Overview of Cisco Prime Collaboration Assurance

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

Cisco Prime Collaboration 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, page 1
- Standard and Advanced Cisco Prime Collaboration Assurance, page 2
- Cisco Prime Collaboration Assurance—Standard Features, page 12
- Cisco Prime Collaboration Assurance—Advanced Features, page 13
- Overview of Cisco Prime Collaboration Assurance—MSP Mode, page 19
- Differences Between the Enterprise Mode and the MSP Mode, page 24
- Cisco Prime Collaboration Assurance NBI , page 26
- Cisco Prime Collaboration Analytics NBI, page 27
- Cisco Prime Collaboration Geo-Redundancy, page 28
- New and Changed Information, page 28
- What's New in Cisco Prime Collaboration, page 36

Document Conventions

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

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

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

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

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

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

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

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

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, 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—Standard and Advanced.

Feature	Standard	Advanced	See Cisco Prime Collaboration Assurance Guide - Advanced
Supported Modes	It supports Enterprise mode only.	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	Does not require a license.	Requires license after evaluation expiry.	For more information on Advanced features, see the section *Manage Licenses*.
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 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	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, Cisco IM and Presence. **For Cisco Prime Collaboration Release 11.5 and later** Cisco Unity is not supported.	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 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.	• 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. **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 limited inventory information by using the Current Inventory Table.	• 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	• Provides an Alarms and Events browser. • Supports setting up email notifications for Alarm Sets. • Supports creation of custom events for Unified Communications Performance Counters. • 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.	• **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	NA	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*.

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

		• 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 . You can add customized dashboards in the home page. **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.	

Voice and Video Endpoint Diagnostics	NA	**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 job status.	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	Yes	-

Device Search	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.	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	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 • 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	NA	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—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
- Support for Cisco TelePresence components including Cisco TelePresence Management Suite (TMS), Cisco TelePresence Video Communication Server(Cisco VCS), Cisco TelePresence MCU, TelePresence Server, Cisco TelePresence System MXP Series, and Cisco TelePresence Conductor
- 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/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 conferences 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 SIP Call Flow 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:

Dashboard	Description	Cisco Prime Collaboration Options
Service Experience	Information about quality of service.	Cisco Prime Collaboration Assurance Advanced
Alarm	Information about Alarm summaries.	Cisco Prime Collaboration
Performance	Provides details on critical performance metrics of each managed element.	Cisco Prime Collaboration Assurance Advanced and Cisco Prime Collaboration Assurance Standard
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 Options
Call Quality	Information about quality of service.	Cisco Prime Collaboration Assurance Advanced
Alarm	Information about Alarm summaries.	Cisco Prime Collaboration
Performance	Provides details on critical performance metrics of each managed element.	Cisco Prime Collaboration Assurance Advanced and Cisco Prime Collaboration Assurance Standard
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 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), 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 conferences in an enterprise.

For Cisco Prime Collaboration Release 11.1 and earlier

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 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 periodically imports information from:

- The management applications (CTS-Manager and 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 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.

For Cisco Prime Collaboration Release 11.5 and later

Cisco Medianet technology is not supported.

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 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 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:

- 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
- NAM & Sensor Reports— Provides call details collected form Sensor or NAM such as MOS, jitter, time stamp, 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.	—

Features	Supported	Notes or Limitations
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.	—
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.	—

Features	Supported	Notes or Limitations
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 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.

- **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 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**

