In Progress.  
  - Complete—The discovery process is complete.  
  - Not available. Try after some time—Appears when you start PIFSver for the first time, or restart it, and the discovery process has not yet begun. |
### Adding an IP Phone Discovery Schedule

Cisco Prime Collaboration provides six default schedules for phone discovery. You can update or delete them; you can also add up to 10 phone discovery schedules.

To add an IP phone schedule:

#### Procedure

1. **Step 1** Choose Device Inventory > Inventory Schedule > IP Phone Inventory Schedule.
2. **Step 2** On the IP Phone Discovery Schedule page, click Add.
3. **Step 3** Enter the required information in the Add Schedule dialog box.
4. **Step 4** Click OK.

You can also edit or delete an IP phone discovery schedule:

- To edit, select a phone discovery schedule and click Edit. Make the required changes, click OK, and then click Apply.
- To delete, select a phone discovery schedule and click Delete. In the confirmation message box, click Yes.

Any information collected through phone polling is not collected for Unified CMs in a NAT environment. IP phone polling does not work in following cases:

- IP phones that are behind the NAT environment.
- IP phones that support only secure HTTP (HTTPS) connections (for example, the Cisco 7936 model).
- IP phones that do not support a HTTP/XML interface (for example, third-party phones). If any of these scenarios are present, the above parameters will not be collected from IP phones.

### Schedule IP Phone XML Discovery Schedule

The IP Phone XML Inventory Collection helps you get information on phone load, serial number, switch information (if applicable), device pool etc.

#### Note

You can collect the switch details like LLDPNeighborDeviceId, LLDPNeighborIP, and LLDPNeighborPort from Phone XML LLDP fields when the CDP fields are empty.
To schedule when phone discovery should take place, you can use the Phone XML Collection page. The default scheduled start for Phone XML discovery is daily at 3:00 p.m. Phone XML discovery collects serial number, load ID, and App ID for each phone.

To schedule an IP Phone XML discovery:

**Procedure**

**Step 1** Choose Device Inventory > Inventory Schedule > IP Phone Inventory Schedule > XML Inventory Collection  
**Step 2** In the XML Collection tab, make the desired changes.  
**Step 3** Click Apply, then click OK in the confirmation message box.  

*Note*  
IP Phone XML Inventory Schedule is applicable only for phones that are registered to Cisco Unified CM Express.

---

**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 does not monitor this device. That is, session, 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 does not poll the devices.
- If a suspended endpoint joins a new session, the endpoint is shown as Unknown in the Session Topology pane.
- If a suspended endpoint is already in an in-progress session, the endpoint icon (in the Session Topology pane) changes to Unknown immediately after the endpoint state is changed to Suspended.
- If CTS-Manager is suspended, new session data is not imported and the CTS-Manager polling is not performed. The existing session data (last polled data) is displayed in the Cisco Prime Collaboration server.
- If Cisco Unified CM publisher is suspended, Cisco Prime Collaboration 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.
- 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.

To suspend or resume managed devices:
Procedure

**Step 1** Choose Device 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.

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 server. To rediscover a deleted device, see Rediscover Devices. You can access the deleted device's details as part of the past session data.

To delete a device:

Procedure

**Step 1** Choose Device 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 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 Topology View, Alarm & Events page, and IP SLA Voice Test 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.
• Data is available on disk from IP SLA Voice Test that you have configured.
• 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.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco recommends following these guidelines for optimal performance graph viewing.</td>
<td>The following guidelines are recommended:</td>
</tr>
<tr>
<td></td>
<td>• No more than five metrics be selected for one graph.</td>
</tr>
<tr>
<td></td>
<td>• No more than ten graphs on the user interface.</td>
</tr>
<tr>
<td></td>
<td>• No more than ten items selected for merge.</td>
</tr>
<tr>
<td></td>
<td>• No more than ten items for IP SLA Voice graphing.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>A voice gateway, MGCP, and H323 on a router. When you have all these capabilities on one device, each metric displays two graphs.</td>
<td>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.</td>
</tr>
<tr>
<td>In the Select Metrics dialog box for Unified CCE and Cisco Packaged Contact Center Enterprise, you will see the following fields:</td>
<td>To view a performance graph for any of these metrics, you must enter the name of the Unified CCE or PCCE instance for which you want the information, in the field next to Instance Name. Each Unified CCE or PCCE contains a list of enterprise contact center applications, which are identified by their instance name.</td>
</tr>
<tr>
<td>• Agents logged on</td>
<td></td>
</tr>
<tr>
<td>• Calls in progress</td>
<td></td>
</tr>
<tr>
<td>• Inbound Calls per second</td>
<td></td>
</tr>
</tbody>
</table>
Cisco Prime Collaboration does not display a performance graph for all Unified Contact Center Enterprise (Unified CCE) and Packaged Contact Center Enterprise (PCCE) machines.

Cisco Prime Collaboration only collects data for Unified CCEs that have router capabilities. To verify your Unified CCE’s capabilities, you can run a device report through device management, and look for Unified CCE or IPCC Router or PCCE in the Device Capabilities column of the Device report.

You cannot view a performance graph for Unified CCEs and PCCEs that do not have router capabilities. Instead, you will get a message window stating such.

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 is collecting data and is configured properly to receive this data.

### Launch a Performance Graph

The performance graphs are available through the following:

- Topology View
- Device 360 degree View - Click on the Launch Tools icon, and then click on Performance Graph.
- Event Details page
- IP SLA Voice Test 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 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 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.

<table>
<thead>
<tr>
<th>Graph Data Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Time</td>
<td>When you launch a performance graph, it shows real time data by default.</td>
</tr>
</tbody>
</table>
### Performance Graphs

<table>
<thead>
<tr>
<th>Graph Data Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly Average</td>
<td>When you select Hourly Average, the performance graph shows average data for the hour.</td>
</tr>
<tr>
<td>Hourly Max</td>
<td>When you select Hourly Max, the performance graph shows peak data for the hour.</td>
</tr>
<tr>
<td>Hourly Min</td>
<td>When you select Hourly Min, the performance graph shows minimum data for the hour.</td>
</tr>
<tr>
<td>History</td>
<td>When you select History, the performance graph shows hourly average data for seven days.</td>
</tr>
<tr>
<td>All</td>
<td>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 selects points at regular intervals and plots them in the graph.</td>
</tr>
</tbody>
</table>

### 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 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.
<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Causes</th>
</tr>
</thead>
</table>
| Cannot collect data. | • Account and credentials are not the same on all Cisco Unified Communications Managers in the cluster.  
• HTTP server problems:  
  • 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.  
• 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 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.  
For a list of devices supported by Cisco Prime Collaboration 11.0, see [Supported Devices for Prime Collaboration Assurance](#). |
| Cannot collect data because of the following:  
• 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. | • No credentials in Cisco Prime Collaboration.  
• Incorrect credentials in Cisco Prime Collaboration.  
To add credentials, see [Add a Device Credentials Profile](#). |
<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot collect data from the device because of the following:</td>
<td>Incorrect Cisco Unified Communications Manager version. Check the following:</td>
</tr>
<tr>
<td>• A processing error occurred.</td>
<td>• The version of the Cisco Unified Communications Manager that is running on the device.</td>
</tr>
<tr>
<td>• Parsing or processing errors occurred.</td>
<td>• The Cisco Unified Communications Manager version number that is stored in Prime Collaboration.</td>
</tr>
<tr>
<td>• Internal initialization errors occurred.</td>
<td>• If the Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration is incorrect, add the device again.</td>
</tr>
<tr>
<td>• Initialization problems occurred in the device data collector.</td>
<td>For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
<tr>
<td>Cannot collect data from the device. The certificate hostname/IP Address cannot be mapped to the URL hostname/IP Address.</td>
<td>The device is not in DNS.</td>
</tr>
<tr>
<td>Incomplete data collected because an error occurred in communicating with the device.</td>
<td>Incorrect Cisco Unified Communications Manager version. Check the following:</td>
</tr>
<tr>
<td></td>
<td>• The version of the Cisco Unified Communications Manager that is running on the device.</td>
</tr>
<tr>
<td></td>
<td>• The Cisco Unified Communications Manager version number that is stored in Prime Collaboration.</td>
</tr>
<tr>
<td></td>
<td>• If the Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration is incorrect, add the device again.</td>
</tr>
<tr>
<td></td>
<td>For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
</tbody>
</table>
### Possible Causes

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot collect data because of the following:</td>
<td>• No data from a required MIB.</td>
</tr>
<tr>
<td>• The device returned no data from a required MIB.</td>
<td>• A required MIB is not populated on the device.</td>
</tr>
<tr>
<td>• The device received no MIB data.</td>
<td>• No MIBs returned data.</td>
</tr>
<tr>
<td></td>
<td>• Device is unreachable due to a network problem.</td>
</tr>
<tr>
<td></td>
<td>• Device credentials do not contain a valid SNMP community read string.</td>
</tr>
<tr>
<td></td>
<td>• SNMP response slow; data collection timed out.</td>
</tr>
<tr>
<td>• The rate of queries on the Cisco Unified Communications Manager exceeds the limit.</td>
<td>Too many queries on a Cisco Unified CM 6.0 or later. Check the polling settings; they should not be less than three minutes.</td>
</tr>
<tr>
<td>• An error has occurred in the data processing stage.</td>
<td>Query exceeded time limit on Cisco Unified CM 6.0 or later.</td>
</tr>
<tr>
<td>• The Cisco Unified Communications Manager did not have enough time to handle the query requests.</td>
<td>Cisco Prime Collaboration must be configured properly using the maximum capacity.</td>
</tr>
<tr>
<td>• An error has occurred in the data processing stage.</td>
<td></td>
</tr>
</tbody>
</table>

Cisco Unity or Unity Express trunk utilization graphs are not working.

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.

### Perform Device Search

You can search for devices within a cluster, based on the search criteria you specify.

If you have deployed Cisco Prime Collaboration in MSP mode, search results depend on the global customer selection.

To perform a device search, go to **Monitor > UC Cluster Status**. You can view the devices based on the saved search criteria you select from the Saved Search drop-down list.
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:

**Procedure**

**Step 1** Choose **Monitor > UC Cluster Status**.

**Step 2** Click **New Search**.

**Step 3** 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 4** 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 5** 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 toolbar 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.
- Devices in your network are not listed in Inventory Management.
- SNMP Polling is not happening successfully.
- Data collection for example for Diagnostics tests is not successful.

Prerequisite - Devices should be supported by Cisco Prime Collaboration.

For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.

To perform SNMP query:

1. Choose **Device 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 Assurance database, the details are auto-populated on the screen. Else, 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 Assurance database, the details are auto-populated on the screen. Else, 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 Assurance database yet.
- If device is in Unknown or Inaccessible state in Inventory Management.
- SNMP Credentials have not been configured on the device.
Poll Devices

• Overview, page 159
• Polling Parameters—Settings, page 160
• View Polling Parameters, page 161
• Edit Polling Parameters, page 161

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 database.

Cisco Prime Collaboration 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 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 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 Topology view, Alarms & Events page, IP SLA Voice Test 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:

• 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.

• The default polling internal 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 Assurance Administration > Polling Settings page, when you select a Device Group.

From the Polling Parameters page, you can perform any of the following tasks:
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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Assurance Administration &gt; Polling Settings</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a Device Group for which you can set polling parameters. (Generally, this is a device group that does not contain subgroups.)</td>
</tr>
<tr>
<td>Step 3</td>
<td>When you are done viewing the polling parameters, close the window.</td>
</tr>
</tbody>
</table>

Edit Polling Parameters

When you edit Cisco Prime Collaboration 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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Assurance Administration &gt; Polling Settings</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a device group for which you can set polling parameters. (Generally, this is a device group that does not contain subgroups.)</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the polling parameter that you want to edit, choose the appropriate value from the Polling Interval drop-down, and click <strong>Enable</strong>.</td>
</tr>
</tbody>
</table>
| 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, page 165
- Set Threshold Rules, page 183
- Monitor Alarms and Events, page 197
Cisco Prime Collaboration 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 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 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.
You can change the event severity sent in notifications from the Cisco Prime Collaboration default value to a user-defined value.

This table describes the alarm and event severity and status.

### Table 31: Alarm and Event Severity and Status

<table>
<thead>
<tr>
<th>Events</th>
<th>Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td></td>
</tr>
<tr>
<td>• Critical.</td>
<td>• Critical</td>
</tr>
<tr>
<td>• Major</td>
<td>• Major</td>
</tr>
<tr>
<td>• Minor</td>
<td>• Minor</td>
</tr>
<tr>
<td>• Warning.</td>
<td>• Warning</td>
</tr>
<tr>
<td>• Informational—If any event is cleared, its severity changes to informational. Some events, by default, have severity as Informational.</td>
<td>• Cleared</td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>• Active—The event is live.</td>
<td>• Acknowledged—A user has manually acknowledged the alarm. A user can acknowledge only active events.</td>
</tr>
<tr>
<td>• Cleared—The event is no longer active.</td>
<td>• Cleared—The alarm is no longer active.</td>
</tr>
<tr>
<td></td>
<td>• Active—The alarm is live.</td>
</tr>
<tr>
<td></td>
<td>• User Cleared</td>
</tr>
</tbody>
</table>

### 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 32: Notification Groups

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification criterion</td>
<td>A named set of reasons to generate a notification.</td>
</tr>
</tbody>
</table>
### 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 supports device-based notification criterion. The following table describes the device-based notification criterion.

**Table 33: Notification Criterion**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>The devices, device groups, or clusters that you want to monitor.</td>
</tr>
<tr>
<td>Alarm sets</td>
<td>(Optional). One or more groups of alarms that you want to monitor. See <em>Notifications Limited to Specific Alarms</em>.</td>
</tr>
<tr>
<td>Alarm severity and status</td>
<td>One or more alarm severity levels and status.</td>
</tr>
</tbody>
</table>

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 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>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification type</td>
<td>The type of notification to send: SNMP trap, e-mail, or syslog.</td>
</tr>
<tr>
<td>Notification recipients</td>
<td>Hostnames and ports for systems that listen for SNMP traps, syslog messages, or e-mail addresses.</td>
</tr>
<tr>
<td>Daily subscription activity period</td>
<td>The hours during which Cisco Prime Collaboration should use this subscription while monitoring the events for which to send notifications.</td>
</tr>
</tbody>
</table>
Table 34: Notification Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SNMP Trap Notifications** | Cisco Prime Collaboration 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. CISCO-EPM-NOTIFICATION-MIB defines the trap message format.  

Using SNMP trap notification is different from forwarding raw traps to another server before they have been processed by Cisco Prime Collaboration.  

**Note** Cisco Prime Collaboration supports SNMP version 1 (SNMPv1) and SNMPv2 traps for polling and receiving. Cisco Prime Collaboration forwards traps as SNMPv2 traps. However, trap processing with SNMPv3 is not supported in Cisco Prime Collaboration.  

See SNMP Trap Notifications for details on mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration for alarms and events. |
| **E-Mail Notifications** | Cisco Prime Collaboration 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.  

In a NAT environment, the Private IP Address of the device is also displayed.  

If you have installed Cisco Prime Collaboration in MSP mode, you can see the customer to which the device belongs to. |
| **Syslog Notifications** | Cisco Prime Collaboration generates syslog messages for alarms that can be forwarded to syslog daemons on remote systems.  

In a NAT environment, the Private IP Address of the device is also displayed.  

If you have installed Cisco Prime Collaboration in MSP mode, you can see the customer to which the device belongs to.  

See Syslog Notifications for sample syslog messages and description. |

**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](http://Cisco.com).
The table below describes the mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration for alarms.

**Table 35: CISCO-EPM-NOTIFICATION-MIB Summary for Alarms**

<table>
<thead>
<tr>
<th>Trap Field Name</th>
<th>OID</th>
<th>Type</th>
<th>Prime Collaboration Alarm</th>
<th>Content as in Trap Forwarder (EPM MIB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cenAlarmIndex</td>
<td>1.3.6.1.4.1.9.9.311.1.12.1.1</td>
<td>Unsigned32</td>
<td>-</td>
<td>MIB index</td>
</tr>
<tr>
<td>cenAlarmVersion</td>
<td>1.3.6.1.4.1.9.9.311.1.12.12</td>
<td>SnmpAdmin String</td>
<td>-</td>
<td>The version of this MIB. The version string will be of the form major version.minor version. <strong>Note</strong>: Always set to 9.0</td>
</tr>
<tr>
<td>cenAlarmTimestamp</td>
<td>1.3.6.1.4.1.9.9.311.1.12.13</td>
<td>Timestamp</td>
<td>Timestamp</td>
<td>The time when the alarm was triggered.</td>
</tr>
<tr>
<td>cenAlarmUpdatedTimestamp</td>
<td>1.3.6.1.4.1.9.9.311.1.12.14</td>
<td>Timestamp</td>
<td>lastmodified timestamp</td>
<td>The last time when the alarm was modified.</td>
</tr>
<tr>
<td>cenAlarmInstanceID</td>
<td>1.3.6.1.4.1.9.9.311.1.12.15</td>
<td>SnmpAdmin String</td>
<td>ID</td>
<td>The unique alarm ID generated by Cisco Prime Collaboration.</td>
</tr>
<tr>
<td>cenAlarmStatus</td>
<td>1.3.6.1.4.1.9.9.311.1.12.16</td>
<td>Integer32</td>
<td>lastcleartime</td>
<td>Indicates whether the alarm is active (1) or cleared (2)</td>
</tr>
</tbody>
</table>
| cenAlarmStatusDefinition | 1.3.6.1.4.1.9.9.311.1.12.17 | SnmpAdmin String    | lastcleartime             | A short description of the status of the alarm:  
  • 1-Active  
  • 2-Cleared |
<p>| cenAlarmType          | 1.3.6.1.4.1.9.9.311.1.12.18 | Integer             | -                         | The alarm type is direct (2). |
| cenAlarmCategory      | 1.3.6.1.4.1.9.9.311.1.12.19 | Integer32           | category                  | The alarm categories. It is represented as an integer value. |</p>
<table>
<thead>
<tr>
<th>cenAlarmCategory</th>
<th>Description</th>
<th>SnmpAdminString</th>
<th>category</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Endpoint-Hardware alarms (peripheral errors) in all endpoints.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Network Devices-Hardware alarms (interface errors) in all network devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Service Infrastructure-Alarms in call and session control (Cisco Unified CM and VCS), management (CTS-Manager and TMS), multipoint switches (CTMS), and multipoint control units (TPS, MCU).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Session-Endpoints alarms (that are part of the session) and network alarms (jitter, latency, or drop).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>cenAlarmServerAddressType</th>
<th>InetSocketAddress</th>
<th>-</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cenAlarmServerAddress</td>
<td>InetSocketAddress</td>
<td>-</td>
<td>Cisco Prime Collaboration IP address.</td>
</tr>
<tr>
<td>cenAlarmManagedObjectClass</td>
<td>SnmpAdminString</td>
<td>Source</td>
<td>Entity type of the source, such as CTS, Cisco VCS, and so on.</td>
</tr>
<tr>
<td>ObjectName</td>
<td>OID</td>
<td>Type</td>
<td>Source</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>cenAlarmManaged</td>
<td>1.3.6.1.4.1.9.931.1.121.14</td>
<td>InetAddress Type</td>
<td>Source</td>
</tr>
<tr>
<td>cenAlarmManaged</td>
<td>1.3.6.1.4.1.9.931.1.121.15</td>
<td>InetAddress</td>
<td>Source</td>
</tr>
<tr>
<td>cenAlarmDescription</td>
<td>1.3.6.1.4.1.9.931.1.121.16</td>
<td>OctetString</td>
<td>Description</td>
</tr>
<tr>
<td>cenAlarmSeverity</td>
<td>1.3.6.1.4.1.9.931.1.121.17</td>
<td>Integer32</td>
<td>Severity</td>
</tr>
</tbody>
</table>
| cenAlarmSeverity Definition| 1.3.6.1.4.1.9.931.1.121.18 | OctetString | Severity | Alarm severity string representation (number,description):
|                            |                         |         |        | • 0,critical
|                            |                         |         |        | • 1,major
|                            |                         |         |        | • 2,minor
|                            |                         |         |        | • 3,warning
|                            |                         |         |        | • 4,info
|                            |                         |         |        | • 5,normal
|                            |                         |         |        | • 6,unknown
|                            |                         |         |        | • 7,cleared
<p>| cenAlarmTriageValue        | 1.3.6.1.4.1.9.931.1.121.19 | Integer32 | -      | Not used.                                                                  |
| cenEventIDList             | 1.3.6.1.4.1.9.931.1.121.20 | OctetString | -      | List of event IDs that led to this alarm.                                  |
| cenUserMessage1            | 1.3.6.1.4.1.9.931.1.121.21 | SnmpAdmin String | isAcknowledged | Indicates whether the alarm is acknowledged or unacknowledged. |</p>
<table>
<thead>
<tr>
<th>cenUserMessage2</th>
<th>1.3.6.1.4.1.9.9.311.1.12122</th>
<th>SnmpAdmin String</th>
<th>previous Severity</th>
<th>Previous severity of the alarm. For example, assume that while the session was in-progress, a major alarm was triggered. After the session is complete, the session alarm is automatically Cleared. The alarm severity displays Major because the previous alarm severity for this session was Major.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cenUserMessage3</td>
<td>1.3.6.1.4.1.9.9.311.1.12123</td>
<td>SnmpAdmin String</td>
<td>-</td>
<td>Not used.</td>
</tr>
<tr>
<td>cenAlarmMode</td>
<td>1.3.6.1.4.1.9.9.311.1.12124</td>
<td>Integer</td>
<td>-</td>
<td>2-alert. Indicates this trap is either an alarm or event notification.</td>
</tr>
<tr>
<td>cenPartitionNumber</td>
<td>1.3.6.1.4.1.9.9.311.1.12125</td>
<td>Unsigned32</td>
<td>-</td>
<td>Not used.</td>
</tr>
<tr>
<td>cenPartitionName</td>
<td>1.3.6.1.4.1.9.9.311.1.12126</td>
<td>SnmpAdmin String</td>
<td>-</td>
<td>Not used.</td>
</tr>
<tr>
<td>cenCustomerId Identification</td>
<td>1.3.6.1.4.1.9.9.311.1.12127</td>
<td>SnmpAdmin String</td>
<td>ownerid</td>
<td>In the Enterprise mode, the Customer Identification details entered in the Cisco Prime Collaboration notification user interface is displayed. In the MSP mode, the customer name will be displayed.</td>
</tr>
<tr>
<td>cenCustomerRevision</td>
<td>1.3.6.1.4.1.9.9.311.1.12128</td>
<td>SnmpAdmin String</td>
<td>-</td>
<td>Not used.</td>
</tr>
<tr>
<td>cenAlertID</td>
<td>1.3.6.1.4.1.9.9.311.1.12129</td>
<td>SnmpAdmin String</td>
<td>id</td>
<td>The Unique alarm ID assigned by Cisco Prime Collaboration. See the Cisco Prime Collaboration Supported Alarms and Events table for the assigned alarm IDs.</td>
</tr>
</tbody>
</table>

The following table describes the mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration for events.
Table 36: CISCO-EPM-NOTIFICATION-MIB Summary for Events

<table>
<thead>
<tr>
<th>Trap Field Name</th>
<th>OID</th>
<th>Type</th>
<th>Prime Collaboration Event</th>
<th>Content as in Trap Forwarder (EPM MIB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cenAlarmIndex</td>
<td>1.3.6.1.4.1.9.9.311.1.121.1</td>
<td>Unsigned32</td>
<td>-</td>
<td>MIB index</td>
</tr>
<tr>
<td>cenAlarmVersion</td>
<td>1.3.6.1.4.1.9.9.311.1.121.2</td>
<td>SnmpAdmin String</td>
<td>-</td>
<td>The version of this MIB. The version string will be of the form major version . minor version . Note Always set to 9.0</td>
</tr>
<tr>
<td>cenAlarmTimestamp</td>
<td>1.3.6.1.4.1.9.9.311.1.121.3</td>
<td>Timestamp</td>
<td>Timestamp</td>
<td>The time when the event was triggered.</td>
</tr>
<tr>
<td>cenAlarmLastUpdatedTimestamp</td>
<td>1.3.6.1.4.1.9.9.311.1.121.4</td>
<td>Timestamp</td>
<td>-</td>
<td>Not used.</td>
</tr>
<tr>
<td>cenAlarmInstanceID</td>
<td>1.3.6.1.4.1.9.9.311.1.121.5</td>
<td>SnmpAdmin String</td>
<td>ID</td>
<td>The unique event ID generated by Cisco Prime Collaboration.</td>
</tr>
<tr>
<td>cenAlarmStatus</td>
<td>1.3.6.1.4.1.9.9.311.1.121.6</td>
<td>Integer32</td>
<td>-</td>
<td>Not used.</td>
</tr>
<tr>
<td>cenAlarmStatus Definition</td>
<td>1.3.6.1.4.1.9.9.311.1.121.7</td>
<td>SnmpAdmin String</td>
<td>-</td>
<td>Not used.</td>
</tr>
<tr>
<td>cenAlarmType</td>
<td>1.3.6.1.4.1.9.9.311.1.121.8</td>
<td>Integer</td>
<td>-</td>
<td>The event type is direct (2).</td>
</tr>
<tr>
<td>cenAlarmCategory</td>
<td>1.3.6.1.4.1.9.9.311.1.121.9</td>
<td>Integer32</td>
<td>category</td>
<td>The event categories. It is represented as an integer value.</td>
</tr>
</tbody>
</table>
### SNMP Trap Notifications

<table>
<thead>
<tr>
<th>cenAlarmCategory</th>
<th>136.1.4.199.311.1.121.10</th>
<th>SnmpAdmin String</th>
<th>category</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td></td>
<td></td>
<td>This is a string representation of AlarmCategory (number,description):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 3, Endpoint-Hardware events (peripheral errors) in all endpoints.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 4, Network Devices-Hardware events (interface errors) in all network devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 5, Service Infrastructure-events in call and session control (Cisco Unified CM and VCS), management (CTS-Manager and TMS), multipoint switches (CTMS),, and multipoint control units (TPS, MCU).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 6, Session-Endpoints events (that are part of the session) and network events (jitter, latency, or drop).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>cenAlarmServerAddressType</th>
<th>136.1.4.199.311.1.121.11</th>
<th>InetAddress Type</th>
<th>-</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cenAlarmServerAddress</td>
<td>136.1.4.199.311.1.121.12</td>
<td>InetAddress</td>
<td>-</td>
<td>Prime Collaboration IP address.</td>
</tr>
<tr>
<td>cenAlarmManagedObjectClass</td>
<td>136.1.4.199.311.1.121.13</td>
<td>SnmpAdmin String</td>
<td>Source</td>
<td>Entity type of the source, such as CTS, Cisco VCS, and so on.</td>
</tr>
<tr>
<td>Object</td>
<td>Description</td>
<td>Type</td>
<td>Source</td>
<td>Note</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>cenAlarmManagedObjectAddressType</td>
<td>1.3.6.1.4.1.9.9.311.1.121.14</td>
<td>InetAddress Type</td>
<td>Source</td>
<td>The type of Internet address at which the managed device is reachable. This value is set to 1 for IPv4 management.</td>
</tr>
<tr>
<td>cenAlarmManagedObjectAddress</td>
<td>1.3.6.1.4.1.9.9.311.1.121.15</td>
<td>InetAddress</td>
<td>Source</td>
<td>IP Address of the managed object.</td>
</tr>
<tr>
<td>cenAlarmDescription</td>
<td>1.3.6.1.4.1.9.9.311.1.121.16</td>
<td>OctetString</td>
<td>Description</td>
<td>A detailed description of the event.</td>
</tr>
<tr>
<td>cenAlarmSeverity</td>
<td>1.3.6.1.4.1.9.9.311.1.121.17</td>
<td>Integer32</td>
<td>Severity</td>
<td>Indicates the severity of the event using an integer value. The valid integers are 0 - 7.</td>
</tr>
</tbody>
</table>
| cenAlarmSeverityDefinition | 1.3.6.1.4.1.9.9.311.1.121.18 | OctetString | Severity | Alarm severity string representation (number, description):  
- 0, critical  
- 1, major  
- 2, minor  
- 3, warning  
- 4, info  
- 5, normal  
- 6, unknown  
- 7, cleared |
| cenAlarmTriageValue | 1.3.6.1.4.1.9.9.311.1.121.19 | Integer32 | - | Not used. |
| cenEventIDList | 1.3.6.1.4.1.9.9.311.1.121.20 | OctetString | - | Not used. |
| cenUserMessage1 | 1.3.6.1.4.1.9.9.311.1.121.21 | SnmpAdmin String | - | Not used. |
| cenUserMessage2 | 1.3.6.1.4.1.9.9.311.1.121.22 | SnmpAdmin String | - | Not used. |
| cenUserMessage3 | 1.3.6.1.4.1.9.9.311.1.121.23 | SnmpAdmin String | - | Not used. |
| cenAlarmMode | 1.3.6.1.4.1.9.9.311.1.121.24 | Integer | - | 3-event. Indicates this trap is either an alarm or event notification. |
| cenPartitionNumber | 1.3.6.1.4.1.9.9.311.1.121.25 | Unsigned32 | - | Not used. |
| cenPartitionName | 1.3.6.1.4.1.9.9.311.1.121.26 | SnmpAdmin String | - | Not used. |
| cenCustomerIdentification | 1.3.6.1.4.1.9.9.311.1.121.27 | SnmpAdmin String | - | Not used. |
| cenCustomerRevision | 1.3.6.1.4.1.9.9.311.1.121.28 | SnmpAdmin String | - | Not used. |
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.

