Overview of Cisco Prime Collaboration Assurance and Analytics

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

Overview of Cisco Prime Collaboration Assurance

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

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

Document Conventions

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

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

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

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

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

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

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

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

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

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

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

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

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

- “Smart Licensing” feature is not supported in the Cisco Prime Collaboration Assurance Release 12.1.
- The “Video Test Call” feature is not supported for Endpoints registration through the Mobile and Remote Access (MRA) solution.
- LDAP configuration with SSL enabled is not supported in the Cisco Prime Collaboration Assurance Release 12.1.

Cisco Prime Collaboration Assurance - Advanced

Cisco Prime Collaboration Assurance is available in the following modes:

- Cisco Prime Collaboration Assurance Advanced—Enterprise and MSP mode

For installing Advanced Assurance, see the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide.

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

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

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

Feature	**Advanced**	**See** Cisco Prime Collaboration Assurance Guide - Advanced
Supported Modes	It supports both the Enterprise and MSP modes.	For more information on Advanced features, see the sections *Overview of Cisco Prime Collaboration Assurance—MSP Mode* and *Differences Between the Enterprise Mode and the MSP Mode*.
License Requirement	Requires license after evaluation expiry.	For more information on Advanced features, see the section *Manage Licenses*.
Role Based Access Control	Supports five roles to provide multiple levels of authorization: • Super Administrator • System Administrator • Network Administrator • Operator • Helpdesk **For Cisco Prime Collaboration Release 11.5 and later** Supports six roles to provide multiple levels of authorization: • Super Administrator • System Administrator • Network Administrator • Operator • Helpdesk • Report Viewer	For more information on Advanced features, see the section *Manage Users*.
Single Sign-On Support	Yes	For more information on Advanced features, see the section *Manage Users*.

Cluster Management	Manages multiple clusters with mixes of cluster revisions and cluster associations.	For more information on Advanced features, see the section *Set Up Clusters*.
Discovery	• You can discover and manage all endpoints that are registered to Cisco Unified CM (phones and TelePresence), Cisco VCS (TelePresence), and Cisco TMS (TelePresence). In addition to managing the endpoints, you can also manage multipoint switches, application managers, call processors, routers, and switches that are part of your voice and video collaboration network. • Provides multiple discovery modes such as Auto Discovery, Import, and Add Device features. • Supports Logical Discovery, Ping Sweep, CDP-based discovery for discovering devices. • Provides the option to perform rediscovery. **For Cisco Prime Collaboration Release 11.5 and later** **Note** CTS-Manager (TelePresence) device is not supported.	For more information on Advanced features, see the section *Discover Devices*.
Inventory Management	• Provides a concise summary information for a device through the Device 360 view. • Provides exhaustive Inventory details.	For more information on Advanced features, see the section *Manage Inventory*.

Fault Management	• **For Cisco Prime Collaboration Release 11.1 and earlier**
	Support for initiating troubleshooting by using quick views.
	• Supports Alarm Correlation rules.
	• Supports customization of events at the device, and global level.
	• Provides configuration of thresholds for:
	  • TelePresence Endpoints
	  • Infrastructure Device
	  • Call Quality
	  • Device Pool
		For more information on Advanced features, see the section *Monitor Alarms and Events*.

Voice and video Reports	Provides the following predefined reports and customizable reports: • Administrative Reports • Communications Manager Reporting • Interactive Reports • Scheduled Reports	For more information on Advanced features, see the section *Dashboards and Reports*.
Dashboard	Provides the following dashboards: • Ops View - Provides high-level information about the Cisco Unified CM and VCS Clusters. • Service Experience - Provides information about quality of service. • Alarm - Provides information about alarm summaries. • Performance - Provides details on critical performance metrics of each managed element. • Contact Center Topology - Provides information about the Contact Center components such as CUIC, Finesse, MediaSense, CVP, and Unified CCE. You can add customized dashboards in the Home page.	For more information on Advanced features, see the section *Dashboards and Reports*.

Dashboards	**For Cisco Prime Collaboration Release 11.5 and later** Provides the following dashboards: • • Ops View - Provides high-level information about the Cisco Unified CM and VCS Clusters. • Call Quality - Provides information about quality of service. • Alarm - Provides information about alarm summaries. • Performance - Provides details on critical performance metrics of each managed element. • Contact Center Topology - Provides information about the Contact Center components such as CUIC, Finesse, MediaSense, CVP, and Unified CCE. 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*.