This table describes the syslog notification parameters based on the above example:

**Table 37: Syslog Notification Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local7.Emerg</td>
<td>IP address and hostname of the Cisco Prime Collaboration Assurance server where the syslog is generated</td>
</tr>
<tr>
<td>10.78.110.27 Feb 19 14:42:49 pcollab-44798 pcollab-44798</td>
<td></td>
</tr>
</tbody>
</table>
| %local7-0-ALARM    | • 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                                 |

| cenAlertID | 13614199311.12129 | SnmpAdmin String | - | Not used. |
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 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 notification monitors. When you do not use alarm sets, Cisco Prime Collaboration 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:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Assurance Administration &gt; Notification Setup</strong>.</td>
</tr>
</tbody>
</table>
| 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. |
| 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.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Assurance Administration &gt; Notification Setup</strong>, then select the <strong>Custom Notification</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add</strong> to add a new criterion.</td>
</tr>
</tbody>
</table>
| 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 Assurance 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 have installed Cisco Prime Collaboration in MSP mode, the devices displayed depends on the customer(s) you have selected from the global Customer Selection field.  
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, 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 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 following 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. The Assurance Domain column depicts the domain to which the notification group belongs and the 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 38: Add General Information*

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion Name field</td>
<td>Enter a name for the notification criterion.</td>
</tr>
</tbody>
</table>
| Customer Identification field   | Enter any desired identifying information. If you leave this field empty, it remains blank in e-mail and syslog notifications.  
In SNMP trap notifications, it is displayed as follows:  
Customer ID: - |
| Customer Revision field         | Enter any desired identifying information. If you leave this field blank, it remains blank in e-mail and syslog notifications.  
In SNMP trap notifications, it is displayed as follows:  
Customer Revision: * |
| Alarm Set Type list box         | Choose one. |
Notifications Limited to Specific Alarms

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Alarm Severity check boxes       | Check none, one, or more of the following:  
• Critical.  
• Major  
• Minor  
• Warning |
| Alarm Status check boxes         | Check none, one, or more of the following:  
• Active.  
• Acknowledged.  
• Cleared.  
• User Cleared |
| OperationInterval                | Click the Always radio button to schedule the notification group to always be active.  
Choose the hours of the day during which you want this notification group to be active:  
• 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.  
By default, the values are from 00:00 to 00:00 and the subscription is active for 24 hours.  
Use this field, for example, to send e-mail notifications during one shift and not during another. |

Set up Destinations Field Descriptions

This table describes the fields in the Set up Destinations page.

Table 39: Set Up Destination

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Link to Notification Details check box</td>
<td>Check to include URLs in the notification from which users can directly open the relevant page in Cisco Prime Collaboration for more information. Uncheck to omit URLs from notifications.</td>
</tr>
</tbody>
</table>
Graphical User Interface Element | Description
--- | ---
Subscription Type radio buttons | Click one at a time to enter data for each subscription type that you want to include in this subscription:
- 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.
Cisco Prime Collaboration 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.

<table>
<thead>
<tr>
<th>Trap Subscription Type fields</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address/Fully Qualified Domain Name editable column</td>
<td>Enter an IP address or Fully Qualified Domain Name (FQDN) of the host.</td>
</tr>
<tr>
<td>Port editable column</td>
<td>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.</td>
</tr>
<tr>
<td>Comments editable column</td>
<td>(Optional) Enter a comment.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E-Mail Subscription Type fields</th>
<th></th>
</tr>
</thead>
</table>
| SMTP Server field | 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.)
To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button.
For instructions on how to configure a default SMTP server, see Setting System-Wide Parameters Using System Preferences. |
| 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. |
| Recipient Address(es) field | Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon.
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. |
| Send Recipient(s) Subject Only check box | Check to include only the subject in the e-mail message. Uncheck to send a fully detailed e-mail message (default). |

| Syslog Subscription Type fields |  |
### Graphical User Interface Element

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter an IP address or Fully Qualified Domain Name (FQDN) of the host.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Include comments.</td>
</tr>
</tbody>
</table>

### Alarm & Event Setup

<table>
<thead>
<tr>
<th>For information on...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Customization</td>
<td>Set Threshold Rules, on page 183</td>
</tr>
<tr>
<td>Notification</td>
<td>Configure Notifications, on page 165</td>
</tr>
<tr>
<td>Polling Settings</td>
<td>Poll Devices, on page 159</td>
</tr>
</tbody>
</table>
Set Threshold Rules

This section explains how to customize alarms and events to suit your business needs.

- Threshold Rules, page 183
- Configure TelePresence Endpoint Thresholds—Global, page 185
- Overview of Device Pool Thresholds, page 186
- Edit Device Pool Thresholds, page 187
- Overview of Voice Call Grade Settings, page 188
- Add Dynamic Syslogs, page 188
- Correlation Rules, page 190
- Create Custom Events, page 193

Threshold Rules

You can configure the devices to generate events when certain parameters cross predefined thresholds. You can perform the settings at Administration > Alarm & Event Setup > Threshold Settings.

The threshold rules page contains two tabs—Basic and Advanced. The Basic tab lists the inline events in Cisco Prime Collaboration 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 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.

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:
<table>
<thead>
<tr>
<th>Actions</th>
<th>Basic</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Severity</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Raise or Suppress events</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Raise or Suppress thresholds</td>
<td>Yes Expand the event, select threshold, and select Raise, or Suppress from the drop-down.</td>
<td>Yes Expand the event, select threshold, and select Raise, Suppress, or Conditional from the drop-down.</td>
</tr>
<tr>
<td>Edit, Reset, and Delete existing thresholds</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Edit or Delete Events</td>
<td>No</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 Thresholds—Global**

You can set up Cisco Prime Collaboration to have events generated 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:

**Procedure**

1. Choose **Assurance Administration > Session Path Threshold Settings**.
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.

**Configure TelePresence Endpoint Threshold—Device Level**

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.

**Procedure**

1. Choose **Assurance Administration > Event Customization > Threshold Rules**.
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.

---

### Enable Automatic Troubleshooting for TelePresence Endpoints

Perform the following procedure to enable automatic troubleshooting of a session when the threshold value exceeds the defined value for packet loss, jitter, and/or latency.

**Procedure**

**Step 1**  Choose **Assurance 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, 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 does not display the device pool even after completing the cluster device discovery.

The device pool threshold settings in Cisco Prime Collaboration 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 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.

For the "ServiceQualityThresholdCrossed" event, Cisco Prime Collaboration rounds off the threshold value from decimal to whole number.

If you have deployed Cisco Prime Collaboration 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 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.

**Procedure**

**Step 1** Choose **Assurance Administration > Event Customization > Correlation Rules**.

**Step 2** Select **PhoneUnregThresholdExceeded** 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:

a) Select a group, change the default threshold, and click **Edit**.

b) 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 default settings:

c) Check the check box for All Device Pools/CMEs and click **Revert**.

d) 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**.

---

**Note**

For the "ServiceQualityThresholdCrossed" event, Cisco Prime Collaboration rounds off the threshold value from decimal to whole number.
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:

<table>
<thead>
<tr>
<th>Call Grade</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor</td>
<td>If the SCSR (%) value of call is greater than threshold value of long call SCSR (%) or short call SCSR (%) then call grade is Poor.</td>
</tr>
<tr>
<td>Acceptable</td>
<td>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.</td>
</tr>
<tr>
<td>Good</td>
<td>If the SCSR (%) value of call is less than threshold value of long call SCSR (%) or SCSR (%) then call grade is good.</td>
</tr>
</tbody>
</table>

To configure the threshold settings for long call SCSR (%) or short call SCSR (%), choose Assurance 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 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; 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.

We recommend that you do not add:

- Syslogs that are likely to create an excessive load on Cisco Prime Collaboration due to a possible flood of syslogs.
More than 20 syslogs.

To add syslogs:

**Procedure**

**Step 1** Choose **Assurance 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 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 section in the Cisco Prime Collaboration Assurance Advanced - Guide for details.

**Example**

In this example, Cisco Prime Collaboration raises an alarm for the syslog **12E800E**, triggered from a Cisco Unified Intelligent Contact Management (ICM) Enterprise, when you stop or recycle the Cisco CTIOS server

Enter the following values:
  * Syslog Name - 12E800E
  * Event Description - ICM Event
  * Event Severity - Critical
  * Event Clear Interval - 24

This is an example for syslog message, which is raised when an endpoint that has previously registered with Cisco Unified Communications Manager has unregistered:

```
<190>761628: Apr 21 2014 22:11:24.260 UTC : %UC_CALLMANAGER-6-EndPointUnregistered: 
%[Device name=SEP44E4D94499EE][Device IP address=10.17.196.34][Protocol=SIP][Device 
type=493][Device description=SEP44E4D94499EE - 70012][Reason 
Code=8][IPAddressAttributes=0][LastSignalReceived=SIPRegisterInd][CallState=70012-active10][App 
ID=Cisco CallManager][Cluster ID=cucm-sj-cluster1][Node ID=cucm-sj-sub1]: An endpoint has unregistered
```
Here, the syslog name is EndPointUnregistered.

## Correlation Rules

When an event is raised from connected devices, Cisco Prime Collaboration 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 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 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:

### Note

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 Prime Collaboration Contact Center Assurance Guide.

<table>
<thead>
<tr>
<th>Name of the Correlation Rule</th>
<th>Main Events Responsible for the Alarm to be Raised</th>
<th>Symptom Events that Occur Due to the Main Event</th>
<th>Name of the Correlated Alarm</th>
<th>The Correlated Alarm is Raised When ...</th>
<th>Window Time (in min) within which the Main Events and Symptom Events are Received</th>
<th>Number of Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Throttling Detected</td>
<td>Code Yellow, CpuPegging</td>
<td>NA</td>
<td>Code Yellow</td>
<td>Both the main events occur.</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>Interface Flapping</td>
<td>OperationallyDown, OperationallyDown cleared</td>
<td>NA</td>
<td>Interface Flapping</td>
<td>OperationallyDown is followed by OperationallyDown cleared event alternatively for more than three instances.</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>Repeated Location Bandwidth Out Of Resource</td>
<td>LocationBWOutOfResources</td>
<td>NA</td>
<td>Repeated Location Bandwidth Out Of Resource</td>
<td>LocationBWOutOfResources is raised on Cisco Unified Communications Manager for three or more instances.</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>Name of the Correlation Rule</td>
<td>Main Events Responsible for the Alarm to be Raised</td>
<td>Symptom Events that Occur Due to the Main Event</td>
<td>Name of the Correlated Alarm</td>
<td>The Correlated Alarm is Raised When ...</td>
<td>Window Time (in min) within which the Main Events and Symptom Events are Received</td>
<td>Number of Occurrences</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>WAN Link Outage Detected</td>
<td>Unresponsive</td>
<td>NA</td>
<td>Wan Link Outage Detected</td>
<td>Unresponsive event is triggered.</td>
<td>10</td>
<td>NA</td>
</tr>
<tr>
<td>VM Down</td>
<td>VMDown</td>
<td>Unreachable</td>
<td>VMDown</td>
<td>VMDown trap is received from vCenter and Unreachable event for VM is received, based on ICMP polling.</td>
<td>5</td>
<td>NA</td>
</tr>
<tr>
<td>ESX Host Down</td>
<td>HostConnectionFailure</td>
<td>Unreachable</td>
<td>ESXDown</td>
<td>HostConnectionFailure trap is received from vCenter and Unreachable event for ESXHost is received, based on ICMP polling.</td>
<td>5</td>
<td>NA</td>
</tr>
<tr>
<td>Network Down</td>
<td>NetworkConnectivityLost, LostNetworkConnectivityEDVRs</td>
<td>Unreachable</td>
<td>NetworkDown</td>
<td>One of the main event occurs and Unreachable event for ESXHost is received, based on ICMP polling.</td>
<td>5</td>
<td>NA</td>
</tr>
<tr>
<td>UCS Chassis Down</td>
<td>ChassisInOperable, ChassisIOCardInaccessible, ChassisInThermalNonRecoverable</td>
<td>Unreachable</td>
<td>UCSDown</td>
<td>One of the main event occurs.</td>
<td>5</td>
<td>NA</td>
</tr>
</tbody>
</table>
### Correlation Rules

<table>
<thead>
<tr>
<th>Name of the Correlation Rule</th>
<th>Main Events Responsible for the Alarm to be Raised</th>
<th>Symptom Events that Occur Due to the Main Event</th>
<th>Name of the Correlated Alarm</th>
<th>The Correlated Alarm is Raised When ...</th>
<th>Window Time (in min) within which the Main Events and Symptom Events are Received</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Unregistered Threshold Exceeded</td>
<td>NA</td>
<td>NA</td>
<td>Phone Unregistered Threshold Exceeded</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Service Quality Threshold Crossed</td>
<td>NA</td>
<td>NA</td>
<td>Service Quality Threshold Crossed</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

**Note**

The last two rules listed in the table above are threshold rules. Alarms for these rules are raised when the "phone unregistered" and "service quality" threshold values exceed the permitted limit.

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 Rule tab, use the name of the correlation rule.

For all the correlation rules in Cisco Prime Collaboration, 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 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**.
Create Custom Events

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:

**Procedure**

**Step 1** Choose Assurance 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 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. 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 Table, on page 439.

---

**Custom Alert Parameters**

Table describes the parameters you can specify for the custom alert.

---

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 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.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Threshold | Check the check box and enter the value that applies.  
- 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.  
**Note** Use these check boxes in conjunction with the Frequency and Schedule configuration parameters. |
| Value | Click the radio button that applies.  
- 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 |  
- Trigger alert only when value constantly...  
- Trigger immediately |  
- 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 | |
## Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Trigger on every poll</td>
<td>Click the radio button that applies.</td>
</tr>
<tr>
<td>• Trigger &lt;&gt; events within &lt;&gt; minutes</td>
<td>• Trigger on every poll—If you want the alert notification to activate on every poll when the threshold is met, click this radio button. 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.</td>
</tr>
<tr>
<td></td>
<td>• Trigger &lt;&gt; events within &lt;&gt; 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.</td>
</tr>
</tbody>
</table>

## Schedule

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Click the radio button that applies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Trigger immediately (Non-stop monitoring)</td>
<td>• Trigger immediately (Non-stop monitoring)—If you want the alert to be triggered 24 hours a day, click this radio button.</td>
</tr>
<tr>
<td>• Schedule between &lt;&gt; to &lt;&gt;</td>
<td>• Schedule between &lt;&gt; to &lt;&gt;—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.</td>
</tr>
</tbody>
</table>
Monitor Alarms and Events

- Alarms and Alarm Summary, page 197
- Events, page 200
- View Call Events, page 202

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 Session link to launch the Endpoints Monitoring or Session Monitoring page. This link is displayed only for session 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 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.

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: session, endpoint, service infrastructure.

Endpoint Name
Indicates the name assigned to the endpoint for ease of identification. By default, the Endpoint 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 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. See Supported Alarms and Events for Cisco Prime Collaboration for a list of supported alarms and events.

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 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 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 sessions, 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 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 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 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:

**Procedure**

**Step 1** Choose **Device 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
Monitor the Network

- Monitor Video Endpoints, page 207
- Monitor Sessions, page 211
Monitor Video Endpoints

The Endpoint Diagnostics dashboard displays the details of all managed video endpoints. You can add any of the managed 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 session 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 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, page 207
- View User 360 Details, page 209

Endpoint Diagnostics Dashboard

Choose Diagnose > Endpoint Diagnostics to view the Endpoints Diagnostics dashboard. The following table describes the information displayed in the Endpoint Diagnostics dashboard.

Table 40: Endpoint Diagnostics Dashboard

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints Summary Metrics</td>
<td>Provides the following details:</td>
</tr>
<tr>
<td></td>
<td>• Managed endpoints</td>
</tr>
<tr>
<td></td>
<td>• Unregistered endpoints</td>
</tr>
<tr>
<td></td>
<td>• Endpoints currently in use</td>
</tr>
<tr>
<td></td>
<td>• Endpoints with alarms</td>
</tr>
<tr>
<td></td>
<td>• Endpoints added to the watch list</td>
</tr>
</tbody>
</table>
If you have deployed Cisco Prime Collaboration in MSP mode, you can see the customer to which that endpoint belongs to. If you have deployed Cisco Prime Collaboration in Enterprise mode, you can see the assurance domain to which that endpoint belongs to.

You can filter on the Device Model, Cluster Name, Device Pool, 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**. 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 session 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 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 session statistics and session 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.

## 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 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,

### Procedure

**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 Session 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 Sessions—Displays the endpoints of the end user that are currently engaged in a call. The details of the device are tracked from Session Diagnostics. This Active Sessions 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.
  - 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.
Monitor Sessions

Cisco Prime Collaboration tracks the lifecycle of video collaboration sessions in your network. It correlates session data received from various sources and provides end-to-end details on the session.

Cisco Prime Collaboration receives session events from call and session control components, such as Cisco Unified CM and Cisco TelePresence Video Communication Server (VCS). It also retrieves session details from applications, such as management applications, call and session control components, conferencing components, and endpoints.

The number of sessions that can be monitored in Cisco Prime Collaboration Assurance depends on the deployment model, such as small, and medium. For information on supported active sessions on Cisco Prime Collaboration 11.0, see the System Capacity for Cisco Prime Collaboration wiki page.

The session data retrieved from the video collaboration applications includes both scheduled and unscheduled sessions. Cisco Prime Collaboration differentiates sessions 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 session through the company's groupware application, such as Microsoft Exchange, Outlook, and so on. You can also schedule the session directly, using Cisco TelePresence Management Suite (TMS) or Cisco TelePresence Manager (CTS-Manager).
- **Static**—Preconfigured Cisco TelePresence session 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 classifies the sessions structure as follows:

- **Point-to-point**—Session between two endpoints.
- **Multipoint**—Session with more than two endpoints. Between endpoints, you may have either Cisco TelePresence Multipoint Switch or MCU.
- **MultiSite**—Session 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.
center endpoint acts as a conferencing device (like MCU). This type of session 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 sessions status can be:

- In-progress
- Scheduled
- Completed
- No Show, a scheduled session without any participants joining the session until the end time. The scheduled session s are moved to No show only after the scheduled end time and after Cisco Prime Collaboration is synchronized with either Cisco TelePresence Manager (CTS-Manager) or Cisco TMS, after the scheduled end time.

If an endpoint did not join an In-Progress session, a no-show icon is displayed on the endpoint. This status is shown even after the session moves to completed state.

If an endpoint joins a session, but later disconnects from the call before the session is over, a disconnect icon is visible on this endpoint in the session topology. Disconnected could mean that there was a problem, or the caller had to leave the session early.

Prerequisites for Session Diagnostics

The following are required for session diagnostics:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as CTMS, MCU must be in the Managed state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the Setting up Devices for Prime Collaboration Assurance wiki.
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.

Note

Cisco Prime Collaboration does not support Session 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.

For information on data collection for video session, importing sessions, session workflows, and the Session Diagnostic dashboard, see:

Data Collection for Video Sessions

Cisco Prime Collaboration periodically polls the following video service infrastructure devices to get information on the sessions:

- Management devices (CTS-Manager and Cisco TMS)—Cisco Prime Collaboration gets information on the scheduled point-to-point and multipoint sessions. For Cisco TMS, if an unscheduled endpoint is added when the session is in progress, Cisco Prime Collaboration shows the session details for the newly added endpoint.
Cisco Prime Collaboration collects scheduled sessions 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 gets information on the multipoint sessions. It also identifies and supports cascading of multipoint sessions.

- **Multipoint Control Units (MCU and Cisco TS)**—Sessions that are scheduled using these systems are always listed as ad hoc sessions in Cisco Prime Collaboration. These types of sessions are listed on the Session Monitoring page only after the session is started. Cisco Prime Collaboration polls these systems after receiving an event from the endpoints.

Cisco Prime Collaboration polls MCU and Cisco TS whenever these systems receive a call. Cisco Prime Collaboration polls MCUs that are not managed by Cisco TelePresence Conductor directly.

For sessions that are hosted by MCUs controlled by Cisco TelePresence Conductor, Cisco Prime Collaboration polls only the Cisco TelePresence Conductor.

Cisco Prime Collaboration does not support cascading of MCU sessions. Only Cisco TelePresence Conductor controlled MCU cascading is supported.

- **Call and Session Controls (Cisco Unified CM and Cisco VCS)**—Cisco Prime Collaboration gets information on the participants using call processors. It collects details, such as when a user joins the session or disconnects from it. Cisco Prime Collaboration polls call and session controllers periodically.

Cisco Prime Collaboration 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 polls Cisco Unified CM and Cisco VCS periodically for all In Progress calls. Hence, they are synchronized.

**Note** The following browsers are supported for the session monitoring windows:

- Internet Explorer- versions 10, 11
- Mozilla Firefox- versions 31, 38
- Google Chrome- versions 39, 40

Cisco Prime Collaboration receives Connect or Disconnect events in real time from CTX. Whenever Connect or Disconnect events are missed, as a backup mechanism, Cisco Prime Collaboration polls CTX periodically for all In Progress calls. Hence, they are synchronized.

**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. The configured JTAPI user must have permission to access all endpoints that are managed in Cisco Prime Collaboration.
Cisco Prime Collaboration listens to the JTAPI events from the Cisco Unified CM. The endpoints are polled once the call is In Progress. Cisco Prime Collaboration depends on the JTAPI event to move the session to the completed status.

Cisco Prime Collaboration manages multiple Cisco Unified CM clusters. Configure unique cluster IDs as it monitors sessions within a cluster and among clusters (intracluster and intercluster sessions).

Cisco Prime Collaboration 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 and Limited) that you have set on the devices. For the visibility limits, see the System Capacity for Cisco Prime Collaboration wiki page.

If JTAPI is not configured on Cisco Unified CM, then the endpoints registered to it are not shown as part of sessions. 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 servers.

**Cisco VCS**
Cisco Prime Collaboration listens to HTTP feedback events from the Cisco VCS. The endpoints are polled once the call is In Progress. Cisco Prime Collaboration depends on the HTTP feedback event to move the session to the completed status.

Cisco Prime Collaboration manages multiple Cisco VCS clusters. You must configure unique cluster names as it monitors sessions within a cluster and among clusters (intracluster and intercluster sessions).

Cisco Prime Collaboration 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 session 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 session topology. However, the endpoints that are registered to the Cisco VCS Expressway are displayed as Unknown endpoints.

If Cisco Prime Collaboration is not subscribed to VCS through feedback subscription, VCS does not notify the PCA when a registered endpoint joins or leaves a session, or registers or unregisters to VCS. In this case, set the visibility of those endpoint(s) to full or limited as required, and contact your network administrator to check PC’s feedback subscription to VCS.

**Note**
Cisco Prime Collaboration ignores Cisco VCS Expressway Connect/Disconnect events.
Import Sessions from CTS-Manager and Cisco TMS

The CTS-Manager and Cisco TMS contain details on the scheduled sessions. Cisco Prime Collaboration periodically polls these devices to retrieve the session details. You can configure the frequency of the periodic polling based on your business needs.

To enable uninterrupted monitoring of the sessions, you can manage a CTS-Manager or Cisco TMS cluster using the Manage Clusters option (Device Inventory > Inventory Management > Manage CTS-MAN/TMS Clusters).

For Cisco TMS, if an unscheduled endpoint is added when the scheduled session is in progress, Cisco Prime Collaboration shows the sessions details of that endpoint.

Cisco Prime Collaboration imports scheduled sessions data for five days (for the past one day, the current day, and for the next three days).

Note the following points when importing sessions from Cisco TMS:

- Cisco Prime Collaboration supports only the default email template for the Booking Confirm email in Cisco TMS. Sessions 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 does not support this type of meeting because resources are not allocated for it while scheduling.

If you have configured a session to start before the scheduled time in CTS-Manager, configure the same time in Cisco Prime Collaboration. That is, if you have configured to start a session 5 minutes before the scheduled time, configure the same time in the Session Path Threshold Settings page. Otherwise, Cisco Prime Collaboration lists two sessions for a scheduled meeting that has started before the scheduled time.

In addition to the periodic polling, if you want to import the session details immediately, you can choose (Diagnose > Session Diagnostics > Import Sessions).

The Import Sessions task impacts Cisco Prime Collaboration System performance. Use Import Sessions only if it is required.

Two jobs are created for the Import Sessions task. You can monitor these jobs at System Administration > Job Management. The job type is displayed as Synch_CtsMAN-MEETING_UniqueJobID and Synch_TMS-MEETING_UniqueJobID on the Job Management page.

TMS_Session_Import regular jobs run periodically and poll complete details of all sessions.

However, the TMS_Frequent_Session_Import job runs frequently and retrieves only the changes in sessions after the previous polling. (You can change the frequency of polling on System Setup page).

If you are using CTS-Manager 1.7 or later, maintain an interval of at least 5 minutes between Import Sessions tasks. If you import sessions within 5 minutes, the job fails.
Session Workflow and Scenarios

The following chart shows the end-to-end scheduled session workflow.

Figure 4: Scheduled Session Workflow

The following are a few scenarios where Cisco Prime Collaboration does not contain up-to-date details on sessions or display different session structure data:

- Cisco Prime Collaboration shows a scheduled session (point-to-point, multipoint, or multisite) as an ad hoc session if the session gets scheduled and was In Progress after the last CTS-Manager or Cisco TMS poll and before the next scheduled or on-demand polling of the CTS-Manager or Cisco TMS takes place.
- For scheduled multipoint sessions, if Cisco Prime Collaboration is not synchronized with the management applications, the session is shown as an ad hoc session and it collects information from the participating Cisco TelePresence Multipoint Switch or Cisco MCU after Cisco Prime Collaboration receives a Connect event.
- If a conferencing system has moved either to the Unmanaged or Unknown state from the Managed state, then the multipoint sessions are displayed as multiple point-to-point sessions.
- Cisco TMS and Cisco MCU displays the session status as Active immediately after the scheduled time is passed. However, Cisco Prime Collaboration does not change the session status to In Progress until an endpoint joins the session.
- Cisco Prime Collaboration displays sessions that include Unmanaged endpoints. However:
  - For point-to-point sessions, one of the endpoints must be managed in Cisco Prime Collaboration.
  - For multisite sessions, the endpoints that conference the other endpoints must be managed in Cisco Prime Collaboration.
  - For multipoint sessions, the conferencing devices must be managed in Cisco Prime Collaboration.
• If you have used Cisco TMS to reserve only TelePresence rooms, then Cisco Prime Collaboration does not display these sessions. (In Cisco TMS, this conference call type is identified as *Reservation Only*.)

• If Cisco VCS Expressway is in the Inaccessible state, Cisco Prime Collaboration can still monitor the sessions. However, the endpoints are displayed as Unknown endpoints.

• The session diagnostic feature does not support endpoints, which are configured with multiple lines in Cisco Unified CM. However, you can manage these endpoints in the Cisco Prime Collaboration inventory database.

Note

The session monitoring feature is supported only on Cisco Unified CM 8.5 and later.

• If there is a session between a TelePresence and one or more WebEx participants, the Session 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.

**Session Scenarios**

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

**Table 41: Session Scenarios**

<table>
<thead>
<tr>
<th>Session Classification</th>
<th>Session Type</th>
<th>Session Structure</th>
<th>Session Topology Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CM <em>intracluster and intercluster sessions</em></td>
<td>Ad hoc, Scheduled</td>
<td>Point-to-point</td>
<td>Cisco TelePresence System 500, 1000, 3000, TX9000 Series.</td>
</tr>
<tr>
<td>Cisco Unified CM <em>intracluster and intercluster sessions</em></td>
<td>Ad hoc, Scheduled Static</td>
<td>Multipoint</td>
<td>Cisco TelePresence System 500, 1000, 3000, TX9000 Series, and CTMS.</td>
</tr>
<tr>
<td><em>Cisco VCS intracluster and intercluster sessions</em></td>
<td>Ad hoc, Scheduled</td>
<td>Point-to-point</td>
<td>Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20, Cisco Cius, and Cisco Jabber. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.</td>
</tr>
<tr>
<td>Session Classification</td>
<td>Session Type</td>
<td>Session Structure</td>
<td>Session Topology Elements</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco VCS <em>intracluster</em> and <em>intercluster</em> sessions (with MCU)</td>
<td>Ad hoc, Scheduled Permanent (displayed as static)</td>
<td>Multipoint</td>
<td>Cisco C series, EX Series, Cisco MCU, Cisco MSE(^2), or Cisco TelePresence Server. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.</td>
</tr>
<tr>
<td>Cisco VCS <em>intracluster</em> and <em>intercluster</em> sessions (without MCU)</td>
<td>Ad hoc, Scheduled</td>
<td>Multisite</td>
<td>Cisco C series, EX Series, Cisco MX, Cisco MXP Series, Cisco IP Video Phone E20. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.</td>
</tr>
</tbody>
</table>
| Sessions between Cisco Unified CM and Cisco VCS clusters\(^2\) | Ad hoc                | Point-to-point Multipoint | • 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) *intracluster* sessions\(^3\) | Ad hoc                | Point-to-point    | • Cisco C series, EX Series, Cisco MX series  
• Cisco TelePresence System 500, 1000, 3000, and TX9000 Series  
• IX 5000 series TelePresence endpoints |
<table>
<thead>
<tr>
<th>Session Classification</th>
<th>Session Type</th>
<th>Session Structure</th>
<th>Session Topology Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CM (8.6(1), 8.6(2), and 9.0) <strong>intracluster sessions</strong></td>
<td>Ad hoc, Scheduled</td>
<td>Multipoint</td>
<td>•Cisco C series, EX Series, Cisco MX series, Cisco IP Video Phone E20</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Scheduler must be</td>
<td></td>
<td>•Cisco TelePresence System 500, 1000, 3000, and TX9000 Series</td>
</tr>
<tr>
<td></td>
<td>CTS-Manager 1.7, 1.8, or 1.9.</td>
<td></td>
<td>•CTMS 1.8 or Cisco TelePresence Server</td>
</tr>
<tr>
<td>Sessions outside the enterprise firewall - Cisco VCS Expressway</td>
<td>Ad hoc Permanent (displayed as static)</td>
<td>Point-to-point, Multipoint, Multisite</td>
<td>•Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>•Cisco MCU or Cisco TelePresence Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>•Cisco VCS Control and Cisco VCS Expressway</td>
</tr>
<tr>
<td>Endpoints in a call (with an MCU in the call) work as a conferencing bridge in Cisco Unified CM.</td>
<td>Ad hoc</td>
<td>Point-to-point</td>
<td>Multipoint conferencing devices and video endpoints.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When a call is put in a</td>
<td>For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>conference mode or when</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>merged with another call,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>it becomes Multipoint.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The session does not show</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the MCU. When the first</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>participant leaves the call,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the session shows it is</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>connected to the MCU, while</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the second and third</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>participants continue in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the same call as a point-to-point call.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This scenario is</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>applicable when in-built</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>video bridge capability is</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>not present in the endpoint.</td>
<td></td>
</tr>
</tbody>
</table>
### Session Classification

| Sessions between MRA endpoints- Cisco Jabber or Cisco TelePresence MX Series or Cisco TelePresence System EX Series or Cisco TelePresence SX Series | Ad hoc, Scheduled | Point-to-point, Multipoint, Multisite | Cisco Jabber, Cisco TelePresence MX Series, Cisco TelePresence System EX Series, and Cisco TelePresence SX Series |

### Session Structure

- Cisco Prime Collaboration does not monitor a Multisite session where an MRA endpoint acts as a conference bridge.

### Session Topology Elements

#### Note

1. The codian software must be running on Cisco MSE.
2. This scenario is supported on CTS 1.7.4, and TC 4.1 to 7.0.
3. The troubleshooting workflow is supported on TC 4.2, 5.0, and above.

---

**Note**

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

---

The following image describes the session topology between two MRA endpoints.

**Figure 5: Session Topology Between MRA Endpoints**

1, 5

MRA endpoints that connect with each other through cloud server.

**Note**

You cannot view the session statistics for MRA endpoints.
Internet cloud servers that connect the MRA endpoints. The MRA endpoints can connect only with the help of cloud servers. You cannot view the session statistics since the system cannot get the IP addresses of the endpoints from the cloud servers.

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 sessions involving MRA endpoints and VCS Expressway Core are as follows:

- **Point-to-point**: Session between two MRA endpoints that are connected with each other through cloud servers and Cisco VCS Expressway Core
- **Multipoint**: Session with more than two MRA endpoints that are connected through cloud servers, Cisco VCS Expressway Core, and TPS or MCU
- **Multisite**: Session with more than two MRA endpoints that are connected without TPS or MCU

Each of the above sessions may also have one non-MRA endpoint connected at either end.

### Table 42: Session Scenarios for MSP Mode

<table>
<thead>
<tr>
<th>Session Classification</th>
<th>Session Type</th>
<th>Session Structure</th>
<th>Session Topology Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTX</td>
<td>Meet Me Rendezvous</td>
<td>Multipoint</td>
<td>Multipoint conferencing devices and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
<tr>
<td>CTX</td>
<td>Meet Me Rendezvous</td>
<td>Multipoint</td>
<td>Multipoint conferencing devices and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
<tr>
<td>Optional - CTX</td>
<td>Ad hoc</td>
<td>Point-to-point</td>
<td>Video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
</tbody>
</table>
### Session Classification | Session Type | Session Structure | Session Topology Elements
--- | --- | --- | ---
Optional - CTX Including Inter-company calls made using Session Border Controller with or without CTX. | Ad hoc | Point-to-point | Session Border Controller (SBC) and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.

Customer calls in a NAT environment. | Ad hoc | Point-to-point | Session Border Controller (SBC) and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.

---

**Table 43: Session Scenarios for MSP Mode**

<table>
<thead>
<tr>
<th>Session Classification</th>
<th>Session Type</th>
<th>Session Structure</th>
<th>Session Topology Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer calls in a NAT environment.</td>
<td>Ad hoc</td>
<td>Point-to-point</td>
<td>Session Border Controller (SBC) and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
</tbody>
</table>

---

**Note**

The following features related to session monitoring or troubleshooting in MSP mode are not supported:

- Session monitoring and troubleshooting of TPS cascaded calls over Cisco TelePresence Conductor
- MRA Multipoint calls and Multisite calls with MCU and CTX devices over Cisco TelePresence Conductor (Other MRA calls are supported)
- Cascading of MCU sessions over Cisco TelePresence Conductor

---

**Session Diagnostics Dashboard**

To access the Session Diagnostic dashboard, choose **Diagnose > Session Diagnostics.**

The Session Diagnostic dashboard provides details on a session and the endpoints that are involved in that session. In addition to monitoring the session, you can troubleshoot and identify faults in the network segment.
You can monitor sessions based on device type, by selecting the desired group from the Group drop-down filter. You can further filter based on the session type using the Show filter in the Video Collaboration Sessions pane.

By default, the All Video Collaboration Sessions table contains information for the current date (24 hours). You can view sessions for the last 30 days. Rest your mouse pointer over the Import Sessions button to see details of when the data was last imported into the Cisco Prime Collaboration database.

You can select a session, and click the Troubleshoot icon to launch the Session Troubleshooting page for that session.

The following image shows the Session Diagnostics Dashboard.

Figure 6: Session Diagnostics Dashboard

1 Predefined Group filter drop-down list. Also includes a launch point for a calendar. By default, the All Video Collaboration Sessions table contains information for the current date (24 hours). You can view sessions for the past 30 days and the next 3 days.

2 Quick summary pane for alarms and sessions.

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 Sessions

5 Count for total number of in-progress sessions (normal and alarmed) and in-progress alarmed sessions for the specified date.

6 Session topology pane.
Monitor Sessions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Session statistics pane.</td>
</tr>
<tr>
<td>8</td>
<td>Endpoint statistics pane. This pane contains details on peripherals, system, and sessions.</td>
</tr>
<tr>
<td>9</td>
<td>Launch point for the import session task. Rest your mouse pointer over the Import Sessions button to see details on when the data was last imported into the Cisco Prime Collaboration database.</td>
</tr>
</tbody>
</table>

The summary pane displays the session 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 Sessions 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 session (Diagnose > Session Diagnostics) with the preceding endpoint(s). In the Session Statistics pane, the DSCP In field displays the DSCP value received from the endpoint in the session.

**Note**

For Cisco Unified IP Phones 8941 and 8945, you can view the DSCP values only if the MSI Highgate feature is enabled for these phones.

The Video Collaboration Sessions table displays the details of in-progress sessions for the current date (00:00:00 hours to 23:59:59 hours). The latest session 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 session details.

Cisco Prime Collaboration keeps session details for the last 30 days.

You can get session statistics between audio-only IP Phones or Software Clients. If there are any alarms for the session, you can cross launch from the Alarms page to the Session Troubleshooting page and see the session statistics and trigger a path trace. Even after the alarm is cleared, you can cross launch to the troubleshooting page, to see the session information, session topology, and troubleshooting status. You cannot perform path assessment for these sessions. These sessions do not appear in the Session Diagnostics Dashboard.

Apart from video collaboration sessions, you can see sessions between an IP Phone or Software Client and TelePresence Endpoint in the Session 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. You can cross launch to the Session Troubleshooting page and see the session statistics and trigger a path trace.

If you have deployed Cisco Prime Collaboration in MSP mode, you see the In-progress sessions shown as Ad Hoc Sessions when the call was scheduled in TMS or CTS MAN was made by selecting MCU as a conferencing device.

If you have deployed Cisco Prime Collaboration in MSP mode, you see the details of a point-to-point call between two customers (through phones registered to different Unified CMs) using Session Border Controller(s). Ensure that the Session 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 Session Diagnostics page (Diagnose > Session Diagnostics).
Prerequisite - The Multipoint Control Unit (MCU) and endpoints must be in a Managed state in Cisco Prime Collaboration.

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 session 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 session topology does not display the MCU.

When the Multipoint Control Unit (MCU) is in Suspended state in Cisco Prime Collaboration and a conference is made, instead of a single ad hoc call, Cisco Prime Collaboration 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 Sessions

This feature enables you to monitor sessions 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.
- 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).

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 Session topology pane on the Session Diagnostics page (Diagnose > Session Diagnostics).

Cascading of Cisco TelePresence Server

This feature allows you to monitor Cisco TelePresence servers during ad hoc conference calls on the Session Diagnostics page (Diagnose > Session Diagnostics).

Prerequisite -

- The Cisco TelePresence Server (TPS), Cisco TelePresence Conductor, and endpoints should be in a Managed state in Cisco Prime Collaboration.
- Ensure that you set the visibility of the devices to Full Visibility.

During an ad hoc session, 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 session topology creates link between the primary and secondary TPS servers with associated participants and displays all the cascaded TPS servers as conference bridges.
Session monitoring or troubleshooting of TPS cascaded calls over Cisco TelePresence Conductor is not supported in MSP mode.

Realtime Visibility of an Endpoint

The visibility feature for a managed endpoint determines to what level Cisco Prime Collaboration 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 session monitoring. Polling is performed only for devices that are configured for real-time full visibility and not all devices.

Cisco Prime Collaboration supports the following types of visibility:

- **Full Visibility**—Call detection using JTAPI/HTTP feedback and realtime monitoring information such as session statistics, session information, and troubleshooting is supported.

- **Limited Visibility**—Automatic call detection using JTAPI/HTTP feedback takes place, but realtime monitoring information such as session statistics, session information, and troubleshooting is not supported. Endpoints with limited visibility are indicated with a half-dimmed icon in the Session Topology.

- **Off**—Call detection using JTAPI/HTTP feedback and realtime monitoring information are not supported. These endpoints are displayed on the Session Monitoring page with a fully dimmed icon.

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

<table>
<thead>
<tr>
<th>Endpoint Type</th>
<th>Default Visibility</th>
<th>Maximum Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CTS 500, 1000, and 3000 Series</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>• Cisco Codec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco TelePresence SX20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco TelePresence MXP Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco IP Video Phone E20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco Jabber Video for TelePresence (Mov)</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>• Polycom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Cius</td>
<td>Off</td>
<td>Full</td>
</tr>
<tr>
<td>Cisco IP Phones (89xx, 99xx)</td>
<td>Off</td>
<td>Full</td>
</tr>
</tbody>
</table>
### Endpoint Type

<table>
<thead>
<tr>
<th>Endpoint Type</th>
<th>Default Visibility</th>
<th>Maximum Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Desktop Collaboration Experience DX650 and DX630</td>
<td>Off</td>
<td>Full</td>
</tr>
<tr>
<td>• Cisco SX80 and Cisco SX10</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>• Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco DX70 and DX80</td>
<td>Off</td>
<td>Full</td>
</tr>
<tr>
<td>MRA Endpoints:</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>• Cisco Jabber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco TelePresence MX Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco TelePresence System EX Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco TelePresence System SX Series</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There is full visibility (default and maximum) for Total Endpoints (except Polycom). 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 session, if visibility is Off for one endpoint and Limited or Full for the other, the endpoint with Off visibility is shown with a fully dimmed icon in the session topology.

For a Multipoint session, an endpoint with Off visibility is not displayed in the session topology.

For scheduled point-to-point or multipoint sessions, endpoints with Off visibility are shown with a fully dimmed icon in the session topology.

To view the visibility of an endpoint, choose **Device 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 **Device 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**.
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 session onward.

The visibility feature is applied on the Session Diagnostics page only. That is, even if you have set visibility to either Limited or Off, the endpoint is listed in the Endpoint Diagnostics and Device Inventory pages.

360° Session View

The 360° Session 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 features. To see the 360° session View for a session, rest your mouse pointer over the Session Subject column in the Video Collaboration Sessions table and click the 360° Session View icon.

The 360° Session 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, session 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 Device Inventory page to view the inventory details of the device by clicking the Device Name.

The following table lists the actions that you can perform in the 360° Session View:

**Table 44: Actions Performed in 360° Session View**

<table>
<thead>
<tr>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click the Troubleshoot Session icon to launch the Session Troubleshooting page for the selected session, where you can select the direction for troubleshooting.</td>
</tr>
<tr>
<td>Click the Add to Watch list icon to add a session to the watch list. It is enabled for scheduled and in-progress sessions.</td>
</tr>
<tr>
<td>If you have added an in-progress session to the watch list, the troubleshooting workflow starts immediately between endpoints for a point-to-point session and between an endpoint and a Multipoint Switch, for a multipoint session.</td>
</tr>
<tr>
<td>If you have added a scheduled session to the watch list, the troubleshooting workflow starts after the session starts.</td>
</tr>
<tr>
<td>If you have scheduled a recurring session, add each instance of the recurring session to the watch list. For example, if you have scheduled a recurring session for every day over 5 days, add the session to the watch list for every day (5 days).</td>
</tr>
<tr>
<td>To monitor troubleshooting, click the icon in the 360° Session View.</td>
</tr>
<tr>
<td>View the troubleshooting report. The link is displayed for a completed session only if you performed troubleshooting, either manually or automatically.</td>
</tr>
<tr>
<td>View the troubleshooting report. The link is displayed for a completed session only if you performed troubleshooting, either manually or automatically.</td>
</tr>
</tbody>
</table>
Click the See Alarms icon to launch the Alarm browser. The Alarm browser lists all alarms for the selected session (includes both session and endpoints alarms).

Click the Monitor Endpoint icon to launch the Endpoint Diagnostics page.

**Session Topology**

The session topology displays the endpoints that are part of a session. If it is a multipoint session, the conferencing devices are displayed along with the endpoints. Also, if the call is a traversal call, Cisco VCS is displayed.

To launch the session topology, select a session in the Video Collaboration Sessions 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 session topology.

*Figure 7: Session Topology*

<table>
<thead>
<tr>
<th>1</th>
<th>An endpoint with a limited visibility icon that participates in the session.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>A No-Show icon associated with an endpoint.</td>
</tr>
</tbody>
</table>
An endpoint with a major alarm that participates in the session. The problem is in peripheral devices.

An active link between an endpoint and a Multipoint Switch with a major alarm.

A Disconnect icon associated with an endpoint.

Unknown endpoint; an endpoint that is not currently managed in Cisco Prime Collaboration. The inventory details for these endpoints may not be available in the Cisco Prime Collaboration 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 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 sessions and between an endpoint and Multipoint Switch for multipoint sessions.

- **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 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 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 sessions. Also, the peripheral status and system information are available for the scheduled sessions.

This page displays information on the peripheral status, endpoint system details, session details, and session statistics for a selected endpoint in the session topology pane.

In a Multisite session, the session statistics (audio and video) and session information are displayed for each connected endpoint when the center endpoint (conferencing device) is selected.

---

**Note**

Session statistics details (present and past) are not displayed for Cisco Cius and Cisco IP Phones.

---

## Session Statistics

The Session 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 **Assurance 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 sessions, Cisco Prime Collaboration does not display the threshold value or alarm badge-in session statistics.

All session and endpoint statistics data older than one day are purged.
PART VI

Dashboards and Reports

- Cisco Prime Collaboration Dashboards, page 235
- Cisco Prime Collaboration Reports, page 283
Cisco Prime Collaboration Dashboards

The Cisco Prime Collaboration 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 data to be populated in the dashboards, you must complete the following tasks:

- Discover the devices
- Import the sessions (for Session-related dashboards)
- Poll the devices

The following table describes the Cisco Prime Collaboration dashboards.

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
<th>Cisco Prime Collaboration Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Experience (Monitor &gt; System View &gt; Service Experience)</td>
<td>Information about quality of service.</td>
<td>Cisco Prime Collaboration Assurance Advanced</td>
</tr>
</tbody>
</table>
If you have deployed Cisco Prime Collaboration in MSP mode, you can view the following dashboards from the Cisco Prime Collaboration home page:

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
<th>Cisco Prime Collaboration Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Center Topology (Monitor &gt; System View &gt; Contact Center Topology)</td>
<td>Information about Unified Contact Center Topology View.</td>
<td>Cisco Prime Collaboration Contact Center Assurance</td>
</tr>
</tbody>
</table>

If CTX devices not managed, no data is populated in any of the dashlets.

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 depending on the licenses you have) in Cisco Prime Collaboration 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 weeks—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 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.

Prerequisites:

- The cluster must be discovered in Cisco Prime Collaboration 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.

<table>
<thead>
<tr>
<th>You can use the treemap view to…</th>
<th>You can use the list view to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 &amp; Events page.</td>
<td>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 &amp; Events page.</td>
</tr>
<tr>
<td><strong>Note</strong> 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).</td>
<td></td>
</tr>
<tr>
<td>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. 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.</td>
<td>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. The CTI Ports and CTI Route Points device types are displayed by default.</td>
</tr>
</tbody>
</table>
You can use the treemap view to… | You can use the list view to …
---|---
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:

<table>
<thead>
<tr>
<th>For severity…</th>
<th>The color displayed is…</th>
<th>If there are…</th>
</tr>
</thead>
</table>
| Critical | Red | • One or more critical alarms in the cluster.  
Or  
• More than or equal to 10% Unregistered hard endpoints.  
Or  
• |

**Note**  
When the Red color is displayed, Ops View displays the hard and soft Unregistered endpoint count separately.
<table>
<thead>
<tr>
<th>For severity…</th>
<th>The color displayed is…</th>
<th>If there are…</th>
</tr>
</thead>
</table>
| Major         | Orange                 | • One or more major alarms in the cluster.  
Or  
• Less than 10% Unregistered hard endpoints.  
Or  
• When the Orange color is displayed, Ops View displays the hard and soft Unregistered endpoint count separately. |
| Minor/Warning | Yellow                 | • One or more minor/warning alarms in the cluster.  
Or  
• Any device in the Registered with BackUp state.  
Or  
• |
| Normal        | Green                  | • No critical, major, or minor alarms.  
Or  
• All devices are in the registered or unknown state.  
Or  
• Or  
• |

**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.

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.

**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. 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.

---

**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.
- The Unified CM publisher should be in Managed state.
- The cluster should be discovered in Cisco Prime Collaboration.

---

**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.

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:

<table>
<thead>
<tr>
<th>Unified CM Cluster</th>
<th>VCS Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Cluster Name</td>
</tr>
<tr>
<td>Unified CM</td>
<td>VCS</td>
</tr>
<tr>
<td>Endpoints</td>
<td>Endpoints</td>
</tr>
<tr>
<td>Unknown Devices</td>
<td>Cisco TelePresence Management Suite (TMS)</td>
</tr>
<tr>
<td>Application Servers</td>
<td>Cisco TelePresence Conductor</td>
</tr>
<tr>
<td>Gateways (H323, MGCP, and SIP)</td>
<td>Cisco TelePresence Server</td>
</tr>
<tr>
<td></td>
<td>Cisco Multipoint Control Unit</td>
</tr>
<tr>
<td>Cisco TelePresence Manager</td>
<td>-</td>
</tr>
<tr>
<td>Cisco IM and Presence</td>
<td>-</td>
</tr>
<tr>
<td>Cisco TelePresence Conductor</td>
<td>-</td>
</tr>
<tr>
<td>Cisco TelePresence Server</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Multipoint Control Unit</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unity Connection</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unified Border Element</td>
<td>-</td>
</tr>
<tr>
<td>Cisco TelePresence Multipoint Switch</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unified MeetingPlace</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unified MeetingPlace Express</td>
<td>-</td>
</tr>
<tr>
<td>Cisco MediaSense</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unified Customer Voice Portal</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Emergency Responder</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unity Express</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unified Contact Center Express</td>
<td>-</td>
</tr>
<tr>
<td>Cisco Unified Contact Center Enterprise</td>
<td>-</td>
</tr>
</tbody>
</table>
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.
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 **Perform Device Search**, on page 155.

**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, and CIUS), 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.
- The cluster should be discovered in Cisco Prime Collaboration.

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 blue.

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 Health 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 and displays the device as **Down**. To view the list of events, see the Service Availability Summary Events wiki page. For event description and device type, see the Supported Alarms and Events for 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.

---

**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**
- **Session 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.

---

**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.

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 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 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

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 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. For example, if three Cisco Unified Communications Manager clusters are added in Cisco Prime Collaboration, 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 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 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
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.

**Session with Alarms**
Displays the number of in-progress sessions with alarms.
You can launch the 360° Session 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.
It contains the following dashlets:

**Top 10 Impacted 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**
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 Device 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.
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, conductor bridge pool utilization, TelePresence endpoints utilization, and license usage.

Trunk Utilization

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 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 45: Utilization Report for SIP Trunk Types

<table>
<thead>
<tr>
<th>SIP Trunk Type</th>
<th>Utilization Report</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercluster Trunks</td>
<td>CDR</td>
<td>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.</td>
</tr>
<tr>
<td>SIP trunk connected to Cisco Unified Border Element (CUBE)</td>
<td>Polling the CUBE directly</td>
<td>Available</td>
</tr>
</tbody>
</table>
SIP Trunk Type | Utilization Report
--- | ---
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 supports utilization only for the SIP trunks that are connected to Cisco Unified Border Element (CUBE). Cisco Prime Collaboration does not support utilization for SIP trunks that are configured in Unified Communications Manager.

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.

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.

Note
Even if trunks are associated to the route group, if polling does not happen then No Data Available error 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.

Cisco Prime Collaboration 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.

**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 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, and Media Switching status (for Cisco TelePresence Multipoint Switch only).
  - 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. 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 column 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. For example, the graph enables you to view data for 7 days by default.

  Note  
  Cisco Prime Collaboration 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. Polycom is included in these reports.

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 session.

  • 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 x 60).

  • By session—The utilization is by number of session. Here, only completed session are considered. If the number of session is one, the value of the x-axis is displayed in decimals (0.2, 0.4...). If the number of session 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 Session 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 session.

You can click on the bar chart to launch the No Show Session 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 session.

- 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 session—The utilization is by number of session. Here, only completed session are considered. If the number of session is one, the value of the x-axis is displayed in decimals (0.2, 0.4...). If the number of session 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 Session 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 Session
Displays the number of in-progress and completed session. Click on the chart to launch the Session Detail report for a particular session.
The Session data is aggregated for every two hours. For example, on a day, assume that you had only two session. The first session started at 01:00 hours and ended at 03:00 hours, and the second session 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 session from 01:00 to 03:00 is displayed between 0:00 and 02:00 hours.
- 4:00—2; a completed session from 01:00 to 03:00 and an in-progress session from 02:20 to 05:50 are displayed between 02:00 and 04:00 hours.
- 6:00—1; a completed session from 02:20 to 05:50 is displayed between 04:00 and 06:00 hours.
- 8:00—Zero; no session occurred between 06:00 and 08:00 hours.
- 10:00—Zero
- 12:00—Zero
- ...
- 24:00—Zero; no session 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 258
- Contact Center Enterprise License Usage, on page 259

Prime License Manager

You can see the following details:

- License Type—Displays the different types of licenses available, such as, CUWLPremium, CUWStandard, 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.

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.

### TelePresence Exchange Dashboard

This dashboard is displayed in the MSP mode. It provides information about cluster node, call and session control devices, conferencing devices, and region summary. It contains the following dashlets:

<table>
<thead>
<tr>
<th>Dashlet Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster-node Health Summary</td>
<td>Displays the list of nodes that are part of the CTX. It also gives the status of the nodes. You can see the following details:</td>
</tr>
<tr>
<td></td>
<td>• Alarm Severity</td>
</tr>
<tr>
<td></td>
<td>• Node Name</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• Node Type</td>
</tr>
<tr>
<td></td>
<td>• Cluster</td>
</tr>
<tr>
<td>Call and Session Control Devices</td>
<td>Displays the call and session control device in your network. You can see the following details:</td>
</tr>
<tr>
<td></td>
<td>• Alarm Severity</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
<tr>
<td></td>
<td>• Region</td>
</tr>
<tr>
<td></td>
<td>• Call Setup Failure</td>
</tr>
<tr>
<td></td>
<td>• Unavailable Duration</td>
</tr>
<tr>
<td></td>
<td>Rest your mouse pointer over the Name column and click the quick view icon to view the Device Type summary and Region Summary.</td>
</tr>
</tbody>
</table>
### Conference Devices

Displays the conferencing devices in your network. You can see the following details:

- Alarm Severity
- Name
- IP Address
- Type
- Region
- Resource Group
- Allocation Failures
- Resource Used

Rest your mouse pointer over the Name column and click the quick view icon to view the Device Type summary and Region Summary.

### Region Summary

This dashlet provides summary of resource usage, Call failures, Out of Resource failures for devices that belong to regions created in CTX. You can see the following details:

- Region
- Resource Used
- Call Failures
- Out of Resources Failures

Rest your mouse pointer over the Region column and click the quick view icon to view the IVR Resources and SIP Resources.

### 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 in MSP mode, you can view the following dashboards from the Cisco Prime Collaboration home page:

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Summary</td>
<td>Information about alarm, endpoints, and inventory aggregated per customer.</td>
</tr>
</tbody>
</table>
The Customer Summary dashboard provides information about alarm, endpoints, session alarms and inventory aggregated per customer. It contains the following dashlets:

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TelePresence Exchange</td>
<td>Information about cluster node, call and session control devices, region summary, and conferencing devices.</td>
</tr>
<tr>
<td>Note</td>
<td>If CTX devices are not managed, no data is populated in any of the dashlets.</td>
</tr>
</tbody>
</table>

### Alarm Summary
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:
- Customer
- Total
- Critical
- Major
- Minor
- Warnings

### Device Summary
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:
- Customer
- Total
- Managed
- Unmanaged
- Suspended
**Description**

Dashlet displays the list of endpoints for each category, based on the Registration status, per customer. You can see the following details:

- Customer
- Total -Registered
- Total -Unregistered
- Hard Endpoints -Registered
- Hard Endpoints -Unregistered
- Soft Clients -Registered
- Soft Clients -Unregistered

Sessions in Alarms displays the number of in-progress sessions with alarms. You can see the following details:

- Session Structure
- Session Type
- Watched Sessions
- Troubleshooting Status
- Session 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 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, 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 in Enterprise Mode, go to Monitor > System View > OpsView > Contact Center Topology.

If you have deployed Cisco Prime Collaboration in MSP mode, all devices that are managed by Cisco Prime Collaboration, 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 that are managed by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.

The following table lists the link status between devices in the Unified Contact Center:

<table>
<thead>
<tr>
<th>Device 1</th>
<th>Device 2</th>
<th>Link Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPCC</td>
<td>VRU PG</td>
<td>Yes</td>
</tr>
<tr>
<td>IPCC</td>
<td>Agent PG</td>
<td>Yes</td>
</tr>
<tr>
<td>VRU PG</td>
<td>CVP Call Server</td>
<td>Yes</td>
</tr>
<tr>
<td>CVP</td>
<td>VXML Gateway</td>
<td>No</td>
</tr>
<tr>
<td>Agent PG</td>
<td>CUCM</td>
<td>Yes</td>
</tr>
<tr>
<td>CUCM</td>
<td>Media Sense</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent PG</td>
<td>Finesse</td>
<td>Yes</td>
</tr>
<tr>
<td>AW/HDS</td>
<td>CUIC</td>
<td>Yes</td>
</tr>
<tr>
<td>UCCE Router</td>
<td>Public Cloud</td>
<td>Yes</td>
</tr>
<tr>
<td>UCCE Router</td>
<td>Private Cloud</td>
<td>Yes</td>
</tr>
<tr>
<td>UCCE Router</td>
<td>CTI</td>
<td>Yes</td>
</tr>
<tr>
<td>CTI</td>
<td>CTIOS</td>
<td>Yes</td>
</tr>
<tr>
<td>UCCE Router</td>
<td>MR PG</td>
<td>Yes</td>
</tr>
<tr>
<td>VRU PG</td>
<td>CVP Reporting Server</td>
<td>No</td>
</tr>
<tr>
<td>UCCE Router</td>
<td>Logger</td>
<td>No</td>
</tr>
<tr>
<td>UCCE Router</td>
<td>AW/HDS</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 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 to 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 purge operation.

If you have deployed Cisco Prime Collaboration 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 in the MSP mode, topology view is not supported in cases where you manage both shared (4K Shared Contact Center) and dedicated deployment models.
- The topology view is automatically refreshed every two minutes.
- Cisco Prime Collaboration supports single Unified CCE enterprise deployment only.
- Expand/collapse icons are available for abstract devices only.

### Performance Dashboards

Performance page displays system-defined dashboards based on the performance counters.

**Note**

- You can monitor only one cluster per product for a single installation of Cisco Prime Collaboration—Standard.
- 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, to view performance dashboards for the selected cluster.

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.

If you have deployed Cisco Prime Collaboration in MSP mode, in the Cluster drop-down list, only those products and clusters which belong to a specific customer (that was selected from the Customer Summary page) are displayed.

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.

### Unified CM and Unity Connection

The following system-defined dashboards are available for Unified CM:
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 total number of calls completed. Also displays the delta of calls completed in the past 1 minute. It can have positive or negative values based on the calls completed in the past minute.

Calls Attempted

Displays the total number of calls completed. Also displays the delta of calls completed in the past 1 minute. It can have positive or negative values based on the calls attempted in the past minute.

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:
  \[
  \frac{(\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} + \text{Used Swap KBytes})}{(\text{Total KBytes} + \text{Total Swap KBytes})} \times 100
  \]

- 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 Total KBytes - 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 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.

TFTPs 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 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

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 RepTask 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

<table>
<thead>
<tr>
<th>Note</th>
<th>Run the CLI command <strong>utils dbreplication status</strong> to see if any tables are out of sync</th>
</tr>
</thead>
</table>

- 3 = Replication data transfer is bad in the cluster

<table>
<thead>
<tr>
<th>Note</th>
<th>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 <strong>utils dbreplication status</strong> find out where and what exactly is broken.</th>
</tr>
</thead>
</table>

- 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 Sessions**

The Number of Active JSM Sessions performance counter contains the number of client emulation sessions 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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern</td>
<td>Displays the name of the learned pattern from the remote call-control entity.</td>
</tr>
<tr>
<td>TimeStamp</td>
<td>Displays the date and time that the local Unified CM marked the pattern as</td>
</tr>
<tr>
<td></td>
<td>a learned pattern.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the learned pattern was reachable or unreachable.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Displays the protocol for the SAF-enabled trunk that was used for the</td>
</tr>
<tr>
<td></td>
<td>outgoing call to the learned pattern. If the remote call-control entity has</td>
</tr>
<tr>
<td></td>
<td>QSIG tunneling configured for the SAF-enabled trunk, the data indicates</td>
</tr>
<tr>
<td></td>
<td>that QSIG tunneling was used; for example, EMCA is listed along with H.323</td>
</tr>
<tr>
<td></td>
<td>in this column.</td>
</tr>
<tr>
<td>AgentID</td>
<td>Displays the name of the remote call-control entity that advertised the</td>
</tr>
<tr>
<td></td>
<td>learned pattern.</td>
</tr>
</tbody>
</table>
### Column

<table>
<thead>
<tr>
<th>Description</th>
<th>Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>IP Address</td>
</tr>
<tr>
<td>Displays the PSTN failover configuration for the learned pattern.</td>
<td>ToDID</td>
</tr>
<tr>
<td>Displays the ID from the local Unified CM node.</td>
<td>CUCMNodeId</td>
</tr>
</tbody>
</table>

### 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 they system has too many or too few ports. The Port Monitor displays the information for each port as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name</td>
<td>The display name of the port in Cisco Unity Connection Administration.</td>
</tr>
<tr>
<td>Caller</td>
<td>For incoming calls, the phone number of the caller.</td>
</tr>
<tr>
<td>Called</td>
<td>For incoming calls, the phone number that was dialed.</td>
</tr>
<tr>
<td>Reason</td>
<td>If applicable, the reason why the call was redirected.</td>
</tr>
<tr>
<td>Redir</td>
<td>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.</td>
</tr>
<tr>
<td>Last Redir</td>
<td>The last extension that redirected the call.</td>
</tr>
<tr>
<td>Application Status</td>
<td>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.</td>
</tr>
<tr>
<td>Display Status</td>
<td>The action that the conversation is currently performing. When the port is not handling a call, the status appears as Idle.</td>
</tr>
<tr>
<td>Conversation Status</td>
<td>Specific details about the action that the conversation is performing. When the port is not handling a call, the status appears as Idle.</td>
</tr>
<tr>
<td>Port Ext</td>
<td>The extension of the port.</td>
</tr>
<tr>
<td>Connected To</td>
<td>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.</td>
</tr>
</tbody>
</table>
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. 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.

**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**

You can add customized dashboards in the home page (**Monitor > System View > 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.
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 the Purge Policies chapter in 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.