Voice and Video Endpoint Diagnostics	**For Cisco Prime Collaboration Release 11.1 and earlier** • Provides a detailed analysis of the end-to-end mediapath, including specifics about endpoints, service infrastructure, and network-related issues. • Uses Cisco Medianet technology to identify and isolate video issues. • Provides mediapath computation, statistics collection, and synthetic traffic generation • Uses the IP SLA to monitor the availability of key IP phones in the network. • Predicts service outage using scheduled synthetic and IP SLA tests. **For Cisco Prime Collaboration Release 11.5 and later** • Uses the IP SLA to monitor the availability of key IP phones in the network. • Predicts service outage using scheduled synthetic and IP SLA tests.	For more information on Advanced features, see the section *Perform Diagnostics*.
Job Management	Enables you to view, schedule, and delete jobs.	For more information on Advanced features, see the section *Manage Jobs*.
Cross Launch to UC Application	Yes	-
Cross Launch to Cisco Prime Collaboration Assurance Serviceability	Yes	-
Device Search	Global Search - Provides filtered search for TelePresence, endpoints, phones, other devices, locations, and users.	For more information on Advanced features, see the section *Global Search Options for Cisco Prime Collaboration Assurance*.

Cisco Prime Collaboration Analytics	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 • Call Quality • UC System Performance • Scheduled Reports • Video Conferences • Custom Report Generator **Note** **For Cisco Prime Collaboration Release 11.1 and earlier** Cisco Prime Collaboration Analytics is not supported in MSP mode deployment. Cisco Prime Collaboration Analytics is a licensed software, which has to be purchased separately with Cisco Prime Collaboration Assurance.	See Cisco Prime Collaboration Analytics Guide.
NB API	NB API is supported for the following: • Managing devices • Viewing and deleting device credentials • Listing all video conferences • **For Cisco Prime Collaboration Release 11.1 and earlier** Troubleshooting video conferences	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; where, pc-server-ip is the Cisco Prime Collaboration Assurance server IP address. **For Cisco Prime Collaboration Release 11.6 and later** To access the NB API documentation, log in to the Cisco Prime Collaboration Assurance server and select **Assurance NB API documentation** from Settings drop-down menu at the top right corner of the user interface.

Cisco Prime Collaboration Assurance - Advanced Features

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

Voice and Video Unified Dashboard

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

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

Device Inventory/Inventory Management

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

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

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

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

See Manage Inventory to learn how to collect the endpoints inventory data and how to manage them.

Voice and Video Endpoint Monitoring

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

For Cisco Prime Collaboration Release 11.1 and earlier

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

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

- In-progress
- Scheduled
- Completed
- No Show

Cisco Prime Collaboration Assurance periodically imports information from:

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

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

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

Diagnostics

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

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

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

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

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

For Cisco Prime Collaboration Release 11.5 and later

Cisco Medianet technology is not supported.

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

Fault Management

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

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

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

See Monitor Alarms and Events to learn how Cisco Prime Collaboration Assurance monitors faults.

Reports

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

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

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

See 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

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

Features	Supported	Notes or Limitations
Device Inventory/Inventory - Inventory Management	Inventory Summary shows IPv6 addresses.	—
Conference Diagnostics	Endpoint Statistics (System and Conference 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 Cisco Prime Collaboration Release 11.5 and later		
Technology Adoption Dashboard	IP address filters supports endpoints with IPv6 addresses.	—
Asset Usage Dashboard	IP address filters supports endpoints with IPv6 addresses.	—
Traffic Analysis Dashboard	IP address filters supports endpoints with IPv6 addresses.	—
Service Experience Dashboard	IP address filters supports endpoints with IPv6 addresses.	—

Note

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

Overview of Cisco Prime Collaboration Assurance—MSP Mode

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

Note You can select the MSP mode deployment only during installation.