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.

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:

**Procedure**

1. **Step 1** Choose the product and the cluster from the Cluster or Device drop-down list.
2. **Step 2** Click the + button adjacent to the Dashboard drop-down list.
3. **Step 3** On the Custom Dashboard page, enter the dashboard name, select the polling interval, view, and server. 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 stating that the historical trend data is lost is displayed, 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.

4. **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.

5. **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.

6. **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 *Create Custom Events in Cisco Prime Collaboration Assurance Guide - Advanced*. When you create custom events from the custom dashboards, you need not provide the cluster details.

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:

**Procedure**

1. **Step 1** Click the “Settings” icon on the top-right corner of the home page, and then click **Add New Dashboard**.
2. **Step 2** Enter a name in the box provided, and click **Apply**.
3. **Step 3** Click **Add Dashlet(s)**.
4. **Step 4** Click **Add** adjacent to the dashlets you want to add.

**Note** For Cisco Prime Collaboration Assurance - Advanced mode—if your endpoints or devices are configured with a common prefix names, you can shorten the display name using the Dashlet Label Prefix Removal setup in the General Settings page.
Cisco Prime Collaboration Reports

- Prerequisites to Generate the Cisco Prime Collaboration Reports, page 283
- Update CDR Data Source Credentials, page 284
- Call Classification, page 286
- Configure SFTP Settings, page 295
- Administrative Reports, page 296
- CDR & CMR Call Report, page 297
- NAM & Sensor Report, page 307
- Session Reports, page 316
- TelePresence Endpoint Reports, page 317
- Launch CUCM Reports, page 318
- Miscellaneous Reports, page 318
- Scheduled Reports, page 327
- Access Data for Reports that Contain More than 2,000 Records, page 328
- Troubleshoot File Download Issues, page 329

Prerequisites to Generate the Cisco Prime Collaboration Reports

You can use the Cisco Prime Collaboration 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 CDR Data Source 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.
Switches that are connected to Cisco 1040 sensors must be in managed state in Cisco Prime Collaboration Assurance.

Cisco Prime Collaboration Assurance must be added as billing server in Unified CM.

Update CDR Data Source Credentials

Cisco Prime Collaboration collects SCS (number of seconds where loss is greater than 5%) from Cisco Unified CM clusters, Cisco 1040 Sensors, and Cisco Prime Network Analysis Module (Prime NAM) 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 1040 sensor monitors the active RTP streams between IP phones and calculates the MOS using the ITU G107 R-factor algorithm. The sensor then forwards the MOS for each monitored stream every 60 seconds to Cisco Prime Collaboration.

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).

You need not provide the credentials for Cisco 1040 Sensors to enable data collection from them. However, for Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) and Cisco Unified CM publisher servers, you must:

• Keep the credentials up-to-date. (Any time you update credentials on a Cisco Prime Network Analysis Module (Prime NAM), or Cisco Prime Virtual Network Analysis Module (Prime vNAM) server, you must also update the corresponding credentials in Cisco Prime Collaboration.)

To update the credentials, choose Assurance Administration > CDR Source Settings > Manage Call Quality Data Sources.

Note: Add, Edit, Delete, and Import options are not applicable for NAM, if you have installed Cisco Prime Collaboration in MSP mode.

Add a Data Source Credential

To add a credential for Prime NAM server:

Procedure

Step 1 Choose CDR Source Settings > Manage Call Quality Data Sources.
Step 2 Click Add, and enter the required data.
Step 3 Click OK.
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.
Add Multiple Data Source Credentials

You can add multiple data source credentials, by importing a csv file with Prime NAMs details. The csv file should contain the following details for each Prime NAMs server:

- Display Name
- IPAddress
- Hostname
- Protocol
- UserName
- Password

To add credentials for multiple Prime NAMs:

Procedure

**Step 1** Choose Assurance Administration > CDR Source Settings > Manage Call Quality Data Sources.

**Step 2** Click Import.

**Step 3** In the Import dialog box, browse to the local csv file, and click Import.

**Step 4** Click the Refresh button for the credential details to reflect on the user interface.

Use Data Source Credentials to Troubleshoot Problems and Verify Credentials

Any problem that prevents Cisco Prime Collaboration from contacting and connecting to data sources can interrupt the collection and analysis of call data and configuration data. Use the information on the Data Source Management page to:

- Verify that credentials are valid and that Cisco Prime Collaboration is actively obtaining data.
- Troubleshoot if you notice potential problems with data source credential status or with reports (such as an unusual time gap).

Procedure

**Step 1** Obtain more information by clicking the status links on the Data Source Management page. The information that you obtain could explain the problem or indicate the need for troubleshooting.

**Step 2** Perform the following troubleshooting:
For a Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM)—Check whether the:
• Credentials on a Viewing Sensor Stream Correlation Data have changed; if so, update the credentials in Cisco Prime Collaboration.

• Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) is reachable; if not, take steps to ensure that the Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) is reachable.

For a Cisco Unified CM—Do the following:

• Confirm that the last successful contact Cisco Prime Collaboration had with the cluster was recent. When the last contact status is Success, in some cases, Cisco Prime Collaboration might not be receiving data, but simply waiting to receive data.

• Verify that credentials for the cluster on Cisco Unified CM match those in Cisco Prime Collaboration, and correct, if necessary.

• Verify that DNS parameters are specified correctly on the Cisco Prime Collaboration server and the Cisco Unified CM hostname has been added to DNS. (Cisco Prime Collaboration 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.

• Wait or take preventive action when the call data status shows that Cisco Prime Collaboration is discarding data. Cisco Prime Collaboration discards data when receiving old data from Unified CM 6.x and later. This can happen after the connection between Cisco Prime Collaboration and Cisco Unified CM is reestablished after a break. Cisco Unified CM first sends old files to Cisco Prime Collaboration.

• Credentials that Cisco Prime Collaboration 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.

Step 3 Verify the credentials:

a) Choose Assurance Administration > CDR Source Settings > Manage Call Quality Data Sources.

b) Select the data source for which you want to verify credentials.

c) Click Verify.

Call Classification

Cisco Prime Collaboration uses call classification to categorize calls in Call Detail Record (CDR) reports. Cisco Prime Collaboration 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)
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.

<table>
<thead>
<tr>
<th>Category Type</th>
<th>Description</th>
<th>Category Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voicemail</td>
<td>Calls to or from voicemail.</td>
<td>Unity Voicemail—Calls that meet system-defined criteria for a voicemail call, such as calls to and from Cisco Unity and Cisco Unity Connection. &lt;br&gt;<strong>Note</strong> You can add user-defined category names to this category type.</td>
</tr>
<tr>
<td>Conference</td>
<td>Calls to or from a conferencing system.</td>
<td>Conference Bridge—Calls that meet system-defined criteria for a call involving a conference bridge. &lt;br&gt;<strong>Note</strong> You can add user-defined category names to this category type.</td>
</tr>
</tbody>
</table>
| ICT                      | Calls to or from an intercluster trunk (ICT).     | • ICT GK Controlled—ICT calls that are gatekeeper controlled.  
                              |                                                  | • ICT Non-GK Controlled—ICT calls that are not gatekeeper controlled. |
| VG/Trunk-Outgoing        | Calls to a voice gateway or a trunk; only OffNet calls are included. <br>**Note** User-defined dial plans are applied to calls in the VG/Trunk-Outgoing call category. | • 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.  
<pre><code>                          |                                                  | SIP Trunk Outgoing—Calls to a SIP trunk. |
</code></pre>
<table>
<thead>
<tr>
<th>Call Category</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>VG/Trunk-Incoming</td>
<td>Includes calls from a voice gateway or a trunk; only OffNet calls are included.</td>
<td>• MGCP Gateway Incoming—Calls from an MGCP voice gateway.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• H.323 Gateway Incoming—Calls from an H.323 voice gateway.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• H.323 Trunk Incoming—Calls from an H.323 trunk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Trunk Incoming—Calls from a SIP trunk.</td>
</tr>
<tr>
<td>Tandem</td>
<td>A tandem call occurs when both endpoints are voice gateways or trunks.</td>
<td>Tandem.</td>
</tr>
<tr>
<td>OnNet Trunk</td>
<td>Calls where one endpoint is a trunk and the call is not an OffNet call.</td>
<td>• OnNet H.323 Trunk.</td>
</tr>
<tr>
<td></td>
<td>For example, the trunk could be used to connect to WebEx or to a PBX.</td>
<td>• OnNet SIP Trunk.</td>
</tr>
<tr>
<td>Internal</td>
<td>Calls that do not fall into any of the above categories.</td>
<td>Internal.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>For system-related reasons, Prime Collaboration could not determine the device type of the endpoints.</td>
<td>Unknown.</td>
</tr>
</tbody>
</table>

Cisco Prime Collaboration 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 **Assurance Administration > CDR Analysis Settings**.

**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 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 update the call categories and 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.

To add a dial plan, choose **Administration > System Setup > Call Classification > Dial Plan Configuration**. Assurance Administration > CDR Analysis Settings > Dial Plan Assignment.

To assign a dial plan, choose **Assurance 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:

- Define your own call category names; however, you must select from the available call category types
- 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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>No. of Chars</th>
<th>Default Pattern</th>
<th>Call Category Name</th>
<th>Call Category Type</th>
<th>Explanation</th>
<th>Priority</th>
</tr>
</thead>
</table>

Cisco Prime Collaboration Assurance Guide - Advanced, 11.0
If the number of digits dialed is greater than 3 and starts with 011, the call is classified as International.

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.

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.
<p>| =   | 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), 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 |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11</td>
<td>T!</td>
<td>Toll Free</td>
<td>Toll Free</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>11</th>
<th>XG!</th>
<th>Local</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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), the call is classified as Local.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

Cisco Prime Collaboration 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 Pattern to a Dial Plan**

You can add a dial pattern to a dial plan that you want to add or edit.

**Procedure**

**Step 1** Choose **Assurance Administration > CDR Analysis Settings > Dial Plan Configuration**. Click **Add**. The **Add Dial Pattern** dialog box is displayed.

**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 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).

• 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.

**Step 3** Click OK.

---

**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.

<table>
<thead>
<tr>
<th>Cisco Prime Collaboration Applies Dial Patterns of This Category Type...</th>
<th>To the Directory Number that is the...</th>
<th>In a Call That Is in This System-Defined Category...</th>
</tr>
</thead>
</table>
| • Conference  
• Emergency  
• International  
• Local  
• Long Distance  
• Service  
• Toll Free  
• Voicemail | Destination | VG/Trunk-Outgoing |
| • Conference  
• Voicemail | Source |  |
| • Conference  
• Voicemail | • Source  
• Destination | • Internal  
• OnNet Trunk |

**Configure Gateway Codes**

Cisco Prime Collaboration uses the gateway codes that you configure to determine the call classification for an external call.
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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Assurance Administration</strong> &gt; <strong>CDR Analysis Settings</strong> &gt; <strong>Gateway Code Configuration</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Gateway Code Summary page, select a cluster and click <strong>Manage Gateway Code</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the gateway code, and then click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

**Configure SFTP Settings**

If you are using Unified Communications Manager to monitor calls, you must configure SFTP settings.

To configure SFTP settings:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Assurance Administration</strong> &gt; <strong>CDR Source Settings</strong> &gt; <strong>CUCM SFTP Credentials</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter the required information. For field descriptions, see the table for SFTP Settings Page - Field Descriptions.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Apply</strong>. A popup window is displayed to confirm whether you want to update the SFTP password across all Unified Communications Manager systems.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>

**SFTP Settings Page - Field Descriptions**

The following table describes the fields in the SFTP Settings page.

**Table 46: SFTP Settings Page - Field Descriptions**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low-Volume Schedule Hours</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Administrative Reports

The following administrative reports are available:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Status Report</td>
<td>Provides information about failed processes, data purging, notifications, phone licensing, and system limits.</td>
</tr>
<tr>
<td></td>
<td>It provides information about synthetic, phone status, and IP SLA Voice tests for the following test results only:</td>
</tr>
<tr>
<td></td>
<td>• Synthetic test: If the test failed to run because of High CPU Utilization in the Cisco Prime Collaboration server.</td>
</tr>
<tr>
<td></td>
<td>• Phone Status test: If the SAA source device is not reachable.</td>
</tr>
<tr>
<td></td>
<td>• IP SLA Voice Test:</td>
</tr>
<tr>
<td></td>
<td>• If the configuration is incorrect.</td>
</tr>
<tr>
<td></td>
<td>• If the device has low memory.</td>
</tr>
<tr>
<td></td>
<td>• If the source device is not responding.</td>
</tr>
<tr>
<td></td>
<td>• If the device has rebooted.</td>
</tr>
<tr>
<td></td>
<td>For the following parameters of System Limits:</td>
</tr>
<tr>
<td></td>
<td>• Port - Ethernet ports are categorized under this parameter.</td>
</tr>
<tr>
<td></td>
<td>• Interfaces - Voice interfaces are categorized under this parameter.</td>
</tr>
</tbody>
</table>
CDR & CMR Call Report

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).

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade</td>
<td>Based on voice call grade settings. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Good—The call value is less than the threshold value of long call SCSR (%)</td>
</tr>
<tr>
<td></td>
<td>or short call SCSR (%). The value of this grade appears in green color.</td>
</tr>
<tr>
<td></td>
<td>• Acceptable—The call value is greater than or equal to threshold value of</td>
</tr>
<tr>
<td></td>
<td>long call SCSR (%) or short call SCSR (%). The value of this grade</td>
</tr>
<tr>
<td></td>
<td>appears in orange color.</td>
</tr>
<tr>
<td></td>
<td>• Poor—The call value is greater than the threshold value of long call</td>
</tr>
<tr>
<td></td>
<td>SCSR (%) or short call SCSR (%). The value of this grade appears in red</td>
</tr>
<tr>
<td></td>
<td>color.</td>
</tr>
<tr>
<td></td>
<td>• N/A—The SCSR (%) value is not available or is negative.</td>
</tr>
<tr>
<td></td>
<td>• All—Select all the grade.</td>
</tr>
</tbody>
</table>

For more information see Overview of Voice Call Grade Settings

Cluster ID      | Unified Communications Manager cluster.                                       |
### Caller/Called

- **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

- **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

<table>
<thead>
<tr>
<th>One of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offnet</td>
</tr>
<tr>
<td>Onnet</td>
</tr>
</tbody>
</table>

**Note** For more information, see *Understand OffNet and OnNet Calls*, on page 288.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Period</td>
<td>Date and time that the call started with respect to the Cisco Prime Collaboration server local time zone (not the time zone in which Cisco Unified CM resides). The maximum time limit is 7 days.</td>
</tr>
<tr>
<td>Call Duration(s)</td>
<td>Length of the call, in seconds.</td>
</tr>
<tr>
<td>Call Category Names</td>
<td>A comma-separated list of the categories to which the call belongs. For more information, see <a href="#">Call Classification, on page 286</a> and <a href="#">Call Category Creation, on page 289</a></td>
</tr>
<tr>
<td>Call Category Types</td>
<td>A comma-separated list of the category types to which the call categories belongs. For more information see <a href="#">Call Classification, on page 286</a> and <a href="#">Call Category Creation, on page 289</a></td>
</tr>
</tbody>
</table>

The following table describes the fields of CMR reports.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOS</td>
<td>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.</td>
</tr>
<tr>
<td>Minimum MOS</td>
<td>The minimum MOS score within the sample duration. The value might be N/A or not available if the sample duration is very short.</td>
</tr>
<tr>
<td>Grade</td>
<td>Based on voice call grade settings. Select one of the following:</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• N/A—The SCSR (%) value is not available or is negative.</td>
</tr>
<tr>
<td></td>
<td>• All—Select all the grade.</td>
</tr>
<tr>
<td></td>
<td>For more information see Overview of Voice Call Grade Settings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Caller/Called</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Directory Number—Directory number where the call was made.</td>
</tr>
<tr>
<td></td>
<td>• Device Type—Type of device making the call.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• B-Channel—B-channel number of the MGCP gateway, or NA, if not applicable.</td>
</tr>
<tr>
<td></td>
<td>• Media IP—IP address where the call originated.</td>
</tr>
<tr>
<td></td>
<td>• Codec—Codec name.</td>
</tr>
<tr>
<td></td>
<td>• Media Port—Port through which the call originated.</td>
</tr>
<tr>
<td></td>
<td>• Device Pool—Device pool where the call originated.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Device Name—Name of the device.</td>
</tr>
<tr>
<td><strong>Listener DN/IP</strong></td>
<td><strong>Identifies the endpoint-called or caller-for which MOS and impairment details are reported; one of these:</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• IP address of the listener.</td>
</tr>
<tr>
<td></td>
<td>• Directory number of the listener.</td>
</tr>
<tr>
<td><strong>Jitter (ms)</strong></td>
<td><strong>Milliseconds of jitter during the sample duration.</strong></td>
</tr>
<tr>
<td><strong>Packet Loss</strong></td>
<td><strong>Number of packets lost due to network transmission during the sample duration.</strong></td>
</tr>
<tr>
<td></td>
<td>Computed based on observed RTP sequence number analysis.</td>
</tr>
<tr>
<td><strong>Max Jitter (ms)</strong></td>
<td><strong>Maximum milliseconds of jitter during the sample duration.</strong></td>
</tr>
<tr>
<td><strong>Conceal Seconds</strong></td>
<td><strong>Number of seconds that have concealment events (lost frames) from the start of the voice stream</strong></td>
</tr>
<tr>
<td></td>
<td>(includes severely conceal seconds).</td>
</tr>
<tr>
<td><strong>Severely Conceal Seconds</strong></td>
<td><strong>Number of seconds during which a significant amount of concealment (greater than fifty milliseconds) was observed.</strong></td>
</tr>
<tr>
<td><strong>Conceal Ratio</strong></td>
<td><strong>Ratio of concealment frames to total frames.</strong></td>
</tr>
<tr>
<td><strong>Latency</strong></td>
<td><strong>Delay</strong></td>
</tr>
<tr>
<td><strong>Cluster</strong></td>
<td><strong>Unified Communications Manager cluster.</strong></td>
</tr>
<tr>
<td><strong>Time Period</strong></td>
<td><strong>Date and time that the call started with respect to the Cisco Prime Collaboration server local time zone (not the time zone in which the Unified Communications Manager resides).</strong></td>
</tr>
<tr>
<td><strong>Call Duration(s)</strong></td>
<td><strong>Length of the call, in seconds.</strong></td>
</tr>
<tr>
<td><strong>Caller Termination Cause</strong></td>
<td><strong>String that describes why the call was terminated on the caller endpoint</strong></td>
</tr>
<tr>
<td><strong>Called Termination Cause</strong></td>
<td><strong>String that describes why the call was terminated on the called endpoint.</strong> See Call termination cause codes section in Cisco Unified Communications Manager Call Details Record Administration Guide for the cause codes for failed calls.</td>
</tr>
</tbody>
</table>
Endpoints Report contain video attributes (for video endpoints) such as:

- Video duration
- Video packets lost
- Video jitter
- Video round trip time
- Video RX Resolution
- Video RX Frames Lost

<table>
<thead>
<tr>
<th>Video attributes</th>
<th>Endpoints Report contain video attributes (for video endpoints) such as:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severely Conceal Seconds Ratio (%)</td>
<td>A metric to measure the voice quality. It is the ratio of Severely Conceal seconds(SCS) and total call duration.</td>
</tr>
<tr>
<td>Conceal Seconds Ratio (%)</td>
<td>A metric to measure the network quality. It is the ratio of Conceal seconds(CS) and total call duration.</td>
</tr>
</tbody>
</table>

All the columns may not appear in CDR & CMR reports by default. To view other fields, click settings button and choose columns.

Note:
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:

**Procedure**

**Step 1** Choose **Assurance Reports > CDR & CMR Reports**. The CDR & CMR Reports page is displayed.

**Step 2** Enter the information in the fields described below:

**Table 47:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Select CDR/CMR from the Display</td>
</tr>
<tr>
<td>Cluster</td>
<td>Select the Clusters from Cluster. The default value is All.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location/Devicepool</td>
<td>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.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Select the devices from Device Type. The default value is Any.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Select Directory Number or IP Address from the Endpoint. The default value is Directory Number.</td>
</tr>
<tr>
<td>Caller</td>
<td>Enter the Directory Number or Caller IP address. The default value of Directory Number is * and default value of IP address is <em>.</em>.<em>.</em>.</td>
</tr>
<tr>
<td></td>
<td>Directory Number can include any combination of alphanumeric characters and special characters like +,*, @, _, *, .</td>
</tr>
<tr>
<td></td>
<td>For Directory Number search, use uppercase X as a single-digit wildcard; use * as multiple-digit wildcard. For example 1100X or 11*.</td>
</tr>
<tr>
<td></td>
<td>For IP address search, the * wildcard applies to the entire octet. For example: 172.30.<em>.</em> or 2005:0420:2e00:0094:<em>:</em>:<em>:</em></td>
</tr>
<tr>
<td>Called</td>
<td>Enter the Directory Number or Called IP address. The default value of Directory Number is * and default value of IP address is <em>.</em>.<em>.</em>.</td>
</tr>
<tr>
<td></td>
<td>Directory Number can include any combination of alphanumeric characters and special characters like +,*, @, _, *, .</td>
</tr>
<tr>
<td></td>
<td>For Directory Number search, use uppercase X as a single-digit wildcard; use * as multiple-digit wildcard. For example 1100X or 11*.</td>
</tr>
<tr>
<td></td>
<td>For IP address search, the * wildcard applies to the entire octet. For example: 172.30.<em>.</em> or 2005:0420:2e00:0094:<em>:</em>:<em>:</em></td>
</tr>
<tr>
<td>Call Category</td>
<td>Select the name or type from the Call Category. The default value is Name.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Category Name/Type</td>
<td>Select the Category name or Category Type. The default value is All.</td>
</tr>
<tr>
<td>Grade</td>
<td>Select Good, Acceptable, Poor, All or N/A. The default value is All.</td>
</tr>
<tr>
<td>Jitter</td>
<td>Select the range from Jitter and enter the value in milliseconds. The default range is greater than or equal to zero.</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Select the range from Packet Loss and enter the value in the field. The default range is greater than or equal to zero.</td>
</tr>
<tr>
<td>Conceal Seconds</td>
<td>Select the range and enter the value in seconds field. The default range is greater than or equal to zero.</td>
</tr>
<tr>
<td>Conceal Ratio</td>
<td>Select the range from Conceal ratio and enter the value in the field. The default range is greater than or equal to zero.</td>
</tr>
<tr>
<td>Call Type</td>
<td>Select Audio, Video or Any. The default value is Any.</td>
</tr>
<tr>
<td>Call Class</td>
<td>Select On-Net, Off-Net, or Any. The default value is Any.</td>
</tr>
<tr>
<td>Call Duration</td>
<td>Select the value of call duration from Call Duration and enter the time in secs field. The default value is Any.</td>
</tr>
<tr>
<td>Termination Type</td>
<td>Select Success, Failed, or Any. The default value is Any.</td>
</tr>
<tr>
<td>Termination Cause Code</td>
<td>Select the cause code from Termination Cause Code. The default value is All.</td>
</tr>
</tbody>
</table>
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**: CDR records in older version has grades Unknown, No MOS, Short Call, but the user cannot see the same grades after upgrading to 11.0.

   **Recommended Action**: After upgrade to 11.0 the Unknown, No MOS, Short Call grades will change to N/A.

3 **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.

4 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.

5 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.

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 in MSP mode.

To generate NAM & Sensor report, choose Assurance Reports > NAM & Sensor Reports. Enter the values in required fields and click Generate Report.

The following table describes the fields of NAM & Sensor reports.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name  | Descriptive name for the sensor that collected the data and analyzed the MOS.  
  Note The name Cisco 1040 + < last 6 digits from MAC address > identifies a Cisco 1040 that automatically registered with Cisco Prime Collaboration. |
| 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 | Directory Number—Displayed when the device is managed by a Unified Communications Manager that:
  • Is added to Cisco Prime Collaboration with the proper credentials
  • Has not been suspended from monitoring.

| Device Type—Can provide the device type or one of these:
  • N/A—Some error prevents Cisco Prime Collaboration from obtaining the device type.
  • Unavailable—This is the first time Cisco Prime Collaboration has seen this phone and the device type is not yet known; or the corresponding Unified CM:
    • Has not been added to Cisco Prime Collaboration.
    • Did not provide a valid device type to Cisco Prime Collaboration.

| IPAddress | If an IP address is clickable, click it to launch the Detailed Device View page or Phone Detail window.

| UDP Port | Transport layer port that is the source of the media stream.

| Device Name | 

| Time | Time at which the sensor calculated MOS.

| TOS | Type of Service (TOS).

| 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. Click the value to open a Sensor Stream Correlation window.

<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Primary Degradation Cause</th>
<th>One of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Jitter</td>
</tr>
<tr>
<td></td>
<td>• Packet loss</td>
</tr>
<tr>
<td></td>
<td>• None—Jitter and packet loss values are both 0 (zero).</td>
</tr>
<tr>
<td></td>
<td>The value might be N/A or not available if the sample duration is very short.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grade</th>
<th>Based on voice call grade settings. Select one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Good—The call value is less than the threshold value of long call SCSR(%) or short call SCSR(%).</td>
</tr>
<tr>
<td></td>
<td>• Acceptable—The call value is greater than or equal to threshold value of long call SCSR(%) or short call SCSR(%).</td>
</tr>
<tr>
<td></td>
<td>• Poor—The call value is greater than the threshold value of long call SCSR(%) or short call SCSR(%).</td>
</tr>
<tr>
<td></td>
<td>• N/A—The SCSR(%) value is not available or is negative.</td>
</tr>
<tr>
<td></td>
<td>• All—Select all the grade.</td>
</tr>
</tbody>
</table>

For more information see Overview of Voice Call Grade Settings, on page 188.

<table>
<thead>
<tr>
<th>Jitter (ms)</th>
<th>Milliseconds of jitter during the sample duration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Loss</td>
<td>Number of packets lost due to network transmission during the sample duration. Computed based on observed RTP sequence number analysis.</td>
</tr>
<tr>
<td>Sample Duration(s)</td>
<td>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.</td>
</tr>
<tr>
<td>Max Jitter (ms)</td>
<td>Maximum milliseconds of jitter during the sample duration.</td>
</tr>
<tr>
<td>Adjusted Packet Loss(%)</td>
<td>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.</td>
</tr>
<tr>
<td>Packet Loss (%)</td>
<td>Percent of packet loss. (Packets lost divided by total packets expected expressed as a percent.)</td>
</tr>
<tr>
<td>SSRC</td>
<td>Synchronization source ID—Identifies the source of a stream of RTP packets.</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Listener DN/IP| Identifies the endpoint-called or caller-for which MOS and impairment details are reported; one of these:  
|               | • IP address of the listener.  
|               | • Directory number of the listener. |
| Cluster       | Unified Communications Manager cluster.                                      |
| Caller/Called | • **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 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 | • **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 | • **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 286 and Call Category Creation, on page 289 |
| 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 286 and Call Category Creation, on page 289 |
| Call Class | One of these:  
• Offnet  
• Onnet  
**Note** For more information, see Understand OffNet and OnNet Calls, on page 288 |
| 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 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 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 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 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 session.
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.

- 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 48: Stream Summary**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>

Speaker/Listener

• Directory Number-Displayed when the device is managed by a Unified Communications Manager that:
  • Is added to Cisco Prime Collaboration 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:
  • N/A-Some error prevents Cisco Prime Collaboration from obtaining the device type.
  • Unavailable-This is the first time that Cisco Prime Collaboration has seen this phone and the device type is not yet known; or the corresponding Unified CM:
    • Has not been added to Cisco Prime Collaboration.
    • Did not provide a valid device type to Cisco Prime Collaboration.

<table>
<thead>
<tr>
<th>TOS</th>
<th>Type of service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codec</td>
<td>Codec name.</td>
</tr>
<tr>
<td>SSRC</td>
<td>Synchronization Source ID-Identifies the source of a stream of RTP packets.</td>
</tr>
</tbody>
</table>

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 49: Call Record

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Disconnect</td>
<td>The time that the call disconnected. Zero (0) is displayed if the call never connected.</td>
</tr>
<tr>
<td>Cluster ID</td>
<td>Unified CM cluster ID.</td>
</tr>
</tbody>
</table>
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.

B-channel number of the MGCP gateway, or NA, if not applicable.

IP address of the device that terminates the call signaling.

B-channel number of the MGCP gateway, or NA, if not applicable.

Length of the call, in seconds.

Populated when the originating party releases the call. Termination causes might not be populated.

Populated when the terminating party releases the call or the call is rejected. 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 50: Stream Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name</td>
<td>Display name of the Cisco 1040 or Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM).</td>
</tr>
<tr>
<td>Time</td>
<td>Time at which the sensor calculated the MOS.</td>
</tr>
<tr>
<td>MOS</td>
<td>Average MOS in the sample duration.</td>
</tr>
<tr>
<td>Minimum MOS</td>
<td>Minimum MOS in the sample duration.</td>
</tr>
<tr>
<td>Primary Degradation Cause</td>
<td>Jitter, Packet Loss, or None when jitter and packet loss values are zero (0).</td>
</tr>
<tr>
<td>Jitter (ms)</td>
<td>Milliseconds of jitter.</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Number of packets lost. (Actual packet loss for the sample duration.)</td>
</tr>
<tr>
<td>Sample Duration (s)</td>
<td>Number of seconds elapsed between the first and last packets that are analyzed.</td>
</tr>
<tr>
<td>Max Jitter (ms)</td>
<td>Maximum jitter, in milliseconds.</td>
</tr>
</tbody>
</table>
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

You can use Sessions reports to view All Sessions Summary report and Sessions Detail report.

The following reports can be generated for Sessions reports:

All Session Summary Report

The All Session Summary report provides information about the in-progress and completed sessions. The reports are available for four weeks.

This report includes the following information: endpoint name, device ID, total utilization, average duration, and longest session.

It displays the scheduled duration of the scheduled session. For an Ad hoc session 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 session.
- Protocol - Displays the protocol used for the session. This is displayed in the Participated sessions of Endpoint pane.

Ensure that the visibility of the phones is set to Full, to view the preceding details.

The protocol is not displayed for MSI-enabled Cisco Unified IP Phones 89 series.

You can view the following additionally:

- Received Video DSCP - The last received DSCP value of the video device(s) in the session. 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 session. 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 session.
To generate the All Sessions Summary report, choose **Assurance Reports > Session Reports > All Session Summary Report**.

**Session Detail Report**

The Sessions Detail report provides the following details: session ID, duration, start/end time, session type, status, and alarm severity.

To generate the Sessions Detail report, choose **Assurance Reports > Session Reports > Session Detail Report**.

**TelePresence Endpoint Reports**

You can use TelePresence reports to view endpoint utilization, and no show endpoints summary.

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:
  
  \[
  \frac{\text{Total number of utilization in minutes}}{\text{maximum utilization} \times 60} \times 100
  \]

- For custom reports:
  
  \[
  \frac{\text{Total number of utilization in minutes}}{\text{maximum utilization} \times 60 \times \text{number of days}} \times 100
  \]

  - 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**.

**No Show Endpoint Summary Report**

The No Show Endpoints Summary report provides information about the endpoints that did not participate in the scheduled sessions. This report is generated based on the scheduled completed sessions data.

To generate the No Show Endpoints Summary report, choose **Assurance 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 Assurance Reports > Launch CUCM Reports, and click a cluster name to open the Cisco Unified Reporting application.

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 in enterprise mode, the Phone Activity reports display the domain name, except the Export Audio Phones report.

If you have deployed Cisco Prime Collaboration in MSP mode, the Phone Activity reports display the customer name, except the Export Audio Phones report.

The following Activity reports are available:

Audio Phone Move Report

The Audio Phone Move report displays the details of IP phones 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 Audio Phone Move report shows the time at which the IP phone move was detected, and not the time at which the move occurred.

Cisco Prime Collaboration obtains fresh data for the Audio Phone Move report every 5 minutes. You can also close the report and regenerate it to refresh the data.

To generate the Audio Phone Move report, choose Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Audio Phone Move.

Note

Audio Phone Move report is not supported for the phones that do not support CDP.

Audio Phone Audit Report

The Audio Phone Audit report shows the changes that have occurred in the managed IP phone network. For example, this report shows the IP phones that have been added or deleted from your network, IP phone outage status, and so on. Phone status changes occur, for instance, when a phone becomes unregistered with the Cisco Unified CM.
To generate the Audio Phone Audit report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Audio Phone Audit.**

---

**Note**  
The IP Phone Audit report is not supported for Cisco Wireless IP Phone 7920.

---

### Removed IP Phones Report

The Removed IP Phones report lists phones that have been removed during the last 30 days.
Cisco Prime Collaboration gathers the information used in this report every 5 minutes.
To generate the Removed IP Phones report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Removed IP Phones.**

---

**Note**  
The Removed IP Phone report is not supported for Cisco Wireless IP Phone 7920.

---

### Extension Number Changes Report

The Extension Number Changes Report lists the audio phones for which extension numbers were changed during the last 30 days.
Cisco Prime Collaboration gathers the information used in this report every 5 minutes.
To generate the Extension Number Changes Report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Audio Phone Extension Changes.**

---

**Note**  
The Extension Number Changes Report is not supported for Cisco Wireless IP Phone 7920.

---

### Suspect Phones Report

The Suspect Phones report displays the attributes of all IP phones that:
- Have not registered with a Cisco Unified CM.
- Have made an unsuccessful attempt to register with a Cisco Unified CM.

To generate the Suspect Phones report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Suspect Phones.**

Some IP phones appear marked as Suspect when they are not. To correct this, make sure that the Cisco Unified CM is managed by Cisco Prime Collaboration.
- If the Cisco Unified CM is not managed by Cisco Prime Collaboration, add it to Cisco Prime Collaboration.
- If the Cisco Unified CM is managed by Cisco Prime Collaboration but is not reachable, this can be due to loss of connectivity. Make sure that connectivity with Cisco Prime Collaboration is restored.
The Suspect Phones report is not supported for Cisco Wireless IP Phone 7920.

**Note**

Duplicate MAC/IP Address Report

The Duplicate MAC/IP Address report lists the attributes of all IP phones that have:

- Duplicate MAC addresses; that is, a phone that has the same MAC address as another phone but a different IP address.
- Duplicate IP addresses; that is, a phone that has the same IP address as another phone but a different MAC address.

Cisco Prime Collaboration does not show a multihomed host as a phone with a duplicate MAC address.

For the Duplicate MAC/IP Address report to display the correct information, the switch to which the phone is connected must be monitored by Cisco Prime Collaboration. If the switch is not monitored by Cisco Prime Collaboration, the report will not display any information.

To generate the Duplicate MAC/IP Address report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Duplicate MAC/IP**.

Video Phone Move Report

The Video Phone Move report displays video phones that have been moved in the last 30 days. It also displays the Extension, Cisco Unified Communications Manager address, switch address, and switch ports used before and after the move.

The Video Phone Move report shows the time at which the video phone move was detected, and not the time at which the move occurred.

Information for the Video Phone Move report is gathered every 5 minutes using Video Phone Movement Tracking.

Video Phone Movement Tracking is used to:

- Check all the switches and Cisco Unified CM
- Identify the list of changes
- Generate the data on video phone moves

To generate the Video Phone Move report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Video Phone Move**.

**Tip**

Tip Video Phone Move report is not supported for the phones that do not support CDP.

Video Phone Audit Report

The Video Phone Audit report shows the changes that have occurred in the managed video phone network. For example, this report shows you the video phones that have been added or deleted from your network,
changes in video phone status, and so on. Phone status changes occur, for instance, when a phone becomes unregistered with the Cisco Unified CM.

To generate the Video Phone Audit report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Video Phone Audit.**

**Removed Video Phones Report**

The Removed Video Phones report lists phones that have been removed during the last 30 days. Cisco Prime Collaboration gathers fresh data for the Video Phone Move report every 5 minutes. You can also close the report and regenerate it to refresh the data.

To generate the Removed Video Phones report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Removed Video Phones.**

**Video Phone Extension Number Changes Report**

The Video Extension Number Changes report lists the video phones for which extension numbers were changed during the last 30 days.

To generate the Video Extension Number Changes report, choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Video Extension Changes.**

**Export Audio Phones Report**

You can export 24-hours IP audio phone status report in the PDF and/or CSV file format for the following:

- **Suspect IP Phones:** IP audio Phones that have:
  - Not registered with Cisco Unified CM.
  - Made an unsuccessful attempt to register with a Cisco Unified CM.

- **Duplicate MAC/IP Address Phones:** IP audio phones that have:
  - The same MAC address as another phone but a different IP address.
  - The same IP address as another phone but a different MAC address.

- **Extension Number Changes:** Audio IP phones for which extension numbers were changed.

- **IP Phone Audit:** Changes that have occurred in your managed IP phone network. For example, this report shows the IP phones that have been added or deleted from your network, IP phone outage status, and so on.

- **IP Phone Move:** Audio IP phones that have been moved. The report shows the time at which the IP phone move was detected, and not the time at which the move occurred.

- **Removed IP Phones:** IP audio phones that have been removed from Cisco Unified CM.

- **All IP Phones/Lines:** Details of all IP audio phones and its configured lines.
The maximum number of records that can be exported to a PDF file is 2,000. The maximum number of records that you can export to CSV is 30,000.

Procedure

Step 1
Choose Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Export Audio Phones. The Export Settings (for Export Audio Phones) page appears, displaying the information described in the following table.

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Type</td>
<td>Select a report type.</td>
</tr>
<tr>
<td>Save at</td>
<td>Enter a location for storing the reports on the server where Cisco Prime Collaboration Assurance is installed; the default location is /opt/emms/cuom/PhoneStatusChangeReports. <strong>Note</strong> 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, Cisco Prime Collaboration cannot create the export files.</td>
</tr>
<tr>
<td>E-mail to</td>
<td>Enter one or more complete e-mail addresses separated by commas.</td>
</tr>
</tbody>
</table>

Step 2
Click Apply.

What to Do Next
You can download the reports by clicking the Download Report button.

Export Video Phones Report
You can export 24-hours video phone status report in the PDF and/or CSV file format for the following:

- Extension Number Changes: Video phones for which extension numbers were changed.
- Video Phone Audit: Changes that have occurred in your managed video phone network. For example, this report shows the video phones that have been added or deleted from your network, video phone outage status, and so on.
- Video Phone Move: Video phones that have been moved. The report shows the time at which the video phone move was detected, and not the time at which the move occurred.
- Removed Video Phones: Video phones that have been removed from Cisco Unified CM.
- Video Phones/Lines: Details of all Video phones and its configured lines.

**Note**
The maximum number of records that can be exported to a PDF file is 2,000. The maximum number of records that you can export to CSV is 30,000.

**Procedure**

**Step 1** Choose **Assurance Reports > Miscellaneous Reports > UCM/CME Phone Activity Reports > Export Video Phones**. The Export Settings (for Export Video Phones) page appears, displaying the information described in the following table.

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Type</td>
<td>Select a report type.</td>
</tr>
<tr>
<td>Save at</td>
<td>Enter a location for storing the reports on the server where Cisco Prime Collaboration Assurance is installed; the default location is /opt/emms/cuom/PhoneStatusChangeReports. <strong>Note</strong> 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, Cisco Prime Collaboration cannot create the export files.</td>
</tr>
<tr>
<td>E-mail to</td>
<td>Enter one or more complete e-mail addresses separated by commas.</td>
</tr>
</tbody>
</table>

**Step 2** Click **Apply**.

**What to Do Next**

You can download the reports by clicking the **Download Report** button.

**Understand the Time Period Covered by Audio IP Phone Activity Reports**

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 following resides:

- Your client system—Cisco Prime Collaboration 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 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 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 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**

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 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 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 in the MSP mode)
- Date
- Export

To generate Call Quality Event History report, choose **Assurance 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.

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.

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 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 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 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 in Enterprise mode.

If you have deployed Cisco Prime Collaboration 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.

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 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.

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 Session 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.

The following scheduled reports are available:

<table>
<thead>
<tr>
<th>Report Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilization Reports (Under Reports selector, select Utilization &gt; Endpoint, and Endpoint No Show to see the Monthly Utilization and Monthly No Show Reports.)</td>
<td>Provides aggregate monthly reports on the utilization of the endpoints. The aggregate value is calculated by Total utilization for all months / 12.</td>
</tr>
<tr>
<td>Monthly Utilization Report</td>
<td>Provides aggregate monthly reports on the utilization of the endpoints. The aggregate value is calculated by Total utilization for all months / 12.</td>
</tr>
<tr>
<td>Monthly No Show Report</td>
<td>Provides aggregate monthly reports on the nonparticipation of endpoints in scheduled sessions. The average aggregate value is calculated by Total no show for all months / 12.</td>
</tr>
<tr>
<td>Session Detail Report</td>
<td>Provides details on the session statistics for all completed sessions.</td>
</tr>
<tr>
<td>Inventory Reports</td>
<td></td>
</tr>
<tr>
<td>Managed Devices Report</td>
<td>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.</td>
</tr>
<tr>
<td>Unmanaged Devices Report</td>
<td>Provides information about unmanaged devices. Use this report to identify devices for which credentials need to be updated.</td>
</tr>
<tr>
<td>Endpoints</td>
<td>Provides information on the endpoints as displayed in the Endpoints Diagnostic page. For more information, see the section.</td>
</tr>
<tr>
<td>Event History Reports</td>
<td></td>
</tr>
</tbody>
</table>
Report Title | Description
--- | ---
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 Session 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:

**Procedure**

1. Select a report from the Reports pane.
2. Click the Settings tab under the Report Details pane, and click Enable Scheduling.
3. Schedule the report generation using options in the Scheduler and Settings pane.
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 reports display up to 2,000 records. If more than 2,000 records are returned when you generate a report, Cisco Prime Collaboration 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 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>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:</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>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:</td>
</tr>
</tbody>
</table>
PART VII

Perform Diagnostics

• Diagnostics for Voice Endpoints, page 333
• Diagnostics for Video Endpoints, page 383
• Media Path Analysis, page 411
• Collect Logs, page 417
• Analyze Call Signaling, page 423
Diagnostics for Voice Endpoints

Cisco Prime Collaboration enables you to run multiple diagnostics tests to identify issues related to Unified Communications phone network.

If you have deployed Cisco Prime Collaboration 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, page 333
- Synthetic Test, page 337
- IP SLA Voice Tests, page 352
- Create a Batch Test, page 371
- Phone Tests—Batch and On Demand Tests, page 374
- UC Phone Tests SummaryAudio Phone Features Test, page 378
- CME Diagnostics, page 380

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 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 ping, and the phone status is unregistered in the phone status process. Cisco Prime Collaboration generates the PhoneReachabilityTestFailed event.

When a router is rebooted, the phone status tests are lost. However, Cisco Prime Collaboration reconfigures the test when the router becomes available. While the router is down, the Cisco Prime Collaboration ping continues to run, if you have enabled Cisco Prime Collaboration 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; 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.

Before uninstalling Cisco Prime Collaboration, 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.

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 device inventory. However, when Cisco Prime Collaboration 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.

**Procedure**

1. Choose **Synthetic Test Center > Phone Status Test**.
2. Click **Create**.
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.
4. Click **Add From Phone Report**.
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**.
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 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:

**Procedure**

**Step 1** Choose **Synthetic Test Center** > **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 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 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 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 51: Seed File Format for Phone Status Testing

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Phone extension.</td>
</tr>
<tr>
<td>2</td>
<td>Phone MAC address.</td>
</tr>
<tr>
<td>3</td>
<td>Phone IP address.</td>
</tr>
<tr>
<td>4</td>
<td>IP SLA-enabled device (router, switch, or voice router).</td>
</tr>
<tr>
<td>5</td>
<td>Read community string for the IP SLA-enabled device.</td>
</tr>
<tr>
<td>6</td>
<td>Write community string for the IP SLA-enabled device.</td>
</tr>
<tr>
<td>7</td>
<td>SNMPv3 username (used in the eight-column format only)</td>
</tr>
<tr>
<td>8</td>
<td>SNMPv3 password (used in the eight-column format only)</td>
</tr>
</tbody>
</table>

### Examples

**Example 1: Phone Status Testing Six-Column Import File**

```
[Extension]:[MAC Address]:[IPAddress]:[IPSLA Router]:[Read Community]:[Write community]
4000:200000000001:172.20.121.1:10.76.34.194: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]
#4000:200000000001:172.20.121.1:10.76.34.194:![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 tests 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 can monitor the information returned from the synthetic tests and generate events based on the results. If a synthetic test fails, Cisco Prime Collaboration generates a critical event. Such events are displayed in Event Browser.

Cisco Prime Collaboration supports synthetic testing for the following applications:

- Cisco Unified CM and Cisco Unified CM Express
- Cisco TFTP Server
- Cisco Emergency Responder
- Cisco Unity, Cisco Unity Express, and Cisco Unity Connection

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 52: Synthetic Test Descriptions and Expected Results**

<table>
<thead>
<tr>
<th>Synthetic Test</th>
<th>Description</th>
<th>Expected Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Registration Test</td>
<td>Opens a connection with the Cisco Unified CM and registers a simulated IP phone.</td>
<td>Successful registration of the phone.</td>
</tr>
<tr>
<td>Dial-Tone Test</td>
<td>Simulates an off-hook state to Cisco Unified CM and checks for receipt of a dial tone.</td>
<td>Receives a dial tone signal from Cisco Unified CM.</td>
</tr>
<tr>
<td>Synthetic Test</td>
<td>Description</td>
<td>Expected Results</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>End-to-End Call Test</td>
<td>Initiates a call to a second simulated or real IP phone.</td>
<td>• Registers, goes off-hook, and places the call</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ring indication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Destination phone goes off-hook to accept the call</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If call progress tones and announcements are configured on the gateway for your</td>
</tr>
<tr>
<td></td>
<td></td>
<td>end-to-end call, the test may succeed even before the phone rings or after a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>couple of rings. This indicates that your gateway is working correctly.</td>
</tr>
<tr>
<td>TFTP Download Test</td>
<td>Performs a TFTP get-file operation on the TFTP server.</td>
<td>Successful download of a configuration file from the TFTP server.</td>
</tr>
<tr>
<td>Emergency Call Test</td>
<td>Initiates a call to the emergency number to test the dynamic routing of</td>
<td>• All calls initiated</td>
</tr>
<tr>
<td></td>
<td>emergency calls.</td>
<td>• Ring indication on Public Safety Answering Point (PSAP) and On Site Alert</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number (OSAN), if configured.</td>
</tr>
<tr>
<td>Message-Waiting Indicator Test</td>
<td>Calls the target phone and leaves a voice message in the voice mailbox.</td>
<td>Activation of the phone's message-waiting indicator. The message is then deleted</td>
</tr>
<tr>
<td></td>
<td>The destination phone for the Message-Waiting Indicator Test should be</td>
<td>and the message-waiting indicator is deactivated.</td>
</tr>
<tr>
<td></td>
<td>configured as Call Forward after X number of rings before moving to voicemail.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If it is configured for Call Forward Always, the test will fail.</td>
<td></td>
</tr>
</tbody>
</table>

**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.

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:

Procedure

Step 1 Choose Synthetic Test Center > 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 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**

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:

**Procedure**

1. Choose **Synthetic Test Center > UC Application Synthetic Test**.
2. Click **Create**.
3. From the Test Type drop-down menu, select **Message-Waiting Indicator Test**.
4. In the Unity Parameters pane, enter the Cisco Unity, Cisco Unity Express, or Cisco Unity Connection system details.
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:

**Procedure**

1. Choose **Synthetic Test Center > UC Application Synthetic Test**.
2. Click **Create**.
3. From the Test Type drop-down menu, select **TFTP Download Test**.
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.
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.

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:

**Procedure**

1. **Step 1** Choose *Synthetic Test Center > UC Application Synthetic Test*.
2. **Step 2** Click *Create*.
3. **Step 3** From the Test Type drop-down menu, select *End-to-End Call Test*.
4. **Step 4** In the Caller pane, do the following: (Depending on the type of phone you select, some selections might become unavailable.)
   a) 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.
   b) 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.
   c) Select a protocol type.
   d) 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 #.

5. **Step 5** In the Recipient pane, do the following:
   a) Select either the Synthetic Phone or Real Phone radio button.
   b) 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.
c) Enter the phone's MAC address (if you selected the Real Phone radio button, this option is grayed out).
d) Select a protocol type (if you selected the Real Phone radio button, this option is grayed out).
e) 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:

Procedure

Step 1  Choose Synthetic Test Center > 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.
### Create a Phone Registration Test

To create a phone registration test:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Synthetic Test Center &gt; UC Application Synthetic Test</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Create</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Test Type drop-down list, select <strong>Phone Registration Test</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter the synthetic phone’s MAC address. See Prerequisites for Synthetic Tests for MAC address limitations.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select a protocol and parameter type.</td>
</tr>
<tr>
<td></td>
<td>• If you select Extension, enter the extension for the phone.</td>
</tr>
<tr>
<td></td>
<td>• 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:<a href="mailto:7690@ct-sd.cisco.com">7690@ct-sd.cisco.com</a>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select a criteria for success (Registration Success or Registration Failure).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the Run pane, name the test and schedule when to run the test.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Click <strong>Create</strong>.</td>
</tr>
</tbody>
</table>

### 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.
**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Synthetic Test Center &gt; UC Application Synthetic Test.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click Import.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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, DAYSOFMONTH, DAYSOFWEEK, 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 53: Import File Format for Phone Registration Tests

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of test—REGISTRATION</td>
</tr>
<tr>
<td>2</td>
<td>Test name</td>
</tr>
<tr>
<td>3</td>
<td>Polling interval</td>
</tr>
<tr>
<td>4</td>
<td>Schedule</td>
</tr>
<tr>
<td>5</td>
<td>Cisco Unified CM to which the phone is connected</td>
</tr>
<tr>
<td>6</td>
<td>Phone’s MAC address. See Prerequisites for Synthetic Tests, for information on MAC details</td>
</tr>
<tr>
<td>7</td>
<td>Phone’s protocol (SCCP or SIP)</td>
</tr>
<tr>
<td>8</td>
<td>SIP URI or extension number</td>
</tr>
<tr>
<td>9</td>
<td>Customer name</td>
</tr>
</tbody>
</table>

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 54: Import File Format for Dial-tone Tests

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of test—DIALTONE/OFFHOOK</td>
</tr>
<tr>
<td>2</td>
<td>Test name</td>
</tr>
<tr>
<td>3</td>
<td>Polling interval</td>
</tr>
</tbody>
</table>
### 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
ENDTOENDTEST|endtoend test|60|*;*;*;*;*|ipif-skate.cisco.com|00059A3B7782|FALSE|ipif-skate.cisco.com|00059A3B7783|4002|TRUE|FALSE|SCCP|4004|SCCP
```

#### Table 55: Import File Format for End-to-End Call Tests

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of test—ENDTOENDTEST</td>
</tr>
<tr>
<td>2</td>
<td>Test name</td>
</tr>
<tr>
<td>3</td>
<td>Polling interval</td>
</tr>
<tr>
<td>4</td>
<td>Schedule</td>
</tr>
<tr>
<td>5</td>
<td>Caller Cisco Unified CM</td>
</tr>
<tr>
<td>6</td>
<td>Caller MAC address. See Prerequisites for Synthetic Tests, for information on MAC details.</td>
</tr>
<tr>
<td>7</td>
<td>Whether or not the recipient phone is a real phone. Enter true or false.</td>
</tr>
<tr>
<td>8</td>
<td>Recipient Cisco Unified CM</td>
</tr>
<tr>
<td>9</td>
<td>Recipient MAC address. See Prerequisites for Synthetic Tests, for information on MAC details.</td>
</tr>
<tr>
<td>10</td>
<td>Recipient extension number</td>
</tr>
<tr>
<td>11</td>
<td>Wait for answer. Enter true or false</td>
</tr>
<tr>
<td>12</td>
<td>Enable RTP transmission. Enter true or false</td>
</tr>
<tr>
<td>Column Number</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>13</td>
<td>Phone’s protocol (SCCP or SIP)</td>
</tr>
<tr>
<td>14</td>
<td>SIP URI or extension number</td>
</tr>
<tr>
<td>15</td>
<td>Destinations phone’s protocol (SCCP or SIP)</td>
</tr>
<tr>
<td>16</td>
<td>Customer name</td>
</tr>
</tbody>
</table>

**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 56: Import File Format for TFTP Download Tests*

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of test—TFTP</td>
</tr>
<tr>
<td>2</td>
<td>Test name</td>
</tr>
<tr>
<td>3</td>
<td>Polling interval</td>
</tr>
<tr>
<td>4</td>
<td>Schedule</td>
</tr>
<tr>
<td>5</td>
<td>Cisco Unified CM</td>
</tr>
<tr>
<td>6</td>
<td>Customer name</td>
</tr>
</tbody>
</table>

**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|10059A3B7B01|71418001|13579
Table 57: Import File Format for Message-Waiting Indicator Tests

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of test—MWITEST</td>
</tr>
<tr>
<td>2</td>
<td>Test name</td>
</tr>
<tr>
<td>3</td>
<td>Polling interval</td>
</tr>
<tr>
<td>4</td>
<td>Schedule</td>
</tr>
<tr>
<td>5</td>
<td>Cisco Unity system</td>
</tr>
<tr>
<td>6</td>
<td>Caller Cisco Unified CM</td>
</tr>
<tr>
<td>7</td>
<td>Caller MAC address. See Prerequisites for Synthetic Tests, for information on MAC details.</td>
</tr>
<tr>
<td>8</td>
<td>Recipient Cisco Unified CM</td>
</tr>
<tr>
<td>9</td>
<td>Recipient MAC address. See Prerequisites for Synthetic Tests, for information on MAC details.</td>
</tr>
<tr>
<td>10</td>
<td>Recipient extension number</td>
</tr>
<tr>
<td>11</td>
<td>Recipient voicemail password</td>
</tr>
<tr>
<td>12</td>
<td>Customer name</td>
</tr>
</tbody>
</table>

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 58: Emergency Call Test Tests

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of test—CCCTEST</td>
</tr>
<tr>
<td>2</td>
<td>Test name</td>
</tr>
<tr>
<td>3</td>
<td>Polling interval</td>
</tr>
<tr>
<td>Column Number</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>4</td>
<td>Schedule</td>
</tr>
<tr>
<td>5</td>
<td>Cisco Emergency Responder system</td>
</tr>
<tr>
<td>6</td>
<td>Caller Cisco Unified CM</td>
</tr>
<tr>
<td>7</td>
<td>Caller MAC address. See Prerequisites for Synthetic Tests, for information on MAC details.</td>
</tr>
<tr>
<td>8</td>
<td>Public Safety Answering Point (PSAP) Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>9</td>
<td>PSAP MAC address. See Prerequisites for Synthetic Tests, for information on MAC details.</td>
</tr>
<tr>
<td>10</td>
<td>Emergency number</td>
</tr>
<tr>
<td>11</td>
<td>Enable On Site Alert Number (OSAN). Enter true or false.</td>
</tr>
<tr>
<td>12</td>
<td>OSAN Cisco Unified CM</td>
</tr>
<tr>
<td>13</td>
<td>OSAN MAC address</td>
</tr>
<tr>
<td>14</td>
<td>Customer name</td>
</tr>
</tbody>
</table>

**Manage Synthetic Tests**

The following table describes the tasks that you can perform from the Synthetic Tests page.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Synthetic tests</td>
<td>You can export the synthetic tests that you have created to a file on your Cisco Prime Collaboration server. If needed, you can use this file to import your configured synthetic tests back into Cisco Prime Collaboration, or to import the tests into another Cisco Prime Collaboration system.</td>
</tr>
<tr>
<td>Edit Synthetic tests</td>
<td>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. 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.</td>
</tr>
<tr>
<td>View Synthetic test details</td>
<td>In the Synthetic Test Details page you can view the parameters that have been configured for a test. The details displayed vary depending on the type of test.</td>
</tr>
</tbody>
</table>
### Synthetic Test

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start and stop Synthetic tests</td>
<td>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.</td>
</tr>
</tbody>
</table>
| View Synthetic test results  | The results are displayed in a report format. As with any of the reports in Cisco Prime Collaboration, you can print the report or export it to a file.  

The Synthetic Tests Results report provides the following information:
- The Test status (passed or failed).
- The day and time that the test finished.
- Any error messages. |
| Schedule Synthetic tests     | When you create a synthetic test, you have the option of running the test now, or scheduling the test to run at regular intervals.  

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.  

If the system time of the Cisco Prime Collaboration 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.  

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.  

Your login determines whether or not you can perform this task. |

**Synthetic Test Notes**

The following table contains information you should be aware of while creating synthetic tests:

<table>
<thead>
<tr>
<th>Summary</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synthetic tests do not run for 30 minutes after the Cisco Prime Collaboration processes are started. However, during this time, you can still create, edit, or delete tests.</td>
<td>Starting Cisco Prime Collaboration processes places a high load on the system. To prevent synthetic tests from failing during this time, Cisco Prime Collaboration delays starting them.</td>
</tr>
<tr>
<td>Synthetic tests may either be skipped or take an extended period of time to run if the server CPU RAM reaches 85%. This anomaly will be reflected in the portlets.</td>
<td>Whenever the server CPU is greater than 85%, synthetic tests are either skipped or would take more time for execution. 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.</td>
</tr>
</tbody>
</table>
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 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 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:

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UDP Jitter for VoIP</strong></td>
<td>Starting Cisco Prime Collaboration processes places a high load on the system. To prevent synthetic tests from failing during this time, Cisco Prime Collaboration delays starting them. Measures packet loss, round-trip latency, and delay variance (or jitter) in IP networks by generating synthetic UDP traffic. 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. 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. 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.</td>
</tr>
<tr>
<td><strong>Ping Echo</strong></td>
<td>Measures end-to-end response time between a source device and any IP-enabled device. The test sends ICMP packets from the source device to the destination device and measures the time it takes to complete the round trip.</td>
</tr>
<tr>
<td><strong>Ping Path Echo</strong></td>
<td>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. <strong>Note</strong> 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).</td>
</tr>
<tr>
<td><strong>UDP Echo</strong></td>
<td>Measures UDP response time between a source device and any IP-enabled device. 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. There are two destination device types for the UDP echo operation: RTR Responders, which use IP SLA, and UDP servers, which do not.</td>
</tr>
</tbody>
</table>
## Test Name | Description
--- | ---
Gatekeeper Registration Delay | Measures the time required for a gateway to register with a gatekeeper. 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. For the Gatekeeper Registration Delay test to run, the source gateway must have SIP or H323 configured on it.

Real-Time Transport Protocol | 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. 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. 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.

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.

**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.

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, 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.

## 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.
**Create an IP SLA Voice Test**

To create an IP SLA Voice test:

**Procedure**

**Step 1** Choose **Synthetic Test Center > 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 59: UDP Jitter for VoIP Test Parameters* for details on the parameters.
- Ping Echo. See *Table 61: Ping Echo Test Parameters* for details on the parameters.
- Ping Path Echo. See *Table 62: Ping Path Echo Test Parameters* for details on the parameters.
- UDP Echo. See *Table 63: UDP Echo Test Parameters* for details on the parameters.
- Gatekeeper Registration Delay
- Real-time Transport Protocol. See *Table 64: 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).

• 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.