NAT Environment - Deployment Scenarios

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

- Scenario - Voice endpoints

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

- Scenario - Voice and Video endpoints

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

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

  Scenario - TelePresence provisioned to Cisco TelePresence Exchange (CTX)

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

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

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

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

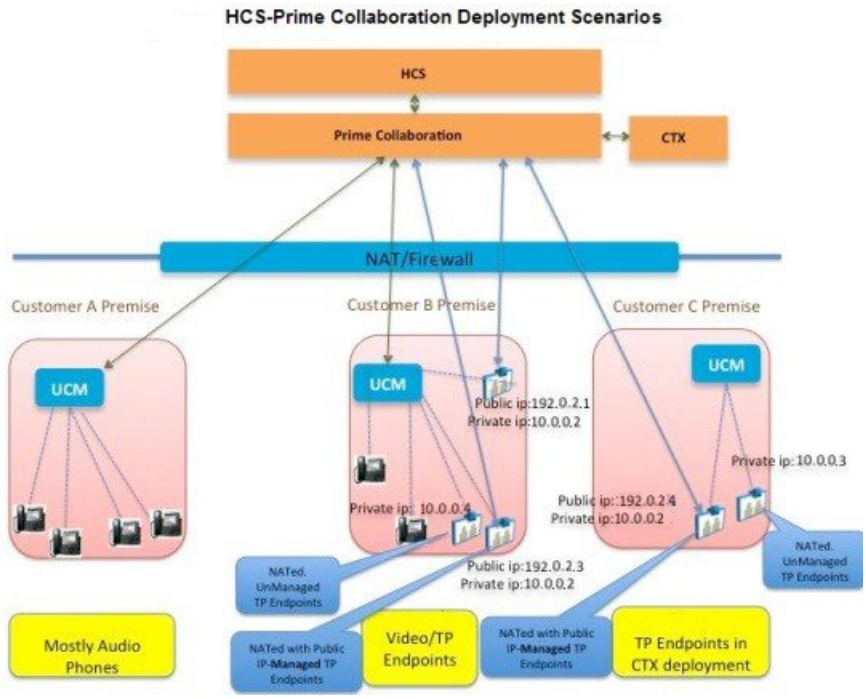
The Private IP address of a device for one customer may overlap with the Public IP address of a device for another customer. However, the Public IP address is unique across different customers that are managed in Cisco Prime Collaboration Assurance.

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

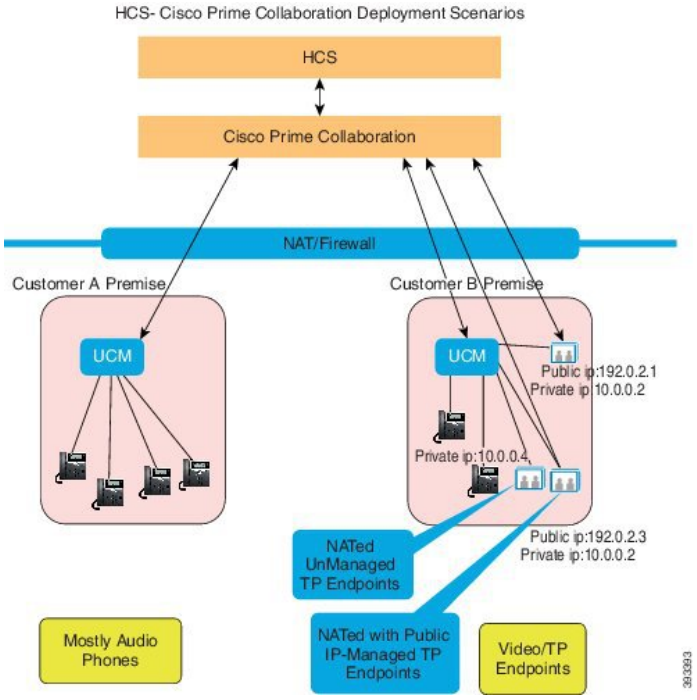
The following diagram displays the HCS-Cisco Prime Collaboration Assurance deployment scenarios in a NAT environment.

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

Figure 1: Cisco Prime Collaboration Deployment Scenarios



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



Voice and Video Unified Dashboard

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

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

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

Device Inventory/Inventory Management

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

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

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

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

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

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

Voice and Video Endpoint Monitoring

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

- In-Progress
- Scheduled
- Completed
- No Show

Diagnostics

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

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

For Cisco Prime Collaboration Release 11.5 and later

Cisco Medianet Technology is not supported.