---

**Table 59: UDP Jitter for VoIP Test Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Available Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codec Type</td>
<td></td>
<td>• G.711ulaw</td>
<td>Used to determine the packet interval and the request payload.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• G.711alaw</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• G.729</td>
<td></td>
</tr>
<tr>
<td>Call Duration</td>
<td>8</td>
<td>1 - 59 seconds</td>
<td>Time of the call.</td>
</tr>
<tr>
<td>Voice Quality Expectation</td>
<td>Land line</td>
<td>• Land line</td>
<td>Corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Wireless campus</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Wireless on the move</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multi-hop</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Default Value</td>
<td>Available Values</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IP QoS                     | IP Precedence | • IP Precedence  
• DSCP                                                      | Defines the quality of service policies for the IP SLA packets.                                |
|                            |               | ▪ 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 60: UDP Jitter for VoIP Test Threshold Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Available Values</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:  
▪ Excellent—5 (500)  
▪ Good—4 (400-499)  
▪ Fair—3 (300-399)  
▪ Poor—2 (200-299)  
▪ Bad—1 (100-199) |

\(^1\) Positive integers must be 32 bit.
### Table 61: Ping Echo Test Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Available Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Payload</td>
<td>32 bytes</td>
<td>28 to 16384 bytes</td>
<td>A default ICMP Ping packet has 32 bytes. Allows for variably sized operations.</td>
</tr>
<tr>
<td>IP QoS</td>
<td>IP Precedence</td>
<td>• IP Precedence</td>
<td>Defines the quality of service policies for the IP SLA packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 (none)</td>
<td>• IP Precedence—0 (none) through 7 (high)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11)</td>
<td>This is converted to TOS and set on the device.</td>
</tr>
</tbody>
</table>

### Table 62: Ping Path Echo Test Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Available Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Payload</td>
<td>32 bytes</td>
<td>28 to 16384 bytes</td>
<td>A default ICMP Ping packet has 32 bytes. Allows for variably sized operations.</td>
</tr>
<tr>
<td>IP QoS</td>
<td>IP Precedence</td>
<td>• IP Precedence</td>
<td>Defines the quality of service policies for the IP SLA packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 (none)</td>
<td>• IP Precedence—0 (none) through 7 (high)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11)</td>
<td>This is converted to TOS and set on the device.</td>
</tr>
</tbody>
</table>
### Table 63: UDP Echo Test Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Available Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Payload</td>
<td>16 bytes</td>
<td>4 to 1500 bytes</td>
<td>Allows for variably sized operations.</td>
</tr>
<tr>
<td>IP QoS</td>
<td>IP Precedence</td>
<td>• IP Precedence</td>
<td>Defines the quality of service policies for the IP SLA packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 (none)</td>
<td>• IP Precedence—0 (none) through 7 (high)</td>
<td>This is converted to TOS and set on the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11)</td>
<td></td>
</tr>
</tbody>
</table>

### Table 64: Real-time Transport Protocol Test Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>General information about a test.</td>
<td></td>
</tr>
<tr>
<td>Codec Type</td>
<td>Used to determine the packet interval and the request payload.</td>
</tr>
<tr>
<td>Call Duration</td>
<td>Test duration. Default is 20 seconds.</td>
</tr>
<tr>
<td>Voice Quality Expectation</td>
<td>Corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (CPIF).</td>
</tr>
<tr>
<td><strong>Threshold Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Interarrival Jitter</td>
<td>Threshold Setting. The Destination to Source Inter-Arrival Jitter (Milliseconds) metric is supported.</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Threshold Setting. The Destination to Source Packet Loss (Number) metric is supported.</td>
</tr>
<tr>
<td>R Factor</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Time</td>
<td>Number of times in minutes in a 24-hour period during which polling occurs.</td>
</tr>
<tr>
<td>Occurrence Pattern</td>
<td>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.</td>
</tr>
<tr>
<td>Test Name</td>
<td>User-defined test name. Cisco Prime Collaboration 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.</td>
</tr>
</tbody>
</table>

### Import Multiple IP SLA Voice Tests

You can import up to 64 tests, the maximum that Cisco Prime Collaboration 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.

#### Procedure

1. **Step 1** Choose **Synthetic Test Center > IP SLA Voice Test**.
2. **Step 2** Click **Import**.
3. **Step 3** Click **OK**.

Cisco Prime Collaboration performs the following actions:

- If this is a file you have imported before, Cisco Prime Collaboration checks to see if any of the devices exist in Cisco Prime Collaboration. If all the information in the import file is the same as what already exists in Cisco Prime Collaboration, a message to that effect appears. Click **OK**.
• Cisco Prime Collaboration 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 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>|<LSRHop2>|<LSRHop3>|<LSRHop4>|<LSRHop5>|<LSRHop6>|<LSRHop7>|<LSRHop8>, <completionTimeThreshold or "">|<start-time>|<end-time>|<AllDaysOfWeek. 1 for all days otherwise 0>|<DaysOfWeek, if AllDaysOfWeek is 0>

**LSRHop<number>** is an optional field.
Import File Example

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

Ping Path Echo Test Import File

Import File Format

Import File Example

ping-path-import2,Ping-Path-Echo,source-2,"",dest-2,3,DSCP,10,32,250,17:00,23:00,0

UDP Echo Test

Import File Format

Import File Example

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

Import File Example

jitter-import2,Data-Jitter,source-1,source-1,dest-with-IPSLA-Responder,3,IPPrecedence,5,711ulaw,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 validates the IP SLA Responder.

VoIP Gatekeeper Registration Delay Test (Scheduled Daily)

Import File Format without Codec (IP SLA Voice Quality) Support

Import File Example

gkregdelay-import1,Voip-GKReg-Delay,source-gateway,3,50,17:00,23:00,0

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.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit IP SLA Voice tests</td>
<td>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 <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Delete IP SLA Voice tests</td>
<td>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 <strong>Delete</strong>.</td>
</tr>
<tr>
<td>View test trending</td>
<td>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 <strong>Trend</strong>. 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.</td>
</tr>
<tr>
<td>View test information</td>
<td>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 <strong>View</strong>.</td>
</tr>
<tr>
<td>Export test details</td>
<td>You can export and save all the details about a single test as shown on the Test Details page, including configuration and status. When you export the test details from Internet Explorer browser, the <strong>Windows Security popup</strong> window may prompt for your credentials. You can cancel the <strong>Windows Security popup</strong> and click <strong>Save</strong> or <strong>Save as</strong> to download the report.</td>
</tr>
</tbody>
</table>

To export test details,

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 an 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 65: IP SLA Voice Test Events

<table>
<thead>
<tr>
<th>Event</th>
<th>PacketLossSD_ThresholdExceeded</th>
<th>RFactorDS_ThresholdExceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeToNodeTestFailed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To determine why an IP SLA Voice test failed and how to clear it, see the IP SLA documentation located on Cisco.com.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RoundTripResponseTime_ThresholdExceeded</td>
<td>PacketLossDS_ThresholdExceeded</td>
<td>MosCQDS_ThresholdExceeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RingBackResponseTime_ThresholdExceeded</td>
<td>IAjitterDS_ThresholdExceeded</td>
<td>RTPPacketLossDS_ThresholdExceeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RegistrationResponseTime_ThresholdExceeded</td>
<td>JitterDS_ThresholdExceeded</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AverageLatency_ThresholdExceeded</td>
<td>Quality Dropped Below Threshold</td>
<td></td>
</tr>
</tbody>
</table>

You can verify whether a test ran and completed correctly. You can also troubleshoot the test if necessary. To do this, select Synthetic Test Center > 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 66: IP SLA Voice Test Status Definition

<table>
<thead>
<tr>
<th>Test Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running</td>
<td>Test is active and collecting data.</td>
</tr>
<tr>
<td>Config Pending</td>
<td>Either the device is not responding or configuration of the test is under way.</td>
</tr>
<tr>
<td>Delete Pending</td>
<td>Intermediate state, before the test is deleted. No actions can be performed on the test.</td>
</tr>
<tr>
<td>Suspended</td>
<td>Test is suspended from data collecting or polling. This occurs because the device was suspended.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Appears after you create or update a test. The status will change to Running at the first polling cycle.</td>
</tr>
<tr>
<td>Dormant</td>
<td>Test is active but not currently collecting data. Tests are in the Dormant state between polling cycles.</td>
</tr>
<tr>
<td>Config Failed</td>
<td>Test was not configured correctly. Possible problems include incorrect device credentials or low device memory.</td>
</tr>
</tbody>
</table>

IP SLA Voice Test Data

Cisco Prime Collaboration 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 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 appends data to a test’s log files. Cisco Prime Collaboration 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 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 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 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 67: Echo Test Data Format**

<table>
<thead>
<tr>
<th>Field Number</th>
<th>Field ID</th>
<th>Content</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Record ID</td>
<td>nnn</td>
<td>Record type 200</td>
<td>200</td>
</tr>
<tr>
<td>2</td>
<td>Date</td>
<td>yyyyymmdd</td>
<td>Calendar date</td>
<td>Example: 20070201</td>
</tr>
<tr>
<td>3</td>
<td>Time stamp</td>
<td>hhmmss</td>
<td>Wall clock time</td>
<td>Example: 230000</td>
</tr>
<tr>
<td>4</td>
<td>Completion time</td>
<td>Number</td>
<td>Round-trip time (RTT), in milliseconds</td>
<td>Between 0 and 4294967295</td>
</tr>
<tr>
<td>5</td>
<td>Completion status</td>
<td>Number</td>
<td>The allowed numbers are:</td>
<td>Between 1 and 16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 1—OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 2—disconnected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 3—overThreshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 4—timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 5—busy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 6—notConnected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 7—dropped</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 8—sequenceError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 9—verifyError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 10—applicationSpecific</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 11—dnsServerTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 12—tcpConnectTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 13—httpTransactionTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 14—dnsQueryError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 15—httpError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 16—error</td>
<td></td>
</tr>
</tbody>
</table>
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 68: Hop-by-hop Statistics for Ping Path Echo Test Data Format**

<table>
<thead>
<tr>
<th>Field Number</th>
<th>Field ID</th>
<th>Content</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Record ID</td>
<td>nnn</td>
<td>Record type 201</td>
<td>201</td>
</tr>
<tr>
<td>2</td>
<td>Date</td>
<td>yyyyymmdd</td>
<td>Calendar date</td>
<td>Example: 20070201</td>
</tr>
<tr>
<td>3</td>
<td>Time stamp</td>
<td>hhmms</td>
<td>Wall clock time</td>
<td>Example: 230000</td>
</tr>
<tr>
<td>4</td>
<td>Completion time</td>
<td>Number</td>
<td>Round-trip time (RTT), in milliseconds</td>
<td>Between 0 and 4294967295</td>
</tr>
<tr>
<td>5</td>
<td>Hop ID</td>
<td>Number</td>
<td>Unique ID chosen by the study and given to a hop on this path.</td>
<td>Maximum value is 30</td>
</tr>
<tr>
<td>6</td>
<td>Hop address</td>
<td>String</td>
<td>IP Address of the hop</td>
<td>ASCII characters</td>
</tr>
<tr>
<td>7</td>
<td>Completion status</td>
<td>Number</td>
<td>The allowed numbers are:</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-------------------</td>
<td>--------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 1—OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 2—disconnected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 3—overThreshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 4—timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 5—busy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 6—notConnected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 7—dropped</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 8—sequenceError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 9—verifyError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 10—applicationSpecific</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 11—dnsServerTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 12—tcpConnectTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 13—httpTransactionTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 14—dnsQueryError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 15—httpError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 16—error</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Between 1 and 16</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8</th>
<th>Application-specific completion status</th>
<th>Number</th>
<th>(Optional) Application-specific status that is valid only when completion status is set to applicationSpecific (10).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Between 1001 and 2147483647</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9</th>
<th>Status description</th>
<th>Text</th>
<th>(Optional) Description for the completion status when completion status is set to applicationSpecific (10). Default value is blank.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASCII characters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10</th>
<th>None</th>
<th>Null indicator</th>
<th>Not used</th>
<th>*</th>
</tr>
</thead>
</table>

**Note**: Fields 11 through 37 are not used and contain the null indicator "*".

<table>
<thead>
<tr>
<th>38</th>
<th>Test name</th>
<th>Text</th>
<th>Name of the IP SLA Voice test</th>
<th>Sjc-VGtest</th>
</tr>
</thead>
</table>

This record format captures end-to-end statistics for Ping Path Echo tests. The tests are from the source to the destination.
### Table 69: End-to-end Statistics for Ping Path Echo Test Data Format

<table>
<thead>
<tr>
<th>Field Number</th>
<th>Field ID</th>
<th>Content</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Record ID</td>
<td>nnn</td>
<td>Record type 204</td>
<td>204</td>
</tr>
<tr>
<td>2</td>
<td>Date</td>
<td>yyyyymmdd</td>
<td>Calendar date</td>
<td>Example: 20070201</td>
</tr>
<tr>
<td>3</td>
<td>Time stamp</td>
<td>hhmmss</td>
<td>Wall clock time</td>
<td>Example: 230000</td>
</tr>
<tr>
<td>4</td>
<td>Completion time</td>
<td>Number</td>
<td>Round-trip time (RTT) in milliseconds</td>
<td>Between 0 and 4294967295</td>
</tr>
<tr>
<td>5</td>
<td>Hop ID</td>
<td>Number</td>
<td>Unique ID given to a hop on this path chosen by the study. For this record, the hop ID is always 1.</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Hop address</td>
<td>String</td>
<td>Mandatory: IP address of the destination</td>
<td>ASCII characters</td>
</tr>
<tr>
<td>7</td>
<td>Completion status</td>
<td>Number</td>
<td>The allowed numbers are:</td>
<td>Between 1 and 16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 1—OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 2—disconnected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 3—overThreshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 4—timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 5—busy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 6—notConnected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 7—dropped</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 8—sequenceError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 9—verifyError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 10—applicationSpecific</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 11—dnsServerTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 12—tcpConnectTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 13—httpTransactionTimeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 14—dnsQueryError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 15—httpError</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 16—error</td>
<td></td>
</tr>
</tbody>
</table>
Between 1001 and 2147483647 (Optional) The application-specific status that is valid only when Completion Status is set to applicationSpecific (10).

Number Application-specific completion status

8

(Optional) This is the description for the completion status when Completion Status is set to applicationSpecific (10). Default value is blank.

ASCII characters

Text Status description

9

None Null indicator Not used *

Fields 11 through 37 are not used and contain the null indicator “*”.

Test name Text Name of the IP SLA Voice test Sjc-VGtest

38

Jitter MOS, ICPIF, and Processed Data record format stores MOS and ICPIF values and processed jitter statistics values.

Table 70: Jitter MOS, ICPIF, and Processed Data Record Format

<table>
<thead>
<tr>
<th>Field Number</th>
<th>Field ID</th>
<th>Content</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Record ID</td>
<td>205</td>
<td>Mandatory: record type 205</td>
<td>205</td>
</tr>
<tr>
<td>2</td>
<td>Date</td>
<td>yyyyymmdd</td>
<td>Calendar date</td>
<td>Example: 20070201</td>
</tr>
<tr>
<td>3</td>
<td>Time stamp</td>
<td>hhmmss</td>
<td>Wall clock time</td>
<td>Example: 230000</td>
</tr>
<tr>
<td>4</td>
<td>ICPIF</td>
<td>Number</td>
<td>Mandatory: Icpif Value</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IP SLA Voice quality</td>
<td>Number</td>
<td>Mandatory: MOS value</td>
<td>Example: 3.6</td>
</tr>
<tr>
<td>6</td>
<td>Source to destination packet loss</td>
<td>Number</td>
<td>Mandatory: number of packets</td>
<td>Any positive integer. Positive integers must be 32 bit.</td>
</tr>
<tr>
<td>7</td>
<td>Destination to source packet loss</td>
<td>Number</td>
<td>Mandatory: number of packets</td>
<td>Any positive integer. Positive integers must be 32 bit.</td>
</tr>
<tr>
<td>8</td>
<td>Source to destination jitter</td>
<td>Number</td>
<td>Mandatory: milliseconds</td>
<td>Greater than or equal to 0 and less than or equal to 100</td>
</tr>
</tbody>
</table>
Create a Batch Test

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. 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.

**Procedure**

**Step 1** Choose **Synthetic Test Center > 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.

---

### Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Destination to source jitter</td>
</tr>
<tr>
<td>10</td>
<td>Average latency</td>
</tr>
<tr>
<td>11</td>
<td>None</td>
</tr>
</tbody>
</table>

**Note** Fields 12 through 37 are not used and contain the null indicator `*`.  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>Test name</td>
</tr>
</tbody>
</table>
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 an 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.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Batch Test Details</td>
<td>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.</td>
</tr>
<tr>
<td>Edit batch tests</td>
<td>To edit batch tests, choose Synthetic Test Center &gt; Batch Test. In the Batch Tests page, select the batch test that you want to change and click Edit.</td>
</tr>
</tbody>
</table>
### Tasks

<table>
<thead>
<tr>
<th><strong>Verify the status of a test</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You can verify whether a test ran and completed correctly. You can also troubleshoot the test if necessary.</td>
<td></td>
</tr>
<tr>
<td>To verify the status of a test, choose <strong>Synthetic Test Center &gt; Batch Test</strong>.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Running</strong> — The test is active and collecting data.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Suspended</strong> — The test is suspended from data collecting or polling. This occurs because the device was suspended.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Scheduled</strong> — Appears after you create or update a test. The status will change to <strong>Running</strong> at the first polling cycle.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Suspend/resume a batch test</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>To suspend and resume a batch test, choose <strong>Synthetic Test Center &gt; Batch Test</strong>.</td>
<td></td>
</tr>
<tr>
<td>The Batch Tests page appears.</td>
<td></td>
</tr>
<tr>
<td>• If the batch test is active and you want to stop it from running, click <strong>Suspend</strong>.</td>
<td></td>
</tr>
<tr>
<td>• If the batch test is suspended and you want it to run at its scheduled time, click <strong>Resume</strong>.</td>
<td></td>
</tr>
<tr>
<td>The scheduled time and day that a batch test is to run is configured in the import file (see <strong>Format IP SLA Voice Test Import Files</strong>). But if you want to run a batch test on demand, you can use the Run Now button.</td>
<td></td>
</tr>
</tbody>
</table>
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.

Cisco Prime Collaboration saves the data collected by the batch tests on the Cisco Prime Collaboration server in the `/opt/emms/cuom/data/bt` folder.

The Batch Test Results report provides the following information for the overall batch test:

- Test status
- Date and time that the test started and finished.

The Batch Test Results report provides the following information for the individual tests that are a part of the batch test:

- 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.

To view the results of a batch test, choose **Synthetic Test Center > Batch Test**. In the Batch Tests page, select the batch test that you want to see the results for, and click **Results**.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
</table>
| View batch test results    | 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. Cisco Prime Collaboration saves the data collected by the batch tests on the Cisco Prime Collaboration server in the `/opt/emms/cuom/data/bt` folder. The Batch Test Results report provides the following information for the overall batch test:  
  - Test status  
  - Date and time that the test started and finished.  
  The Batch Test Results report provides the following information for the individual tests that are a part of the batch test:  
    - 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.  
  To view the results of a batch test, choose **Synthetic Test Center > Batch Test**. In the Batch Tests page, select the batch test that you want to see the results for, and click **Results**. |
| 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  | You can use the export functionality to save the test results on your client system. To export the results of a batch test:  
  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 Test Center > 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 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 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 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 71: Phone Test Descriptions—Batch and On-Demand Tests**

<table>
<thead>
<tr>
<th>Test</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Hold</td>
<td>Takes control of two phones and performs the following:</td>
</tr>
<tr>
<td></td>
<td>1 Places a call from phone A to phone B.</td>
</tr>
<tr>
<td></td>
<td>2 Has phone B put the call on hold.</td>
</tr>
<tr>
<td></td>
<td>3 Disconnects the call.</td>
</tr>
<tr>
<td>Call Forward</td>
<td>Takes control of three phones and performs the following:</td>
</tr>
<tr>
<td></td>
<td>1 Places a call from phone A to phone B.</td>
</tr>
<tr>
<td></td>
<td>2 Forwards the call to phone C from phone B.</td>
</tr>
<tr>
<td></td>
<td>3 Verifies that the call is received by phone C.</td>
</tr>
<tr>
<td></td>
<td>4 Disconnects the call.</td>
</tr>
<tr>
<td>Test</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Call Park           | Takes control of three phones and performs the following:  
  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     | Takes control of three phones and performs the following:  
  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       | Takes control of three phones and performs the following:  
  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           | 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.  
  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. |

**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**.

The following table describes the fields, which you can select while creating the on-demand phone test:
### Table 72: Phone Test Descriptions—Batch and On-Demand Tests

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>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 &gt;&gt; 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.</td>
</tr>
<tr>
<td>JTAPI Username and JTAPI Password</td>
<td>Enter the JTAPI username and password configured on Unified CM.</td>
</tr>
<tr>
<td>Test Phones</td>
<td>To add more phones to Test Phones:</td>
</tr>
<tr>
<td></td>
<td>1  Click <strong>Add from Phone Report</strong>.</td>
</tr>
<tr>
<td></td>
<td>2  In the phone report window, select the additional phones to add and click <strong>Select</strong>. The phones added must belong to the same Cisco Unified CM provided at the beginning for this test.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td>Helper Phones</td>
<td>To add more phones to Helper Phones:</td>
</tr>
<tr>
<td></td>
<td>1  Click <strong>Add from Phone Report</strong></td>
</tr>
<tr>
<td></td>
<td>2  Select the additional phones to add and click <strong>Select</strong>. The phones added must belong to the same Cisco Unified CM provided at the beginning for this test.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td>Phone Tests</td>
<td>Select the phone test that you want to see the results for. See Phone Test Descriptions—Batch and On-Demand Tests. When Call Test is selected Call Type, Success Criterion, and Phone Number fields are enabled.</td>
</tr>
<tr>
<td>Call Type</td>
<td>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.</td>
</tr>
<tr>
<td>Success Criterion</td>
<td>From the drop-down list, choose the success criterion.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The destination phone number to be dialed for the call test needs to be specified in this field.</td>
</tr>
</tbody>
</table>
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 PhoneNumber field is used instead.

When Inter Cluster Call is selected for Call Type, enter the Cisco Unified CM for the phone number specified in the Phone Number field.

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.

### UC Phone Tests Summary

Audio Phone Features Test

The UC Phone Tests Summary 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:**

<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Privileges/Resources for the Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard AXL API Access</td>
<td>Allows access to the AXL database API</td>
</tr>
<tr>
<td>Standard CCM Admin Users</td>
<td>Login rights to Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>Standard SERVICEABILITY Administration</td>
<td>A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.</td>
</tr>
<tr>
<td>Standard CTI Enabled</td>
<td>Enables CTI application control</td>
</tr>
<tr>
<td>Standard CTI Allow Call Monitoring</td>
<td>Allows CTI applications or devices to monitor calls</td>
</tr>
<tr>
<td>Standard CTI Allow Control of Phones supporting Connected Xfer and conf</td>
<td>Allows control of all CTI devices that supports connected transfer and conferencing</td>
</tr>
<tr>
<td>Standard Role</td>
<td>Privileges/Resources for the Role</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standard CTI Allow Control of all devices</td>
<td>Allows control of all CTI-controllable devices</td>
</tr>
</tbody>
</table>

**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.

**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
- 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

**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.
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

**Update the JTAPI.JAR files in Cisco Prime Collaboration Assurance**

To update the JTAPI.JAR files in Cisco Prime Collaboration Assurance

**Procedure**

**Step 1** Log in to Cisco Unified Communications Manager Administration and select Application > Plugins.

**Step 2** Click Find to list the available plugins.

**Step 3** From the list, select Download Cisco JTAPI 32-bit Client for Windows and save the file on your local system.

**Step 4** Click the executable file to install the Cisco JTAPI client on your computer.

**Step 5** In the Cisco Prime Collaboration Assurance server, go to /opt/emms/cuom/objects/bt/lib, and look for the directories listed for each Unified CM version installed.

**Note** Root access feature is mandatory to access the directories, hence you must raise a TAC case to obtain root access.

**Step 6** Click the directory for the Unified CM version that you are currently using. For example, go to directory 10.0 if your current version of CUCM is 10.0.x. Replace the .JAR files (jtapi.jar, updater.jar, jtracing.jar) in the directory with the .JAR files from the newly installed Cisco JTAPI client on your computer.

By default, the .JAR files are in C:\Windows\java\lib on your computer if the default directory was selected during the Cisco JTAPI client installation.

**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 phones registered with each CME. You can click on the number to cross-launch to the Endpoint Diagnostics page.
- Number of unregistered phones. 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, 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.
Diagnostics for Video Endpoints

During the troubleshooting workflow, the devices are polled, based on the values defined for the System Status Polling Interval, Interface Statistics Polling Interval, and Flow Statistics Polling Interval in the Session Path Threshold Settings page.

During the troubleshooting workflow, the endpoints and conference devices are polled every minute to check the status.

For Cisco 500, 1000, and 3000 Series TelePresence Systems, Cisco Unified IP Phone 8900 and 9900 Series, and Cisco Cius, the Cisco Prime Collaboration discovery ends after discovering the Layer 2 devices for an endpoint. That is, Cisco Prime Collaboration discovers the switches and first hop router to which an endpoint is connected.

The newly discovered devices are added to the Cisco Prime Collaboration inventory. The network topology is discovered using CDP, and the links between devices are persisted in the Cisco Prime Collaboration database.

For Cisco C and Ex series TelePresence Systems, Cisco MXP series TelePresence System, Polycom, and Cisco Jabber, the Layer 3 devices between the endpoints are discovered during the troubleshooting workflow.

The Layer 2 devices to which an endpoint is connected are not discovered during the Cisco Prime Collaboration discovery.

You can view details, such as CPU utilization, memory utilization, interface, and so forth for a network device. In addition to the system details, the fault information is also displayed for a device.

---

**Note**

Session troubleshooting is not supported, if you have deployed Cisco Prime Collaboration Assurance in MSP mode.

The troubleshooting workflow impacts the Cisco Prime Collaboration system performance. Add a session or an endpoint to the watch list only if it is required.
The troubleshooting workflow for a session is represented below.

**Figure 8: Troubleshooting Workflow for a Session**

- Features of the Troubleshooting Workflow, page 384
- Start a Troubleshooting Workflow, page 389
- Troubleshoot Data Analysis, page 392
- Export Troubleshooting Data, page 404
- Cisco Mediatrace, page 406
- Cisco Prime Infrastructure Cross-Launch, page 408

**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 session 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 session.
Automatic troubleshooting is not triggered when the packet loss, jitter, or latency alarm occurs in a multipoint session.

Manual troubleshooting can be started from the Session Diagnostics page.

See Start a Troubleshooting Workflow for details on how to start a troubleshooting workflow for sessions and endpoints.

- For a multipoint session, troubleshooting is performed between a multipoint switch and endpoints. The troubleshooting direction is from an endpoint to a multipoint switch, not in the reverse direction.

- 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 in both directions.

- For Cisco C and Ex Series and MCU (point-to-point, multipoint, and multisite):
  - Troubleshooting is supported between two endpoints.
  - Troubleshooting is not supported between an endpoint and MCU. That is, you cannot troubleshoot from an endpoint to MCU and vice versa.

- 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 in both directions.

- You can view the third party devices as part of the topology in the session troubleshooting page (from Session Diagnostics). However, you cannot view the performance and other troubleshooting statistics details for third party devices.

- If the endpoint is in an Unknown state, you can troubleshoot from a known endpoint to this unknown endpoint. For multipoint sessions 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 ends the workflow automatically.

- You can have a maximum of 50 concurrent troubleshooting workflows at a time; that is, you can have 10 VSAA troubleshooting sessions, 30 reactive troubleshooting sessions, and 10 proactive troubleshooting sessions simultaneously.

  If this limit is exceeded, an error message is displayed in the troubleshooting log file.

---

**Note**

Troubleshooting is not supported between an endpoint and voice gateway.
Features of the Troubleshooting Workflow for Sessions

The following are the key behaviors of the troubleshooting workflow, when scheduled sessions are added to the watch list:

- The automatic troubleshooting workflow starts for all sessions added to the watch list.
- In a multipoint session, the troubleshooting starts as soon as the endpoints join the session.
- In a multipoint session, if a troubleshooting is stopped for an endpoint, the troubleshooting workflow continues for the other endpoints in the session. You need to manually start the troubleshooting for this endpoint.
- In a multipoint session, if an endpoint restarts because of a problem, a new troubleshooting workflow is triggered for this endpoint after it rejoins the session. There is no impact on the other endpoints in the session.
- If a session is removed from the watch list, the associated troubleshooting workflow stops, provided:
  - There are no packet loss, jitter, or latency alarms triggered for that session.
  - 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 session is not added to watch list.
  - There are no manually triggered troubleshooting workflows.
  - The troubleshooting workflow is manually stopped, or the session ends.

- If a troubleshooting workflow is triggered manually, the troubleshooting workflow can only be stopped manually; otherwise, it stops when the session ends.
- If a session 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 session. You can stop the troubleshooting workflow for a session that is associated with an endpoint (added to a watch list). You need to manually start the troubleshooting for this session.
- During the session, if an endpoint is removed from the watch list, the troubleshooting stops for that endpoint.
- If a session 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 session until it ends.
- If a session and the associated endpoints are part of the watch list and if the session is removed from the watch list, the troubleshooting workflow continues for the endpoints, until they disconnect from the session. That is, if the session and endpoints are part of the watch list, the endpoints are given higher priority.
• CDP needs to be enabled on all network devices if troubleshooting path trace is desired. If CDP cannot be enabled on any of the devices, you can use Cisco Mediatrace to check whether the adjacent Layer 3 nodes on the media path are directly connected and what ingress and egress interfaces are used.

• For routers and switches, CLI login credentials are required if Medianet-based troubleshooting is desired. Also, privileged EXEC level (level 15) access is required.

• When you start troubleshooting from an MSI-enabled endpoint, Mediatrace will start from the MSI-enabled endpoint itself (not from the nearest Medianet-enabled router). In addition, the Mediatrace Flow Information is not displayed for the source MSI-enabled endpoint from where Mediatrace is initiated.

• 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:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTS</td>
<td>CTS, CTMS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, Polycom, E20, Router</td>
</tr>
<tr>
<td>C_CODEC</td>
<td>CTS, CTMS, VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, MCU, Polycom, E20, Router</td>
</tr>
<tr>
<td>CIUS</td>
<td>CTS, CTMS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, MCU, Polycom, E20</td>
</tr>
<tr>
<td>MXP</td>
<td>CTS, CTMS, VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, MCU, Polycom, E20</td>
</tr>
<tr>
<td>Phone</td>
<td>CTS, CTMS, VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber, MCU, Polycom, E20</td>
</tr>
</tbody>
</table>

**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.
### Source | Destination
--- | ---
Cisco Jabber | CTS, CTMS, VCS, C_CODEC, TPS, CIUS, MXP, IP Phone, Cisco Jabber MCU, Polycom, E20
POLYCOM | CTS, (CTMS) VCS, C_CODEC, TPS, CIUS, MXP, MCU, PHONE, Cisco Jabber, Polycom, E20
E 20 | E20, CTS, (CTMS), VCS, C_CODEC, TPS, CIUS, MXP, MCU, PHONE, Cisco Jabber, Polycom
Switch | Switch, Router
Router | Switch, Router, C_CODEC, MCU, TPS, (CTMS)
VSAA | VSAA
CTMS | CTS, Router
MCU | C_CODEC, E20, MXP, CUIS, IP Phone, Cisco Jabber, Polycom, Router
TPS | C_CODEC, E20, MXP, CTS, CUIS, IP Phone, Cisco Jabber, Polycom, Router
VCS | C_CODEC, E20, MXP, CUIS, IP Phone, Cisco Jabber, Polycom

### Source | Destination
--- | ---
Cisco endpoint | Cisco endpoint, MCU, TPS, virtual TPS, VG, CUBE, VCS, Expressway-Core, Unknown endpoint

---

**Note**

- Cisco Prime Collaboration supports troubleshooting only when the source device is a Cisco endpoint that contains 5-tuple information.
- Cisco Prime Collaboration does not support troubleshooting for Cisco Jabber endpoints.

---

**Traceroute Command**

Endpoints with the traceroute or traceroute equivalent command enabled show the path or direction of troubleshooting. While most endpoints have this command enabled, few endpoints such as Cisco Jabber and Polycom do not support this.

For the endpoints that do not support the traceroute or traceroute equivalent command, the First Hop Router (FHR) is determined first. Pathtrace is performed from the first hop router to the destination endpoint. After
this is complete, the source endpoint to the first hop router is stitched, and the complete path from source endpoint to destination endpoint is shown in the path topology. The first hop router information is available for endpoints such as Cisco Cius, IP Phones, and so on using the HTTP interface of the device.

For certain endpoints, such as the Cisco Jabber and Polycom, Cisco Prime Collaboration cannot get the FHR information from the endpoint itself. For these endpoints, Cisco Prime Collaboration initiates the traceroute command from the linux virtual machine appliance to the source endpoint. The result of the traceroute command is processed and the last hop router before the endpoint in Cisco Prime Collaboration’s traceroute is considered as first hop router for the endpoint.

Note

- If you have deployed Cisco Prime Collaboration in MSP mode, the endpoints and/or the FHR or FHS which ever acts as Initiator must be in Managed state as these devices are not auto-discovered.
- You need to manually manage the preceding devices with customer information to perform traceroute.

Cisco Performance Monitor

Cisco Performance Monitor (Performance Monitor) enables you to monitor the flow of packets in your network and become aware of any issues that might impact the flow before it starts to significantly impact the performance of the application. Performance monitoring is especially important for video traffic because high quality interactive video traffic is highly sensitive to network issues. Even minor issues that may not affect other applications can have dramatic effects on video quality.

Cisco Prime Collaboration uses the performance monitor feature within medianet to display the flow statics. There can be multiple traffic flows passing through a device at any time. Cisco Prime Collaboration monitors the flow on a single interface at a time. You can view the flow statics for all IP or only RTP.

You must manually select the interface to monitor the flow. Cisco Prime Collaboration uses SNMP to poll the interface for the flow statics details.

You must configure the performance monitor on the network devices. The following documents help you to enable the performance monitor feature on network devices.

Table 73: Additional Information Resources

<table>
<thead>
<tr>
<th>For Information About . . .</th>
<th>See . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Medianet features</td>
<td>Cisco Enterprise Medianet home page</td>
</tr>
<tr>
<td>Specific Cisco Medianet features utilized by Collaboration Manager</td>
<td>Cisco IOS feature pages</td>
</tr>
<tr>
<td>Cisco Performance Monitor and configuring and Cisco Performance Monitor</td>
<td>Configuring Performance Monitoring</td>
</tr>
</tbody>
</table>

Start a Troubleshooting Workflow

You can start the troubleshooting workflow for a session from the 360° Session View in the Session Diagnostics page.
To reduce troubleshooting time, it is recommended that the devices in the media path are already discovered and available in Device Inventory before you start troubleshooting.

You can start the troubleshooting workflow for an endpoint from the quick view window in the Endpoint Diagnostics page.

Table 74: Launch Points for the Troubleshooting Workflow

<table>
<thead>
<tr>
<th>Troubleshooting Type</th>
<th>Launch Points</th>
</tr>
</thead>
</table>
| Automatic            | 1  Choose Assurance Administration > Session Path Threshold Settings.  
                       | 2  Set the threshold value for Rx Packet Loss, Average Period Jitter, and Average Period Latency, based on your requirement. 
                       | 3  Click Save. |
| Automatic            | 1  Choose Diagnose > Session Diagnostics.  
                       | 2  Select a scheduled session.  
                       | 3  Rest your mouse pointer over the Session Subject column in the Video Collaboration Session table and click the 360° Session view icon.  
                       | 4  Click Add to Watch List. |
| Automatic            | 1  Choose Diagnose > Session 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.  
                       | The troubleshooting workflow starts as soon as the endpoint joins a session. |
| Manual               | 1  Choose Diagnose > Session Diagnostics.  
                       | 2  Select an in-progress session. We recommend that you select an alarmed in-progress session.  
                       | 3  Rest your mouse pointer over the Session Subject column in the Video Collaboration Session table and click the 360° Session view icon.  
                       | 4  Click icon to launch the Troubleshooting page and select the direction from where you want to start the troubleshooting. |
**Troubleshooting Type** | **Launch Points**
--- | ---
**Manual** | 1. Choose **Diagnose > Session Diagnostics**.  
2. Select an in-progress session. We recommend that you select an alarmed in-progress session.  
3. Rest your mouse pointer over the network link (if there is an alarm on the network link) in the Session topology pane and click the 360° Session view icon.  
4. Click **Troubleshoot Network Link**.

---
**Manual** | 1. Choose **Diagnose > Session 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.

---

**MSI-enabled Device Troubleshooting**

Cisco Mediatrace enables you to isolate and troubleshoot network degradation problems for data streams. When Mediatrace-capable devices are deployed in the network, Cisco Prime Collaboration provides network path visibility, down to the granularity of video flow statistics.

If an endpoint supports Media Services Interface (MSI) for Mediatrace, Cisco Prime Collaboration will use this interface to obtain Mediatrace information, discover media path, and collect statistics for the various midpoints.

If MSI is not enabled on an endpoint, Cisco Prime Collaboration will log into the endpoint, obtain 5 tuple information, and use that information to start Mediatrace from a nearby router or switch.

When you start troubleshooting from a MSI-enabled endpoint, Mediatrace will start from MSI-enabled endpoint itself (not from the nearest Medianet enabled router).

The MSI Highgate is enabled on Cisco Unified IP Phones 8941 and 8945 endpoints by default. However to use the PCA-MSI Highgate feature, you need to complete the PCA-MSI Highgate Certificate Exchange on the Cisco Unified Communications Manager cluster for which you want to use the feature. For information on PCA-MSI Highgate Certificate Exchange, see the Setting up Devices for Prime Collaboration Assurance wiki. Ensure that these endpoints (Cisco Unified IP Phones 8941 and 8945) are set to full visibility to use the feature.

---

**Note**

MSI Highgate is enabled only for Cisco Unified IP Phones 8941 and 8945 endpoints.
MSI-enabled endpoints are displayed with Medianet badge (see the following figure) in the troubleshooting path topology.

Figure 9: Troubleshooting for MSI-enabled Endpoint

---

**Note**

MSI-enabled endpoints must be discovered using the MSI credentials. For more information on MSI credentials, see Credential Profiles Field Descriptions.

---

**Troubleshoot Data Analysis**

You can view troubleshooting data for both in progress sessions and completed sessions, if manual or automatic troubleshooting is/was activated for sessions or endpoints. During the troubleshooting job, the path between the endpoints is discovered. After the path is discovered, the network device details are collected. The inventory is updated with the discovered network devices details.

You can see mediatrace statistics for devices that are not in Managed state (Unreachable, Unsupported, Undiscoverable, and devices not in Device Inventory) in Device Inventory. In this case, ensure that there is a Mediatrace Initiator in the troubleshooting path, in a managed state and should report the statistics for the devices.

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 and Cisco Prime Collaboration is able to discover the devices.
- A dotted line between the devices indicates that the devices may not be connected and Cisco Prime Collaboration is not able to discover the devices, based on the CDP link details.
The following image shows a troubleshooting session between endpoints.

**Figure 10: Troubleshooting Session Between Endpoints**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Troubleshooting results tab. Based on the configurations (mediatrice, performance monitor) on the devices, some of the tabs may not be displayed.</td>
</tr>
<tr>
<td>2</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>Mediatrace enabled devices are displayed with an additional badge on the device.</td>
</tr>
<tr>
<td>4</td>
<td>Inaccessible devices are displayed in gray</td>
</tr>
<tr>
<td>5</td>
<td>An alarm badge on the endpoint indicates that there is a fault in the endpoint.</td>
</tr>
<tr>
<td>6</td>
<td>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 Session Path Threshold Settings page (Assurance Administration &gt; Session Path Threshold Settings).</td>
</tr>
</tbody>
</table>
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, and mediatrace flow details.

The following table lists the system, interface, and flow details that are listed in the quick view.

Table 75: System, Interface, and Flow Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Hostname configured for the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used for managing the device. You can launch to the endpoint or infrastructure device log in page, using this link.</td>
</tr>
<tr>
<td>Mediatrace Capable</td>
<td>Mediatrace Role - Configured Cisco Mediatrace role on the device.</td>
</tr>
<tr>
<td>This information is</td>
<td>IP SLA Role - Configured IP SLA role on the device.</td>
</tr>
<tr>
<td>displayed only if you</td>
<td>Performance Monitor - Configured Performance Monitor.</td>
</tr>
<tr>
<td>have enabled Mediatrace on the device.</td>
<td></td>
</tr>
<tr>
<td>System Status</td>
<td>Physical Memory Utilization (in%) - Percentage of the physical memory utilization.</td>
</tr>
<tr>
<td>Swap Memory Utilization</td>
<td>Swap Memory Utilization (in%) - Percentage of the swap memory utilization.</td>
</tr>
<tr>
<td>(in%)</td>
<td>CPU Utilization (in%) - Percentage of the CPU utilization.</td>
</tr>
<tr>
<td>Multipoint Switch</td>
<td>Number of Active Meetings - Number of active sessions defined in the multipoint switch.</td>
</tr>
<tr>
<td>Number of Segments Used</td>
<td>Number of segments (individual video displays) being used.</td>
</tr>
<tr>
<td>Interface Details</td>
<td>Speed - Speed of the interface, in Mbps as specified in the snmpifSpeed object.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Operational state of the interface as specified in the ifAdminStatus object.</td>
</tr>
<tr>
<td>Operation Status</td>
<td>Administrative status of the interface as specified in the ifOperStatus object.</td>
</tr>
<tr>
<td>Input Metrics</td>
<td>The data displayed are based on the RFC1213 MIB attributes.</td>
</tr>
<tr>
<td>Output Metrics</td>
<td>The data displayed are based on the RFC1213 MIB attributes.</td>
</tr>
</tbody>
</table>
This is displayed only if you are managing these devices in the Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime LMS.

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.

The flow information is displayed only if you have configured Cisco IOS Performance Monitor on the device.

Cisco Prime Collaboration inventory uses the DNS name (or the IP address if the DNS name is unavailable) for all devices. But the sysname is displayed for all midpoints in the troubleshooting path topology. The DNS name or IP address of the midpoint is displayed in the quick view.

During troubleshooting, if a device is inaccessible, the troubleshooting workflow skips that device. You must update the credentials, rediscover the device, and continue troubleshooting.

### Logs

You can view the detailed troubleshooting workflow status using the Log tab. The log file contains the following information:

- When the troubleshooting workflow started and ended.
- How the troubleshooting started and whether it is automatic or manual.
- When the endpoint system details were retrieved.
- When the path discovery started and ended.
- Whether there were any problems while retrieving the path topology details.
- When the polling started.
- Faults that occurred in any of the devices in the path topology.
**Medianet Path View**

The Medianet Path View contains output from each mediatrace-enabled device. Cisco Prime Collaboration analyzes and shows hop and statistics information for Mediatrace sessions (video flows).

The following graphs are displayed in the Medianet Path View View:

**CPU and Memory**

The graph is displayed for all devices and includes the following information:

- The vertical axis (y-axis) provides 1-minute CPU utilization details as a percentage.
- The horizontal axis (x-axis) provides lists of all network devices that were discovered during the path trace. The devices in gray indicate that the Cisco Mediatrace is not configured.
- The spheres in the graph provides 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 mediatrace flow details.

**CPU and Packet Loss**

This graph is displayed *only for Cisco Mediatrace-configured* devices and includes the following information:

- The vertical axis (y-axis) provides 1-minute CPU utilization details as a percentage.
- The horizontal axis (x-axis) provides lists of all network devices that were discovered during the path trace. The devices in gray indicate that the Cisco Mediatrace is not configured.
- 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 mediatrace is not configured on the device and hence the video packet loss data are not available.

*Figure 11: CPU and Packet Loss Graph*

Click on the sphere or square box (red icon) to view the system, interface, and mediatrace flow details.

**Video IP Bit Rate and Packet Loss**

This graph is displayed only for Cisco Mediatrace-configured 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 devices in gray indicate that the Cisco Mediatrace is not configured.
- The spheres in the graph indicate 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.
No sphere indicates that the Cisco Mediatrace is not configured on the device and hence the video packet loss data are not available.

**Figure 12: Video IP Bit Rate and Packet Loss Graph**

This graph is displayed only for Cisco Mediatrace-configured 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 devices in gray indicate that the Cisco Mediatrace is not configured.
- 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.

Click on the sphere (red icon) to view the system, interface, and mediatrace flow details.

**Video Interarrival Jitter and Packet Loss**

This graph is displayed only for Cisco Mediatrace-configured 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 devices in gray indicate that the Cisco Mediatrace is not configured.
- 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.
No sphere indicates that the Cisco Mediatrace is not configured on the device and hence the video packet loss data are not available.

*Figure 13: Video Interarrival Jitter and Packet Loss Graph*

Click on the sphere (red icon) to view the system, interface, and mediatrace flow details.

**IP DSCP and Packet Loss**

This graph is displayed only for Cisco Mediatrace-configured 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 devices in gray indicate that the Cisco Mediatrace is not configured.
- 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, lesser the video packet loss.
  - No sphere indicates that the mediatrace is not configured on the device and hence the video packet loss data are not available.

Click on the sphere (red icon) to view the system, interface, and mediatrace flow details.

**Medianet Enabled Network**

Medianet enhances visibility into the network to simplify and accelerate troubleshooting. In Cisco Prime Collaboration, the following are the key differences between a medianet-enabled network and a non-medianet-enabled network.
View All Flows

This information is displayed only if you have configured Cisco IOS Performance Monitor on the device. To view the flow of the packets in your network:

**Procedure**

1. **Step 1** Select a device in the troubleshooting topology. Ensure that the Performance Monitor field shows Configured.
2. **Step 2** Click View All Flows.
3. **Step 3** Select the interface where you want to monitor the packet flow.
4. **Step 4** Select the type of the traffic.
5. **Step 5** Click Start. See Performance Monitor for the details that are displayed.

**Performance Monitor**

The flow statics data is both static and dynamic. The 5-tuple data is static; whereas the bit rate, packet loss, jitter are dynamic, which changes at every measurement interval. All static data is collected from the selected
interface only once for every flow at the start of the session. The dynamic data is collected on every user interface refresh request. The historical statics data is not stored in the database.

**Figure 14: Performance Monitor**

The interface that you have selected is displayed either as ingress or egress. Cisco Prime Collaboration displays all the flow details for the selected interface.

**Table 76: Flow Details of the Interface**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Selection</td>
<td>Selected device details.</td>
</tr>
<tr>
<td>Interface</td>
<td>Selected interface on the device.</td>
</tr>
<tr>
<td>Type of Traffic Selected</td>
<td>Whether the selected traffic is All or RTP.</td>
</tr>
<tr>
<td>Maximum Bandwidth</td>
<td>Maximum available bandwidth for the interface in Mbps.</td>
</tr>
<tr>
<td>Interface Usage / Interface Utilization</td>
<td>Utilization of the selected interface in Kbps.</td>
</tr>
<tr>
<td>Flow Usage / Flow Usage Pie Chart</td>
<td>This value is the sum of the bandwidth utilized by the individual flows for the selected interface in the following table.</td>
</tr>
</tbody>
</table>

**Table 77: Individual Flow Usage Details for of the Interface**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress</td>
<td>Details on ingress interface.</td>
</tr>
</tbody>
</table>
Path Assessment

You can view the troubleshooting summary information for testable devices, nontestable device, mediattrace-enabled devices, 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 troubleshooting is complete for the session.

**Note**

- Path Assessment tests can be performed only on midpoints that are in the Managed state and have CLI access level (RW/RO). Path Assessment tests cannot be performed on the endpoints.
- If you have deployed Cisco Prime Collaboration in MSP mode, in a NAT environment, path assessment is not supported for a device with a private IP only.

The following table lists the types of path assessment tests.

<table>
<thead>
<tr>
<th>Source</th>
<th>Name of the source device (from where the packet flow started).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>Details on egress interface.</td>
</tr>
<tr>
<td>Destination</td>
<td>Name of the destination device.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used for the packet flow.</td>
</tr>
<tr>
<td>Source and Destination Port</td>
<td>Port used for the flow.</td>
</tr>
<tr>
<td>Application</td>
<td>Type of the application.</td>
</tr>
<tr>
<td>Application Category</td>
<td>Whether audio, video, or other category.</td>
</tr>
<tr>
<td>Bandwidth (bps)</td>
<td>Bandwidth used by the application.</td>
</tr>
<tr>
<td>Packet Loss (%)</td>
<td>Packet loss for audio and video.</td>
</tr>
<tr>
<td>Jitter (ms)</td>
<td>Jitter for audio and video.</td>
</tr>
<tr>
<td>Category</td>
<td>Tests</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Controller slips</td>
</tr>
<tr>
<td></td>
<td>Collisions in output queue</td>
</tr>
<tr>
<td></td>
<td>Controller path code violations</td>
</tr>
<tr>
<td></td>
<td>Input queue drops</td>
</tr>
<tr>
<td></td>
<td>Output queue drops</td>
</tr>
<tr>
<td></td>
<td>Controller line code violations</td>
</tr>
<tr>
<td></td>
<td>Controller line errors</td>
</tr>
<tr>
<td></td>
<td>Flapping interfaces</td>
</tr>
<tr>
<td></td>
<td>Duplex mismatch</td>
</tr>
<tr>
<td></td>
<td>Controller errored seconds</td>
</tr>
<tr>
<td></td>
<td>Babbles in output queue</td>
</tr>
<tr>
<td></td>
<td>Errors in output queue</td>
</tr>
<tr>
<td></td>
<td>Controller frame loss</td>
</tr>
<tr>
<td>Classification/Marking</td>
<td>DSCP-CoS mapping</td>
</tr>
<tr>
<td></td>
<td>CoS-DSCP mapping</td>
</tr>
<tr>
<td>Trust</td>
<td>Trust configuration.</td>
</tr>
<tr>
<td>Queuing</td>
<td>Egress priority queue</td>
</tr>
<tr>
<td></td>
<td>LLQ burst value</td>
</tr>
<tr>
<td></td>
<td>CBWFQ queue limit</td>
</tr>
<tr>
<td></td>
<td>CBWFQ/LLQ check</td>
</tr>
<tr>
<td>Policing/Shaping</td>
<td>CBWFQ/LLQ for video streams</td>
</tr>
<tr>
<td></td>
<td>Output policy-map scan for video traffic</td>
</tr>
</tbody>
</table>

**Test Result**

Test result is displayed as follows:
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Check Mark]</td>
<td>Indicates passed. The test result is passed, only if all tests are passed for a device/category.</td>
</tr>
<tr>
<td>![X]</td>
<td>Indicates failed. The test result is failed, if at least one test has failed for a device/category.</td>
</tr>
<tr>
<td>![Question Mark]</td>
<td>Indicates that for some reason the test could not be executed, and the result is unknown. For example, if CDP is not enabled, then the ingress and egress interfaces are not determined. As a result, tests such as Trust DSCP cannot be executed and the results are unknown.</td>
</tr>
</tbody>
</table>

If the test has failed (shown by icon), click the quick view icon on the Result Field, to see the root cause and recommendation for the test.

You can select devices you are interested in, and click the arrow next to the IP address of the device to see the details of the test performed for the device.

To further troubleshoot a single device, rest your mouse pointer over the result column for the failed/unknown test result and click the quick view to see the root cause and recommendation. There is no quick view available for the passed tests.

---

**Note**

All session and troubleshooting details older than 14 days are purged, every hour.

### Export Troubleshooting Data

You can export the data only after the session ends. After the troubleshooting job is completed, the troubleshooting job status is displayed in the Session Monitoring page.

To export the troubleshooting data:

**Procedure**

1. **Step 1** Choose **Diagnose > Session Diagnostics**. The Session Diagnostics page is displayed.
2. Choose **Diagnose > Conference Diagnostics**. The Conference Diagnostics page is displayed.
3. **Step 2** Select a past session, where the troubleshooting status icon displays Troubleshooting Report Available.
4. **Step 3** Rest your mouse pointer over the Session Subject column in the Video Collaboration Session table and click the 360° Session view icon.
5. **Step 4** Click **Export Troubleshooting Data** icon in the 360° Session 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:

<table>
<thead>
<tr>
<th>Report Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Identifier</td>
<td>A unique ID for the session.</td>
</tr>
<tr>
<td>Session Subject</td>
<td>Displays whether the session is ad hoc, scheduled, or static.</td>
</tr>
<tr>
<td>Session Date</td>
<td>Date when the session occurred.</td>
</tr>
<tr>
<td>Session Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Session Duration in Minutes</td>
<td>Duration of the session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Displays whether the session is point-to-point or multipoint.</td>
</tr>
<tr>
<td>Endpoints</td>
<td>Details of the endpoints that were part of the session.</td>
</tr>
<tr>
<td>Call Segment</td>
<td>Displays the direction that was used while troubleshooting.</td>
</tr>
<tr>
<td>Troubleshooting Session</td>
<td>Start and end time of troubleshooting workflow.</td>
</tr>
<tr>
<td>Troubleshooting Session ID</td>
<td>A unique ID for the troubleshooting workflow.</td>
</tr>
<tr>
<td>Troubleshooting Start Time</td>
<td>Start time of the troubleshooting workflow.</td>
</tr>
<tr>
<td>Troubleshooting Initiation</td>
<td>Displays whether the troubleshooting was started manually or whether it started automatically.</td>
</tr>
</tbody>
</table>

Path Topology and Metrics

The following are the fields and their description:

- 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.
Cisco Mediatrace enables you to isolate and troubleshoot network degradation problems for data streams. Although it can be used to monitor any type of flow, it is primarily used with video flows. It can also be used for nonflow-related monitoring, along a media flow path.

It dynamically enables monitoring capabilities on the nodes along the path, and collects information on a hop-by-hop basis.

Prerequisites:

- You must enable the Mediatrace on each network node that you want to collect flow information from.
- You must enable the Mediatrace Initiator on the network node that you use to configure, initiate, and control the Mediatrace sessions or polls.
- You must enable the Mediatrace Responder on each network node that you want to collect information from.
- You must verify whether the Mediatrace initiator and responder features are enabled on the device using Cisco Prime Collaboration Inventory.

If you have enabled Cisco Mediatrace on your network nodes, Cisco Prime Collaboration provides Medianet Path View as part of the troubleshooting data. The Medianet Path View includes a graphical view of:

- CPU and packet loss
- Video IP bit rate and packet loss
- Video interarrival jitter and packet loss
- IP DSCP and packet loss

Cisco TelePresence TC and TE Software, version 6.0 and later, supports MSI so the endpoint itself can be the mediatrace Initiator if MSI credentials are provided. Cisco TelePresence TC and TE software, version 6.0 and later also supports CDP. For Cisco TelePresence System C and EX series with version 6.0, you can mediatrace from L2 switch connected to the endpoint in case mediatrace is not started from the endpoint.

**Note**

- In case mediatrace from L2 switch to the endpoint does not work, please rediscover the switch from Inventory Management.
- From the phone endpoint, mediatrace from L2 switch is not supported.
WSMA and SNMP Support in Mediatrace 3.0

If you have installed Mediatrace 3.0, WSMA credentials are not mandatory although both WSMA and SNMP are supported. Cisco Prime Collaboration allows you to configure and poll mediatrace statistics, using SNMP credentials.

If the device is a Mediatrace initiator and has SNMP Write credentials, these credentials are used to provision Mediatrace; However, if SNMP Write credentials are not provided, and CLI Read-Write is provided, then WSMA is used to provision Mediatrace.

Cisco Mediatrace on Switches

You must enable Cisco Mediatrace on the switches from which you want to collect the flow information.

Prerequisites:

- You must ensure that the Mediatrace Initiator role is configured to the first hop switch. This is the node closest to the source.
- You must ensure that the switch is directly connected to the endpoint (connection must not be a dotted line). Also, CDP must be enabled on the switch.
- You must ensure that the voice VLAN ID is configured on the ingress interface for Layer 2 switches.
- You must ensure that the IP RSVP snooping for Layer 2 switches (you need not configure IP RSVP snooping for Layer 3 switches) is configured.

For Cisco C or Cisco EX series devices, Cisco Prime Collaboration does not support CDP. As a result, you cannot initiate Mediatrace from a switch if the source is a Cisco C or Cisco EX series device.

Cisco Mediatrace Diagnostics

This information is displayed only if you have enabled Mediatrace on the device. If the mediatrace statistics is not available, that is, mediatrace flow information does not appear in the quick view, Cisco Prime Collaboration supports application diagnostics to understand why it is not displayed.

You must click Run Diagnostics from the quick view, to see the root cause and recommendation. Cisco Prime Collaboration checks the following:

- Cisco Prime Collaboration has CLI access to the device
- Cisco Mediatrace initiator role is configured on the device
- Cisco Mediatrace responder role is configured on the device
- WSMA is configured
- HTTP server is configured
- Cisco Mediatrace is provisioned for the session
- Cisco Mediatrace license is installed on the device
- Call is on hold (applicable to CTS only).
Cisco Mediatrace 2.0 is not supported in this release. If you are using a device with an IOS image that supports Cisco Mediatrace 2.0, note the following points while you are troubleshooting using Cisco Mediatrace:

- If a device having Cisco Mediatrace 2.0 configured with Cisco Mediatrace Initiator role, Cisco Prime Collaboration does not start Mediatrace sessions from the device. But the Mediatrace role for that device might be shown as Initiator or Initiator/Responder in the Device Inventory page (Device Inventory > Current Inventory table). If the IOS image version of the device is 15.2(3)T (which has Cisco Mediatrace 2.0), an error message will be displayed in the Troubleshooting Logs tab.

- If the devices having Cisco Mediatrace 2.0 are configured with Mediatrace Responder role, you can view the Mediatrace statistics for these devices only if the Initiator device used during troubleshooting has Cisco Mediatrace 1.0.

**Cisco Prime Infrastructure Cross-Launch**

Cisco Prime Collaboration 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.

Cisco Prime Collaboration 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 applications.
- You must ensure that all the required credentials for routers and switches are added in Cisco Prime Collaboration. For more information, see the Setting Up Devices for Prime Collaboration Assurance wiki page.
- You must ensure that the network devices that contain the Cisco Prime Infrastructure software is accessible from Cisco Prime Collaboration.

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**

To setup cross-launch for Cisco Prime Infrastructure:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>System Administration &gt; 360 Integration</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the required details in the Cisco Prime Infrastructure Setup pane. See <a href="#">Cisco Prime Infrastructure Pane - Field Descriptions</a> for more details on field descriptions.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**Cisco Prime Infrastructure Pane - Field Descriptions**

*Table 78: Field Descriptions for the Cisco Prime Infrastructure Pane*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Prime Infrastructure Server</td>
<td>Hostname or the IP address of the Infrastructure server. If you have deployed the Cisco Prime Infrastructure in a multiserver setup, you must enter the Cisco Prime Infrastructure master server details.</td>
</tr>
<tr>
<td>Prime Infrastructure User and Password</td>
<td>A dummy user, configured on the Cisco Prime Infrastructure server. 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</td>
</tr>
</tbody>
</table>
Media Path Analysis

This section contains the following:

- Analyze Media Paths Using VSAA, page 411
- Manage a Video Test Call, page 414

Analyze Media Paths Using VSAA

The Video SLA Assessment Agent (VSAA) is used in Cisco Prime Collaboration 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 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 software download site on Cisco.com. See Video SLA Assessment Agent 3.1 Installation Guide for the installation guidelines.

Procedure

Step 1  Choose Diagnose > Media Path Analyzer.
Step 2  Enter the required assessment details.
Step 3  Enter the Table 79: Profile Details.
Step 4  Click Start.
Table 79: Profile Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Displays the profile settings you want to assess. RTP packets sent will be of based on the device type.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of devices or streams you want to add to the network. You can add upto five devices.</td>
</tr>
<tr>
<td>DSCP</td>
<td>DSCP value indicates priority to traffic quality. The highest quality DSCP value is selected to ensure good quality video streaming.</td>
</tr>
</tbody>
</table>

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 Medianet Path View contains output from each mediatrace-enabled device. 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, non testable device mediatrace-enabled devices, , 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 session. For more information, see Path Assessment.

The Test Result tab displays the following charts. For these charts, only the results of last twenty tests are displayed.
Test Summary

Figure 15: Test Summary

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Video Result</th>
<th>Audio Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSP</td>
<td>a1h2(36)</td>
<td>a1h2(36)</td>
</tr>
<tr>
<td>Profile</td>
<td>E15-10000</td>
<td>E15-10000</td>
</tr>
<tr>
<td>Max Rate</td>
<td>30.02 frames/s</td>
<td>50.04 packets/s</td>
</tr>
<tr>
<td>Total Packets Lost</td>
<td>439079 packets</td>
<td>44627 packets</td>
</tr>
<tr>
<td>Total Packet Loss</td>
<td>0 packets</td>
<td>0 packets</td>
</tr>
<tr>
<td>Maximum Seconds of Concealment</td>
<td>0.0 s</td>
<td>0.0 s</td>
</tr>
<tr>
<td>Maximum Jitter</td>
<td>0.01 ms</td>
<td>0.03 ms</td>
</tr>
<tr>
<td>Maximum Peak-To-Peak Jitter</td>
<td>0.81 ms</td>
<td>0.85 ms</td>
</tr>
<tr>
<td>Maximum Peak Playout Delay</td>
<td>0.87 ms</td>
<td>0.83 ms</td>
</tr>
<tr>
<td>Maximum Latency</td>
<td>2.32 ms</td>
<td>2.31 ms</td>
</tr>
<tr>
<td>Maximum Frame Jitter Average</td>
<td>0.01 ms</td>
<td>0.0 ms</td>
</tr>
<tr>
<td>Time Obtained</td>
<td>21:47:52 PDT</td>
<td>21:47:52 PDT</td>
</tr>
</tbody>
</table>

Peak-to-Peak Jitter

Figure 16: Peak-to-Peak Jitter Graph
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, session statistics, endpoint statistics, and network topology with medianet statistics like other calls. Only the CTS, C and EX series codecs are supported for this call.
• 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 in MSP mode.

### Table 80: Managing a Video Test call

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| • Start a video test call from **Endpoint Diagnostics** (Under Diagnose)  
• Start a video test call from **Session Diagnostics** (Under Diagnose) | Select the video endpoints, and click **Video Test Call**, to create a test call between two selected endpoints.  
**Note**  
• 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.  

or  
Select a particular session on the Session Diagnostic page, and click **Video Test Call**, to create a test call for that scheduled session.  
**Note**  
This button gets activated only after you select a scheduled session. To see the list of the list of scheduled sessions, filter for scheduled sessions. Remember to select a session for a future time and date only.  
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.  
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.  
The scheduled call details can be seen on the Session Diagnostics page. You can see events and alarms, session statistics, endpoint statistics, and network topology with medianet statistics like other calls. This information is available for completed test calls also. You can stop the call immediately if it causes a problem on the network.  