Fault Management

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

You can also create customer-specific device notification groups.

Reports

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

See Differences Between the Enterprise Mode and the MSP Mode, on page 18 for more information on the Enterprise and the MSP modes.

Cisco Prime Collaboration Analytics

For Cisco Prime Collaboration Release 11.5 and later

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

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

Differences Between the Enterprise Mode and the MSP Mode

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

Managed Service Provider (MSP) Mode	Enterprise Mode
Comes with Advanced mode only.	Comes with both Advanced mode .
Enables you to create customers and add specific devices to them.	Enables you to create logical units in your enterprise called domains. This is an optional feature in the Advanced mode.
Filters information, by customer, Inventory Management, phone inventory reports, conference diagnostics, and endpoint diagnostics.	Filters information, by domains, in the inventory table, Inventory Management, conference diagnostics, and endpoint diagnostics.
Provides dashboards and dashlets on Customer Summary. **For Cisco Prime Collaboration Release 11.5 and later** Cisco TelePresence Exchange (CTX) is no longer available.	Does not provide dashboards and dashlets on Customer Summary.
IP SLA testing can be performed for a specific customer's routers and switches also.	IPSLA testing is available all for IP SLA-enabled routers and switches.

Managed Service Provider (MSP) Mode	Enterprise Mode
Provides support for CTX clusters and meeting types supported by CTX. **For Cisco Prime Collaboration Release 11.5 and later** Cisco TelePresence Exchange (CTX) is no longer available.	Does not support CTX.
Provides Role Based Access Control (RBAC) for customer groups.	Provides Role Based Access Control (RBAC) for assurance device pools and endpoints.
Supports Static NAT.	Does not support NAT.
Supports CTX manageability for both hosted and non-hosted deployment models. **For Cisco Prime Collaboration Release 11.5 and later** Cisco TelePresence Exchange (CTX) is no longer available.	Does not support CTX.
RTP-based diagnostics tests (for example, Synthetic tests) are only supported in a non-NAT environment.	All functionalities are supported.
In a NAT environment, for phones, the data from Phone XML discovery is not available. Video conference stats and conference information will not be available for phones even if they are set to full visibility.	All functionalities are supported.
Sensor-based call quality reports are not available.	All reports are available.
In a NAT environment, the Cisco TelePresence endpoint health monitoring is only supported for Cisco TelePresence endpoints with Public IP addresses.	All functionalities are supported.
In a NAT environment, video conference diagnostics is only supported for endpoints with Public IP addresses.	All features of video conference diagnostics are supported.
Auto Discovery is not supported.	Auto Discovery is supported.
For Cisco Prime Collaboration Release 11.5 and later FIPS Compliance is not supported. **For Cisco Prime Collaboration Release 12.1 and later** FIPS Compliance is not supported.	**For Cisco Prime Collaboration Release 11.5 and later** FIPS Compliance is supported. **For Cisco Prime Collaboration Release 12.1 and later** FIPS Compliance is not supported.

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

Cisco Prime Collaboration Assurance NBI

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

- Managing devices
- Viewing and deleting device credentials.
- Listing all video sessions based on the filtering criteria.
- Troubleshooting video sessions.
- Get the endpoint count from the Unified CM cluster

  .
- Lists the alarms based on the filtering criteria.

For Cisco Prime Collaboration Release 11.5 and later

Troubleshooting is not supported.

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

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

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

For Cisco Prime Collaboration Release 11.6 and later

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

For Cisco Prime Collaboration Release 12.1 and later

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

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

For example:

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

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

Cisco Prime Collaboration Assurance and Analytics Geo-Redundancy

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

New and Changed Information

The following table describes the information that has been added or changed in this guide for 12.1 SP1 release.

Table 2: New and Changed Information

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

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

Table 3: New and Changed Information

Date	Updates
July 21, 2017	Added What's New in Cisco Prime Collaboration Assurance section.
March 13, 2017	Updated information on Device Status Summary.
March 14, 2017	Made changes to the existing content on TMS Cluster in the chapter "Set Up Cluster".

Date	Updates
March 27, 2017	Audio Phone and Video Phone Audit Reports are merged to a single report "Endpoint Audit Report".
March 31, 2017	Audio Phone and Video Phone Move Reports are merged to a single report "Endpoint Move Report".
April 24, 2017	Removed IP Phone and Removed Video Phone Reports are merged to a single report "Endpoint Remove Report".
May 30, 2017	Audio Extension and Video Extension Reports are merged to a single report "Endpoint Extension Report".
April 05, 2017 April 17, 2017	There are a few changes with respect to user interface. **1.** Handling dependencies for removal of device **2.** CUBE SIP Trunk - changes for session server group configuration
March 23, 2017	Updated information in the section "Rediscover Devices" with respect to removal of devices from Cisco Prime Collaboration Assurance on deletion.
June 06, 2017	As part of PIFServer process removal, the following are removed "IP Phone Inventory Collection and IP Phone XML Collection" from Inventory Schedule Page. This change addresses the following aspects: **1.** Updated information in the following sections "Configure System Parameters", "Schedule Cluster Data Discovery", "Update and Collect Inventory Details", "Inventory Details Collection", and table "Global System Parameters". **2.** Removed sections on "IP Phone Discovery Schedule" and "Schedule IP Phone XML Discovery Schedule".
July 06, 2017	A new section "Monitoring IP Phones Using Cisco Unified CME Syslog Messages" is added that explains the configuration of the syslogs in CME.
July 06, 2017	Updated the section on "License Count" to address the changes made in "Licensing of Registered Endpoints in Inventory".
June 18, 2017	Revamped the section on "Schedule a Job" and added a new section "Defining a Timetable" to address the issue on "Fixing Settings button on Job Management page".
June 18, 2017	The changes related to all audit reports should be purged for data older than 30 days on daily basis are addressed in the section on "Perform Backup and Restore" and to the table on "Purge Policies".
June 18, 2017	Added information to the section on "Manage Licenses > View License Details" to address the change related to "Cisco Prime Collaboration Assurance Licensing User Interface should restrict the maximum license you can import based on each profile(Small/Large/BE6k)".

Date	Updates
June 01, 2017	Added a note in the section on "Upgrade Cisco Prime Collaboration Assurance" to address the issue on handling schema changes through Data Migration Assistant Tool.
June 01, 2017	All the occurrences of FIPS Compliance is hidden. As part of Cisco Prime Collaboration Assurance 12.1 Enterprise mode, FIPS compliance is not certified. The entire section on "Enable FIPS Compliance" is hidden.
May 21, 2017	There is a change in the navigation with respect to sFTP Credentials User Interface. Changes are made in the section on "Configure System Parameters" > in the "Table: on System Parameters" and corresponding section on "Configure sFTP Settings".

What's New in Cisco Prime Collaboration Assurance

You can access the Cisco Prime Collaboration Assurance 12.1 Service Pack 1 features from Cisco.com.

Table 4: Cisco Prime Collaboration Assurance 12.1 Service Pack 1 Features

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

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

You can access the Cisco Prime Collaboration Assurance 12.1 features from Cisco.com.

Table 5: Cisco Prime Collaboration Assurance 12.1 Features

Feature Name	Feature Description
Inventory - Device Status Summary	Fixing Unmanaged count: The unmanaged count in header must match the count in the Device Status Summary page. Count for both categories must meet this criteria.
Inventory - TMS Cluster	TMS discovery discovers all TMS provisioned devices (CUCM/VCS/endpoint/MCU/TPS/TP_Conductor) even though Cisco Prime Collaboration Assurance does not manage the CUCM/VCS devices. However, TMS discovery does not logically discover CUCM/VCS/endpoints.
Reports	Following reports are merged into a single report: **1.** The Endpoint Audit Report is a single report that merges Audio Phone and Video Phone Audit Reports. **Navigation** - Reports -> Miscellaneous Reports -> Endpoint Audit Report **2.** The Endpoint Move Report is a single report that merges Audio Phone and Video Phone Move Reports. **Navigation** - Reports -> Miscellaneous Reports -> Endpoint Move Report **3.** The Endpoint Remove Report is a single report that merges Removed IP Phone and Removed Video Phone Reports. **Navigation** - Reports -> Miscellaneous Reports -> Endpoint Remove Report **4.** The Endpoint Extension Report is a single report that merges Audio Extension and Video Extension Reports. **Navigation** - Reports > Miscellaneous Reports -> Endpoint Extension Report