**Stop a running video test call** | 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 Sessions Diagnostic page, by setting the filter to Test Call Sessions. Hover around the session subject to launch the 360° Session View, and click the Stop Call icon to stop the in progress video test call.  
Test call lasts for around 5 minutes, after which it automatically stops. |
### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a scheduled video test call from Video Test Call Configurations page Synthetic Test Center &gt; Video Test You can also view or delete video test calls from the same page.</td>
<td>To edit a video test call, click <strong>Edit</strong>, and reschedule or run the call immediately by clicking <strong>Save</strong>. A message appears to notify you that the call has been modified successfully.</td>
</tr>
</tbody>
</table>
Collect Logs

Cisco Prime Collaboration 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 Call Signaling 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 Call Signaling 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 user interface.
- For Standard mode, the devices should be in Managed state in Device Work Center.

The following is required/supported by this feature:

<table>
<thead>
<tr>
<th>Description</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum disk size required for this feature.</td>
<td>25 GB for small, 50 GB for medium, and very large profiles</td>
</tr>
<tr>
<td>Maximum number of devices from which log collection to be done concurrently.</td>
<td>100</td>
</tr>
<tr>
<td>Maximum number of log collection jobs to be run at the same time</td>
<td>3</td>
</tr>
<tr>
<td>Maximum size of a zipped log file that can be downloaded at one instance.</td>
<td>0.5 GB for small, and 1 GB for other profiles.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
</tbody>
</table>
Note

- Only logs collected from System CLI tool or another Cisco Prime Collaboration server 10.5 and later are supported.

- Time zone of the device is not collected from the System CLI tool.

- If you are using Cisco Prime Collaboration Assurance - Standard mode, you can add CVP, CUC, Cisco IM & P, and Unified CCE to Log Collection Center. Also, you can collect logs for a single cluster only.

- 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 Log Collection Center menu pages.

Log Collection Center

Cisco Prime Collaboration enables you to collect call logs from the Log Collection Center (LCC) available at Diagnose > Log Collection Center for the following Unified Communications (UC) components:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Supported Release</th>
<th>Components or Type of Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Contact Center Enterprise (Unified CCE)</td>
<td>9.x and later</td>
<td>Router, and Peripheral Gateway</td>
</tr>
<tr>
<td>Cisco Voice Portal (CVP)</td>
<td>9.x and later</td>
<td>All</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager (Unified CM)</td>
<td>9.x and later</td>
<td>All</td>
</tr>
<tr>
<td>IOS Gateways (TDM, CUBE (Enterprise Edition), VXML GWs)</td>
<td>15.1(4)M and later</td>
<td>Output of show logging command</td>
</tr>
<tr>
<td>Cisco Unity Connection (CUC)</td>
<td>9.x and later</td>
<td>All</td>
</tr>
<tr>
<td>Cisco IM and Presence</td>
<td>9.x and later</td>
<td>All</td>
</tr>
</tbody>
</table>

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 Log Collection Center, 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 Log Collection Center (LCC).

• TimeZone - Displays the device time zone.

Sync a Device with Device Inventory
To add or update device(s) (UC components) of Device Inventory to Log Collection Center (LCC), you can select a device, all devices of a device group and then click Sync to Inventory Management. The devices in the Log Collection Center (LCC) and Device Inventory are synched in the following ways:

• Automatically: Devices from Device Inventory are synched 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 Log Collection Center.

Periodic sync happens every hour. Sync does not remove devices from LCC if the devices in Device Inventory are deleted. If a new device is added in Log Collection Center (LCC) 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 Log Collection Center.

• The credentials from LCC are overwritten by the credentials in Device Inventory after a sync. Thus we recommend you to keep the credentials same across Device Inventory and LCC.

• Only the devices in Managed state in Device Inventory are synched.

• If a device in Device Inventory is deleted but not deleted in LCC, you can still perform log collection in Log Collection Center.

• If the IOS gateway in Device Inventory does not have CLI credentials, it will not be synched to Log Collection Center.

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Group</td>
<td>Click Diagnose &gt; Log Collection Center &gt; Group &gt; Create New.</td>
</tr>
<tr>
<td>Edit a Group</td>
<td>Click Diagnose &gt; Log Collection Center, select a device or a group, and then click Group &gt; Edit Group.</td>
</tr>
</tbody>
</table>
## 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

### Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a Group</td>
<td>Click <strong>Diagnose &gt; Log Collection Center</strong>, select a device or a group, and then click <strong>Group &gt; Delete Group</strong>. It takes</td>
</tr>
<tr>
<td>Add Devices to Group</td>
<td>Click <strong>Diagnose &gt; Log Collection Center</strong>, select a device or a group, and then click <strong>Group &gt; Delete Group</strong>. It takes</td>
</tr>
<tr>
<td>Delete Devices from Group</td>
<td>Click <strong>Diagnose &gt; Log Collection Center</strong>, select device(s), and then click <strong>Group &gt; Add to Group</strong>.</td>
</tr>
<tr>
<td>View Devices in Group</td>
<td>Select a group from the Device Group Center. The devices of that group are displayed in the Devices pane.</td>
</tr>
</tbody>
</table>

### Other Tasks

You can perform the following tasks from the Device pane on the Log Collection Center page. Select device(s) from the Devices pane for which you want to perform the task, and then do the following as required.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify Credentials</td>
<td>Click the <strong>Modify Credentials</strong> button to edit the port number or credential details of device(s). You cannot modify the device type.</td>
</tr>
<tr>
<td>Modify Time zone</td>
<td>Click the <strong>Modify Time Zone</strong> button to modify the device time zone. Cisco Prime Collaboration server time zone is shown by default.</td>
</tr>
</tbody>
</table>

### 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. Also 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.
• Cisco Unity Connection
• Cisco IM and Presence

Choose **Diagnose > Log Collection Center**.

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:

**Procedure**

**Step 1** Choose **Diagnose > Log Collection Center**, 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**.

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 server IP address. This URL can be viewed by users with administrator role and helps you troubleshoot issues related to log collection.
Analyze Call Signaling

The Call Signaling Analyzer enables you to determine the reason of call failure. Call Signaling Analyzer analyzes calls at a high level and then drills down to a lower level within the components themselves using the same tool.

The Call Signaling 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:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Supported Release in Advanced Mode</th>
<th>Supported Release in Standard Mode</th>
<th>Components or Type Of Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Contact Center Enterprise (Unified CCE)</td>
<td>9.x and later</td>
<td>Not supported</td>
<td>Router</td>
</tr>
<tr>
<td>Cisco Voice Portal (CVP)</td>
<td>9.x and later</td>
<td>Not supported</td>
<td>All</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager (Unified CM)</td>
<td>9.x and later</td>
<td>9.x and later</td>
<td>Call logs, and SDL logs</td>
</tr>
<tr>
<td>IOS Gateways (TDM, CUBE (Enterprise Edition), VXML GWs)</td>
<td>15.1(4)M and later</td>
<td>Not supported</td>
<td>Output of show logging command</td>
</tr>
</tbody>
</table>
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.

• Ensure that you complete the configuration mentioned in following sections in the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page for Cisco Prime Collaboration Assurance 11.0:
  * 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"

• For Standard mode, the devices must be in Managed state in Device Inventory.

Note

• The Advanced mode allows log analysis from any of supported devices (Unified CM, CVP, IOS Gateway, Unified CCE) while the Standard mode allows only Unified CM devices from a single managed cluster only.

• 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 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 Call Signaling 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 Call Signaling Analyzer menu pages.

The following is required/supported by this feature:

<table>
<thead>
<tr>
<th>Maximum disk size required for this feature.</th>
<th>18 GB for small, 35 GB for medium, and large profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum file size that can be imported.</td>
<td>0.5 GB for small, and 1 GB for other profiles.</td>
</tr>
<tr>
<td>Maximum number of calls that can be selected for ladder generation at a time.</td>
<td>25</td>
</tr>
<tr>
<td>Maximum number of devices from which log collection to be done at a time.</td>
<td>100</td>
</tr>
</tbody>
</table>
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 1 GB 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**, page 425
- **Create a Call Ladder Diagram**, page 427
- **Filter a Message in the Call Ladder Diagram**, page 429
- **Understand a Call Ladder Diagram**, page 430

**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 19: Call Flow 1**

```
  ICM
 /   \
VXMPL  CUCM
 |     |
PSTN -> TDM -> GW -> CVP
```

**Figure 20: Call Flow 2**

```
  ICM
 /   \
VXMPL  CUCM
 |     |
PSTN -> CUBE -> CVP
```

**Figure 21: Call Flow 3**

```
PSTN -> GW -> CUCM -> IP phone
```

**Figure 22: Call Flow 3 A**

```
PSTN -> CUBE -> CUCM -> IP phone
```

**Figure 23: Call Flow 4**
Create a Call Ladder Diagram

Procedure

**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 Log Collection Center 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 Log Collection Center, see Log Collection Center, on page 418. 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
Create a Call Ladder Diagram

<table>
<thead>
<tr>
<th>Calling Number/URI</th>
<th>A SIP-URI is the SIP addressing schema to call another person through SIP. By default ALL listed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called Number/URI</td>
<td>By default ALL listed.</td>
</tr>
<tr>
<td>Disconnect Code</td>
<td>The error code for that call, for example - 200 OK.</td>
</tr>
<tr>
<td>Call ID</td>
<td>An ID that uniquely identifies calls in a Cisco UC product. Each Call Leg of a call has a different Call ID.</td>
</tr>
<tr>
<td>GUI ID</td>
<td>An ID that uniquely identifies calls across product.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>By default it displays the Cisco Prime Collaboration server time zone.</td>
</tr>
<tr>
<td>Heartbeat Messages</td>
<td>This includes the heartbeat messages - OPTIONS, and NOTIFY. If you select this field, performance of this feature may be adversely affected.</td>
</tr>
<tr>
<td>Time Range</td>
<td>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.</td>
</tr>
<tr>
<td>Device Type to Parse</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Number of Calls</td>
<td>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.</td>
</tr>
<tr>
<td>Initial Message</td>
<td>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.</td>
</tr>
<tr>
<td>Comment</td>
<td>You can add your comments to show when, where, and why the logs are collected.</td>
</tr>
</tbody>
</table>

**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 in 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.

**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 27: Transition Diagram*

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 [Setting Up Devices for Cisco Prime Collaboration Assurance 11.0](#) wiki page for Cisco Prime Collaboration Assurance 11.0.

---

**Filter a Message in the Call Ladder Diagram**

You can further create a call ladder diagram for a specific message.

**Procedure**

**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).

![Call Ladder Diagram](image)

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.
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 29: 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.
Understand a Call Ladder Diagram
PART VIII

Maintain the Server

• Manage Jobs, page 435
• Purge Policies, page 439
• Perform Backup and Restore, page 441
• Set Log Levels, page 447
Manage Jobs

Cisco Prime Collaboration 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 sessions. The polling jobs are triggered based on user-configured values.

Table 81: 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 81: Job Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description of the job as defined in the Cisco Prime Collaboration Assurance server.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the type of the job.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the job.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of a job. It can be:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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).</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Suspended—Job is halted temporarily and can be later resumed for execution.</td>
</tr>
<tr>
<td></td>
<td>• Running—Job is in execution.</td>
</tr>
<tr>
<td>Owner</td>
<td>User, who created the job. If it is a predefined system job, the creator is displayed as SYSTEM.</td>
</tr>
<tr>
<td>Job Start Time</td>
<td>Time when the job is scheduled to run for the first time.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run ID</td>
<td>If it is a periodic job, it displays the job instances count. If it is not a periodic job, it displays zero.</td>
</tr>
<tr>
<td>Status</td>
<td>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.</td>
</tr>
<tr>
<td>Status Progress</td>
<td>Indicates the stage of the job and the percentage complete.</td>
</tr>
<tr>
<td>Results</td>
<td>Indicates the job was successful or a failure.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Start time of a job instance of the same job.</td>
</tr>
<tr>
<td>End Time</td>
<td>End time of a job instance of the same job.</td>
</tr>
<tr>
<td>Duration</td>
<td>Time taken between the Start Time and End time of a job instance of the same job.</td>
</tr>
</tbody>
</table>

---

**Note**

For more information on Purge Policies, see Purge Policies Table, on page 439.

- Schedule a Job, page 436
- Cancel a Job, page 437
- Predefined Quick Filters, page 437

---

**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:
To schedule a job:

**Procedure**

**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.

**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.

**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 supports the following predefined quick filters:

**Note** Not all of these options are applicable to Cisco Prime Collaboration Standard mode.
• 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, either by using or by selecting a device and clicking Rediscover or Update Inventory.

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. For more information, see the section Discover Devices in the Cisco Prime Collaboration Assurance Guide - Advanced.

• All Polling Jobs—An example of a polling job is MCU_Session_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 CTS-Manager and 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).
Purge Policies

Cisco Prime Collaboration Assurance uses the following purge policies.

- Purge Policies Table, page 439

Purge Policies Table

<table>
<thead>
<tr>
<th>Module</th>
<th>Purge Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Faults</td>
<td>Cleared alarms are purged in 30 days (4 weeks).</td>
</tr>
<tr>
<td></td>
<td>Events are purged in 60 days (8 weeks).</td>
</tr>
<tr>
<td></td>
<td>If an alarm is purged, all associated events are also purged.</td>
</tr>
<tr>
<td></td>
<td>Active events and alarms are not purged.</td>
</tr>
<tr>
<td></td>
<td>If the threshold rules for any performance counter of a device are</td>
</tr>
<tr>
<td></td>
<td>purged, the associated active alarms are also purged.</td>
</tr>
<tr>
<td>Monitor the Network</td>
<td>All sessions and endpoint statistics data older than one day are purged.</td>
</tr>
<tr>
<td></td>
<td>All sessions and troubleshooting details older than 14 days are purged every hour.</td>
</tr>
<tr>
<td>Module</td>
<td>Purge Policy</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dashboards</td>
<td>Call quality event history, and audio/video phone audit report data older than 30 days are purged.</td>
</tr>
<tr>
<td></td>
<td>CDR reports older than seven days are purged.</td>
</tr>
<tr>
<td></td>
<td>CMR records older than seven days are purged.</td>
</tr>
<tr>
<td></td>
<td>Data from Sensor, older than seven days is purged.</td>
</tr>
<tr>
<td></td>
<td>Data from Cisco Prime NAM/vNAM, older than seven days is purged.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Perform Diagnostics</td>
<td>IP SLA Voice Test Data - Cisco Prime Collaboration 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.</td>
</tr>
<tr>
<td>Maintain the Server</td>
<td>Jobs that are older than 14 days and have a status of completed, failed, or cancelled are purged every hour.</td>
</tr>
<tr>
<td></td>
<td>Event and Alarm Database - All events and alarms, including active and cleared, are persisted in the Cisco Prime Collaboration 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.</td>
</tr>
<tr>
<td>Job Management</td>
<td>Jobs that are older than 32 days are purged.</td>
</tr>
</tbody>
</table>
Perform Backup and Restore

- Perform Backup and Restore, page 441

Perform Backup and Restore

You can schedule periodic backups using the Cisco Prime Collaboration Assurance user interface, or run backup commands manually by logging in to the system as an admin user (CLI user). However, you must manually run restore commands by logging in to the system as an admin user through VM console using the vSphere client. We recommend you to not to trigger the restore from SSH/Putty prompt.

For Cisco Prime Collaboration Analytics, based on your license type the Analytics & Assurance option is displayed in the Create New Backup page.

Overview of Backup and Restore

Cisco Prime Collaboration Assurance uses the following purge policy:

- All session and endpoint statistics data older than one day are purged. For more details, see the section Monitor Sessions in the Cisco Prime Collaboration Assurance Guide - Advanced.

- All session and troubleshooting details older than 14 days are purged every hour. For more details see the section Diagnostics for Video Endpoints in the Cisco Prime Collaboration Assurance Guide - Advanced.

- Call quality event history and audio/video phone audit report data older than 30 days are purged. For more details, see the section Purge Policies Table in the Cisco Prime Collaboration Assurance Guide - Advanced.

- 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. For more details, see the Concepts chapter in Cisco Prime Collaboration Assurance Guide - Advanced.

- 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:
### Folder Name | Type of Data
--- | ---
emms database | Database
/cpcm/conf | Configuration files
/cpcm/export | Troubleshooting and endpoint utilization reports
/cpcm/logs and tomcat/logs | Assurance application and Tomcat log files
/jre/lib/security | Keystore files

**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 Assurance 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.

**Procedure**

**Step 1** Log in to the Cisco Prime Collaboration Assurance 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:

```bash
admin# config terminal
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 Assurance 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 User Interface**

You can schedule and run backup for both Assurance and Analytics from the user interface. You must be logged in as an administrator to perform backup.

To create a new backup job:

**Procedure**

1. **Step 1** Choose *System Administration > Backup settings.*
2. **Step 2** On the Backup page, click *New.*
3. **Step 3** Enter a name for the backup job. If backup name is not specified, the *Backup Title* field is defaulted with date stamp.
Perform Backup and Restore

**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** While backing up using SFTP, ensure that you provide relative path. The relative path must contain directory details (for example DIRNAME or DIRNAME 1 / DIRNAME 2), to avoid backup in root directory.

- 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.

**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 location is relative to the specified SSH user home directory. The relative path must contain directory details (for example DIRNAME or DIRNAME 1 / DIRNAME 2), to avoid backup in root directory.

- 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 (**Assurance 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.
**Backup Cisco Prime Collaboration Assurance Data using CLI**

Only Assurance data is backed up in this method. You cannot backup Analytics data using CLI.

CLI is supported only through SSH; telnet is not supported. The port used for Cisco Prime Collaboration Assurance server is 26. After creating the repository, log in to the Cisco Prime Collaboration Assurance 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 as `admin` and run the following command:

```
admin# show backup history
```

**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 Assurance 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 Assurance 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
```

If you want to restore both Cisco Prime Collaboration Assurance and Analytics data, you are prompted with the following:
Perform Backup and Restore

1. Restore may require a restart of application services. Continue? (yes/no)
   Enter yes.

2. Do you want to restore Analytics [y/n]?
   Enter y.

3. Enter the following details for the Cisco Prime Collaboration Analytics data:
   • Remote server IP address, where the analytics backup data is stored.
   • Remote server SSH port
   • SSH username
   • SSH password
   • Backup file path

---

**Note**

While restoring the data, ensure that you provide relative path. The relative path must contain directory details (for example DIRNAME or DIRNAME 1 / DIRNAME 2), to avoid backup in root directory.

After checking the remote server connection, the Cisco Prime Collaboration Assurance and Analytics data restore starts. This may take a few minutes to complete based on the data.

---

**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 on the Same System. See also, Create a Repository on FTP, Disk, SFTP, or TFTP Server.

---

**Note**

As a post requirement, you must rediscover all the devices after restoring the data.
Set Log Levels

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 Settings 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 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.
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 83: Number of Phones Required for Synthetic Tests**

<table>
<thead>
<tr>
<th>Number of Tests</th>
<th>Type of Test</th>
<th>Phones Needed for Test</th>
<th>Total Phones Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Phone Registration</td>
<td>1 (synthetic phone)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dial-Tone</td>
<td>1 (synthetic phone)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>End-to-End Call with real phones</td>
<td>2 (1 synthetic phone and 1 real phone)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>End-to-End Call with synthetic phones</td>
<td>2 (synthetic phones)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TFTP Download</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency Call (without On Site Alert Number)</td>
<td>2 (synthetic phones)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency Call (with On Site Alert Number)</td>
<td>3 (synthetic phones)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Message-Waiting Indicator</td>
<td>2 (synthetic phones)</td>
<td></td>
</tr>
</tbody>
</table>
As you configure phones on each Unified CM, use the following worksheets to simplify data entry into Cisco Prime Collaboration.

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 84: Cisco Unified Communications Manager**

<table>
<thead>
<tr>
<th>Synthetic Test</th>
<th>MAC Address</th>
<th>Destination Phone Extension Number</th>
<th>Destination Phone Cisco Unified Communications Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Registration</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dial-Tone</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-source phone</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-destination phone (synthetic phone)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-destination phone (real phone)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Phone Registration</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dial-Tone</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-source phone</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-destination phone (synthetic phone)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-destination phone (real phone)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Phone Registration</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dial-Tone</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-source phone</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-destination phone (synthetic phone)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>End-to-End Call-destination phone (real phone)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Table 85: Cisco Emergency Responder**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name or Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency number</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Public Safety Answering Point</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On Site Alert</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
</tr>
</tbody>
</table>

**Table 86: Cisco Unity**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name or Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller</td>
<td>Cisco Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>MAC address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Name or Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
</tr>
<tr>
<td>Phone extension number</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Voice mail</th>
<th>Name or Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>
Cisco 1040 Sensor Management

Cisco Prime Collaboration 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:

The Cisco 1040 Sensor management is not applicable if you have installed Cisco Prime Collaboration in MSP mode.

This section contains the following:

• Overview of Cisco Prime NAM/vNAM, page 453
• Perform Initial Configuration in Cisco Prime Collaboration, page 454
• Configure Cisco 1040 Sensors in Cisco Prime Collaboration, page 456
• Edit Configurations for Multiple Cisco 1040s, page 459

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 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 307.
Perform Initial Configuration in Cisco Prime Collaboration

For initial configuration of Cisco 1040 Sensors, do the following:

Procedure

Step 1  Add one or more TFTP servers for Cisco Prime Collaboration 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.

Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files

Cisco Prime Collaboration 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 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 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 to each TFTP server that is configured for Cisco Prime Collaboration.

Add and Delete a TFTP Server

To enable Cisco 1040s to register with Cisco Prime Collaboration, you must define at least one TFTP server where Cisco Prime Collaboration can provide Cisco 1040 configuration files (and the binary image file).

Note

- Using Cisco Prime Collaboration as a TFTP server is not supported. Additionally, we recommend disabling the CWCS TFTP service on the Cisco Prime Collaboration 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 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.

Procedure

Step 1  Choose Assurance 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 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 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 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:

### Procedure

#### Step 1
Select **Assurance 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 stores the configuration file locally and copies it to the TFTP servers that are added to Cisco Prime Collaboration.
### Cisco 1040 Sensor/NAM Setup Page—Graphical User Interface Elements

**Table 87: Cisco 1040 Sensor/NAM Setup Page—Graphical User Interface Elements**

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Call Metrics Archiving          | Select one of the following:  
  - Enable—After analysis, Cisco Prime Collaboration saves data from sensors to disk files.  
  - Disable—After analysis, Cisco Prime Collaboration discards data.  
  Default: Disable. |
| 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 every 60 seconds. Cisco Prime Collaboration 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 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. |

### Configure Cisco 1040 Sensors in Cisco Prime Collaboration


This section contains the following:
Cisco 1040 Sensor Details

To see Cisco 1040 Sensor details, choose Assurance Administration > 1040 Sensor Setup > Management. The Cisco 1040 Sensor Details page displays information listed in the following table:

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exports data from the Cisco 1040 Sensor/NAM Details page to a CSV or PDF file.</td>
</tr>
<tr>
<td></td>
<td>Opens a printer-friendly version of the data in another window; for printing from a browser window.</td>
</tr>
<tr>
<td>Check box column</td>
<td>Select Cisco 1040s that you want to edit, reset, or delete.</td>
</tr>
<tr>
<td>Name column</td>
<td>Click the name link to view details of the Cisco 1040 configuration.</td>
</tr>
<tr>
<td>Cisco 1040 Address columns</td>
<td>Displays MAC and IP addresses for Cisco 1040. Click the MAC address link to launch an HTML page on the Cisco 1040.</td>
</tr>
<tr>
<td>Prime Collaboration columns</td>
<td>Displays the following:</td>
</tr>
<tr>
<td></td>
<td>• Primary—IP address or hostname of the primary Cisco Prime Collaboration defined for the Cisco 1040.</td>
</tr>
<tr>
<td></td>
<td>• Registered with—Displays one of the following:</td>
</tr>
<tr>
<td></td>
<td>◦ IP address or hostname of the Cisco Prime Collaboration to which the Cisco 1040 is currently sending data.</td>
</tr>
<tr>
<td></td>
<td>◦ Waiting—The Cisco 1040 is not yet registered.</td>
</tr>
<tr>
<td></td>
<td>◦ Older Image—The binary image on the Cisco 1040 is not supported.</td>
</tr>
<tr>
<td>Reset Time column</td>
<td>The last date and time that Cisco Prime Collaboration sent a reset command to the Cisco 1040.</td>
</tr>
<tr>
<td>Buttons</td>
<td>See Add a Cisco 1040 Sensor.</td>
</tr>
<tr>
<td>Add</td>
<td>See Edit Configurations for Multiple Cisco 1040s.</td>
</tr>
<tr>
<td>Delete</td>
<td>See Delete a Cisco 1040 Sensor.</td>
</tr>
<tr>
<td>Reset</td>
<td>See Reset Cisco 1040s.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refresh the Cisco 1040 Sensor Details page.</td>
</tr>
</tbody>
</table>
Restart Processes to Update Cisco 1040 Registration Information in Cisco Prime Collaboration

Cisco Prime Collaboration 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 `pdeexec` 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:

  ```
pdeexec QOVR
  ```

- Changes the time on the system where Cisco Prime Collaboration 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, perform the following procedure.

**Procedure**

**Step 1** Select **Assurance 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 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

<table>
<thead>
<tr>
<th>Graphical User Interface Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Sensor Name                      | Enter up to 20 characters. This name is used to identify the sensor on Cisco Prime Collaboration windows, such as reports. **Note**: Cisco 1040 names must be unique. Cisco 1040s that register to Cisco Prime Collaboration using the default configuration file use the name Cisco 1040 + `<last 6 digits from MAC address>`.
| Image File Name                  | Enter the binary image file name. The filename format is SvcMonAB2 nnn.img where nnn is a revision number. |
| 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 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 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 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:

**Procedure**

1. **Step 1** Select **Assurance Administration > 1040 Sensor Setup > Management**.
2. **Step 2** Select check boxes for more than one Cisco 1040 and click **Edit**.
3. **Step 3** Update any of the fields.
4. **Step 4** Click **OK**.

Cisco Prime Collaboration saves the configuration files on the local server copies it to all TFTP servers. Then Cisco Prime Collaboration resets the Cisco 1040s, so that they load the updated configuration.
Cisco 1040 Management - Field Descriptions

Table 88: Cisco 1040 Management - Field Descriptions

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image File Name</td>
<td>Enter the binary image filename. The filename format is SvcMonAB2_nnn.img where nnn 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.</td>
</tr>
<tr>
<td>Primary Prime Collaboration</td>
<td>Enter an IP address or DNS name of a host where Cisco Prime Collaboration is installed. The Cisco 1040 sends data to this Cisco Prime Collaboration unless it becomes unreachable.</td>
</tr>
<tr>
<td>Secondary Prime Collaboration</td>
<td>(Optional) Enter an IP address or DNS name of a host where Cisco Prime Collaboration is installed. The Cisco 1040 sends data to this Cisco Prime Collaboration only if the primary Cisco Prime Collaboration becomes unreachable.</td>
</tr>
</tbody>
</table>

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.

Procedure

**Step 1** Select Assurance 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.

**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 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, you must shut the switch port that physically connects to the 10/100-1 Fast Ethernet port on the Cisco 1040:

**Procedure**

| 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 until you shut the switch port.


After you delete a Cisco 1040, it cannot automatically register again to the Cisco Prime Collaboration from which it has been deleted. To enable such a Cisco 1040 to register with this Cisco Prime Collaboration again, you must add the Cisco 1040 Sensor manually. See **Add a Cisco 1040 Sensor**.

To delete, select **Assurance 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 sends a time synchronization message to each Cisco 1040 Sensor hourly. Cisco Prime Collaboration 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 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](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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Time</td>
<td>Current time and date (HH:MM:SS MM/DD/YYYY).</td>
</tr>
<tr>
<td>Clock Drift</td>
<td>Seconds of drift and the last time and date that the clock was reset; for example, &quot;1 second(s) updated at 9:23:37 03/16/2009&quot;.</td>
</tr>
<tr>
<td>Last Analysis Time</td>
<td>Time and date when the Cisco 1040 last ran an analysis.</td>
</tr>
<tr>
<td>Streams Analyzed</td>
<td>Number of RTP streams that were analyzed during the last interval.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Communication</td>
<td>Time and date when the sensor last received an ACK or timeSet message, or any supported message from the Cisco Prime Collaboration.</td>
</tr>
<tr>
<td>Last Successful Report Time</td>
<td>Time and date that the Cisco 1040 last sent data to Cisco Prime Collaboration.</td>
</tr>
<tr>
<td>Report Destination</td>
<td>Destination hostname or IP address and port number to which the report was sent.</td>
</tr>
<tr>
<td>Report Length (bytes)</td>
<td>Number of bytes in the last report record.</td>
</tr>
<tr>
<td>Received Packets</td>
<td>Number of packets that the Cisco 1040 received during the last interval.</td>
</tr>
<tr>
<td>Receive Errors</td>
<td>Number of errors received on the monitoring interface as reported by pcap.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>Number of packets dropped on the monitoring interface as reported by pcap.</td>
</tr>
<tr>
<td>Buffer overruns</td>
<td>Number of buffer overruns on the monitoring interface as reported by pcap.</td>
</tr>
<tr>
<td>Framing Errors</td>
<td>Number of framing errors on the monitoring interface as reported by pcap.</td>
</tr>
<tr>
<td>Interface Promiscuous</td>
<td>Monitoring interface is in promiscuous mode (yes) or not (no).</td>
</tr>
</tbody>
</table>
User Interface

- Overview, page 463
- Filters, page 464
- Launch the Advanced Filter and Save Filter Criteria, page 465
- Quick View, page 465
- View About Details, page 465

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 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 11.0 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.
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

Filters

You can use the Filter feature to display specific information on the Cisco Prime Collaboration 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 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 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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the <strong>Filter</strong> drop-down menu, choose <strong>Advanced Filter</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter advanced filter criteria.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Go</strong> and then click the <strong>Save</strong> icon.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Save Preset Filter</strong> page, enter a name for the <strong>Preset Filter</strong> and click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

To clear the Advanced Filter, click the **Filter** button.

Cisco Prime Collaboration 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 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 **MSP** mode, click **globaladmin - All Customers > About** at the top right corner of the User Interface.

To launch this page in **Enterprise** mode, click **globaladmin - Enterprise > About** at the top right corner of the User Interface.

- Click Assurance Information link to view the following system information details in a quick view.
• Build Version
• License Type
• Assurance Expiration Date (displayed in red for the last 15 days before expiry)
  Analytics Expiration Date (displayed in red for the last 15 days before expiry)
• IP Address
• DB server MAC Address

Note

• DB server IP Address and DB server MAC Address fields are 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.

• Click Licensing link to open the License Management page.