Feature Name	Feature Description
User Interface Changes	Following are the changes with respect to user interface: **1.** Handling dependencies for removal of device - Devices like CUCM that includes Publisher and Subscriber, VCS, TMS, ESX, VCENTER, TPS, UNITY CONNECTION, MULTIPOINT Controller, IM&P and other infrastructure devices and their associated endpoints are removed from the database when the State is Deleted. **2.** CUBE SIP Trunk - changes for session server group configuration A Collaboration Network Administrator access the Utilization Monitor -> CUBE SIP Trunk tab to view the CUBE SIP Trunk with "session server group configuration". In case of server group, this screen provides information about its limitation in supporting many-to-one configuration of Dialpeer to SIP Trunk. There is also an option to raise/suppress events for the server group configuration.
	Removal of devices from Cisco Prime Collaboration Assurance on deletion The update explains that the Administrator must add a device first before rediscovering it. Remove the devices from Cisco Prime Collaboration Assurance when you delete them.
	Remove IP Phone Inventory Schedule and IP Phone XML Inventory Schedule from Inventory Schedule Page. PIFServer removal from the Cisco Prime Collaboration Assurance Enterprise/MSP mode also removes the IP Phone Inventory Collection and IP Phone XML Collection discoveries. This change addresses the following aspects: **1.** Removed Inventory Schedule -> IP Phone Inventory Schedule and Inventory Schedule -> IP Phone XML Discovery pages. **2.** Renamed Inventory Schedule to Cluster Data Discovery Schedule under Inventory tab.
CME Syslog	The steps explain configuration of the syslogs in CME. This syslogs help monitor IP Phones using Cisco Unified CME Syslog messages.

Feature Name	Feature Description
Licensing of Registered Endpoints in Inventory	First, purge the latest registered endpoints within a particular cluster. Sort the registered endpoints by clustername, identify their clusters and purge them to meet licensing requirements. Port the phone licenses to the inventory module while removing the PIFServer from Cisco Prime Collaboration Assurance.
Fixing Settings button issue on Job Management page	Use the Schedule and Settings tab under the Job Details pane to schedule a job and set options.
30 day purge for Audit reports	Call quality event history and endpoint related (audio/video phone is now replaced with endpoint related) Audit report data older than 30 days are purged.
Cisco Prime Collaboration Assurance Licensing User Interface should restrict the maximum licenses one can import based on each profile like Small, Large, and BE6k	Cisco Prime Collaboration Assurance licensing allows uploading of a license file with a count more than it supports. For instance, Small - 3K endpoints. An error message must notify the user when a Cisco Prime Collaboration Assurance accepts a license file with an endpoint count lesser than the maximum count supported per profile. This is applicable for Assurance Mass, Contact Center Assurance and Analytics Licensing and supports all the profiles such as Small/Medium/Large/Very Large/BE6k/BE7K.
Handling Schema changes through DMA	There will be schema changes around Inventory while upgrading from 11.x (11.0, 11.1, 11.5 and 11.6) to 12.1. During the upgrade, a few Database related table columns available in 11.x will be removed. There will be no impact on the overall Cisco Prime Collaboration Assurance functionality. The Deleted state devices/endpoints will be purged and after the upgrade these (the devices/endpoints) will not be available.
FIPS User Interface has to be hidden	As part of Cisco Prime Collaboration Assurance 12.1 Enterprise mode, FIPS compliance is not certified. Hence, in the System Administration page, the FIPS enable/disable setup menu is hidden.
sFTP Credentials User Interface Implementation	Additional buttons like CUCM/sFTP Credentials and Save are introduced in the User Interface. A check box to change the smuser password and options to confirm password options are available. Change in Navigation from Alarm & Report Administration -> CDR Source Settings -> CUCM SFTP Credentials to Inventory -> Inventory Management -> CUCM/sFTP Credentials

Feature Name	Feature Description
Implementation of RTMT Polling Inconsistency - Notes for Alarms and Events	In a multi-node call manager cluster, if the same alert exists on more than one node at the same time, Cisco Prime Collaboration Assurance displays one latest alert.
Phone to Endpoint unregistered threshold	"Phone unregistered" is changed to "Endpoint unregistered".
Process Description Column - Serviceability	The process description column is added that describes each process to know the status of the processes in the output.
Prime License Manager does not show License Usage in Prime Collaboration Assurance	Provide both CLI and HTTP credentials in Monitor -> Utilization Monitor -> License Usage while managing co-resident PLM. Administrators can use CLI credentials to access the license information and HTTP credentials to manage Prime License Manager in Cisco Prime Collaboration Assurance.
Inaccessible status reason is shown as SNMP timeout	A note is added indicating that only HTTP credentials are required when a VMware VCenter Server or UCS Manager is added through Inventory -> Inventory Management -> Manage Credentials tab. The Inaccessible State column shows "SNMP timeout" where SNMP is not required for these devices.
Standalone PLM gets discovered as non-Cisco in PCA 11.6	A troubleshooting section is added to address this defect. This is likely to happen when PLM has a SNMP community string configured. If you want to discover PLM correctly, do not configure the community string. If configured t a community string, delete it and proceed to discover PLM in Cisco Prime Collaboration Assurance. Cisco Prime Collaboration Assurance does not support SNMP community string configuration for PLM discovery.
PCA BACKUP job status shows failure even after generating reports in SFTP	A troubleshooting section is added to address this defect. The troubleshooting section explains the method to generate the GPG key in the user folder.
The OpsView Dashlet page do not load due to corrupted globaladmin user	The troubleshooting section explains the Recommended Action and Path A new script (opsview_globaladmin.sh) and the recommended path (/opt/emms/emsam/bin) addresses this defect.

Feature Name	Feature Description
Ampersand is not allowed in LDAP parameter value	A Note is added to address this defect. A new LDAP parameter value (?CN=hq-prime,OU=Service Access Groups,DC=Megafon,DC=ru?) is defined to connect to LDAP.
CME Discovery & Phone XML Discovery job need to be restricted to be scheduled	A Note is added to address this defect. CMEPhoneDiscovery and PhoneXML Discovery Job is scheduled to execute at every regular four-hour intervals. These jobs can be modified to run once without re-occurrence. After the discovery, you cannot change it back to schedule.
Full Octets is not showing properly	During the deployment of Cisco Prime Collaboration Assurance 12.1 OVA, only three octets appear to IP address, IP Default Gateway, IP Default Netmask, and Backup Server IP. The fourth octet is invisible. Press the Tab button to display all octets.
Remove auto refresh of Device Status Summary from documentation	There is a change in the behavior of the Device Status Summary page. The page does not refresh automatically in every 30 seconds.
Execute this script on the server to generate and export CDR_CMR reports	Only an administrator can export CDR/CMR reports. Create a script to automate the task of exporting on the server.
NBI API Documentation	Reviewed and corrected Sample Input codes.
Performance data for Device 360	The performance data can no longer be viewed in Device 360 view. Instead, click the link 'Click here for performance data' to view the same data.
Performance data for Ops View Cluster Summary	A column is added to Call Health Summary tab.

Feature Name	Feature Description
Features or Devices Not Supported From This Release	**1.** Cisco TelePresence-Manager (CTS-Manager/CTS-MAN) device is not supported. Hence, removed all occurrences of the device from the document. **2.** FIPS Compliance is not supported. Hence, removed all occurrences from the document. **3.** Content specific to CTX is removed from the document. **4.** Enable Logical Discovery button - Content specific to enabling logical discovery button is removed from the document. **5.** CLI is not supported. Hence, removed content specific to CLI from the document.
General	**1.** Renamed "Cisco Prime Collaboration" to "Cisco Prime Collaboration Assurance". **2.** Renamed "PhoneUnregThresholdExceeded" to"EndpointUnregThresholdExceeded".
Support UCM in Mixed mode	Cisco Prime Collaboration Assurance supports Cisco Unified CM cluster in Mixed mode. However, the following features on Cisco Prime Collaboration Assurance will only support non-secure way of communication to CUCM: • Session Monitoring will continue to use non-secure JTAPI communication to monitor sessions. • Synthetic Test: Does not support secure signaling (TLS) and secure media (SRTP) connections to CUCM and endpoints registered to CUCM in secure mode.