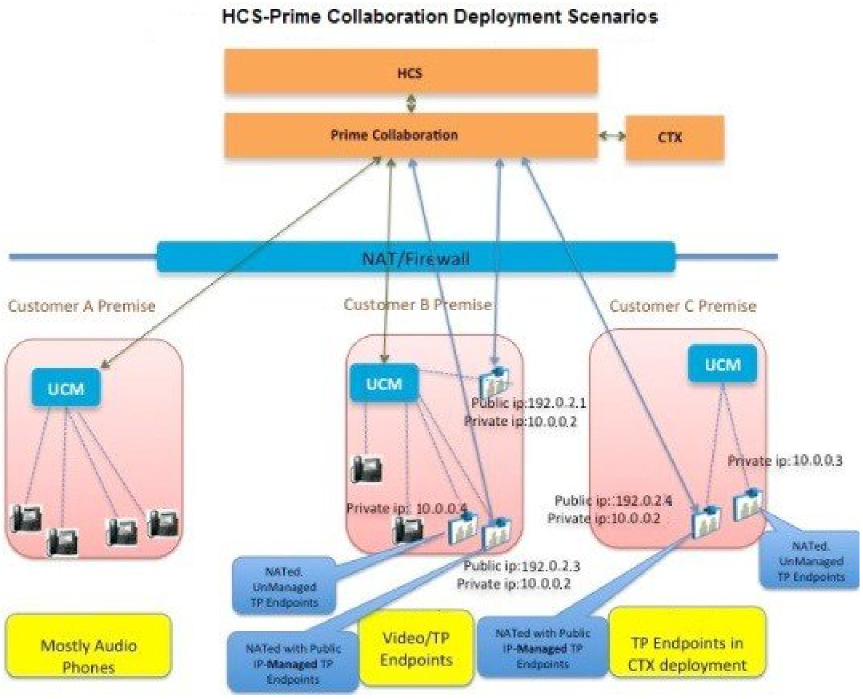
The Private IP address of a device for one customer may overlap with the Public IP address of a device for another customer. However, the Public IP address is unique across different customers that are managed in Cisco Prime Collaboration.

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.

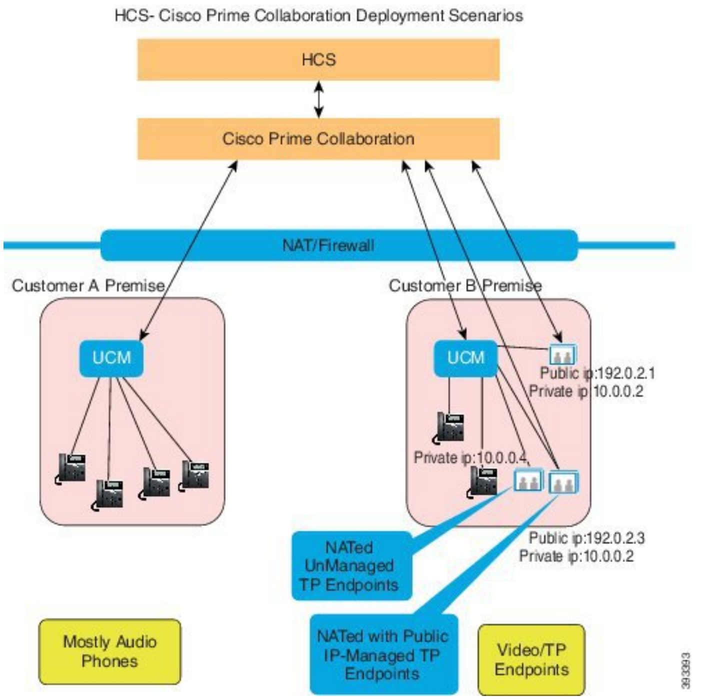
The following diagram displays the HCS-Cisco Prime Collaboration deployment scenarios in a NAT environment.

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

Figure 1: Cisco Prime Collaboration Deployment Scenarios



Note The following diagram is applicable to Cisco Prime Collaboration 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), CTS-Manager (TelePresence), Cisco TMS (Cisco TelePresence) and Cisco TelePresence Exchange. 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 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 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, 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 24 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 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 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 and Standard modes.
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. **Note** This feature is not available in the Standard 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 Cisco TelePresence Exchange (CTX) and 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 Cisco TelePresence Exchange (CTX) and 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.
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.

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

Managed Service Provider (MSP) Mode	Enterprise Mode
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 11.5 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 11.5 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.

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
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.

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 Analytics NBI

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

- NBI API support is available for the following dashboards:
  - Capacity Analysis
  - UC System Performance
  - Video Conference Analysis
  - License Usage

> **Note** As part of Cisco Prime Collaboration Release 11.5, NBI API is already supported for the following dashboards:
>
> - Technology Adoption
> - Asset Usage
> - Traffic Analysis
> - Service Experience

- Following are the supported naming conventions:
  - For Dashlet:

    ```
    https://<PC Server>/emsam/nbi/<dashboard>/<dashletname>/summary/parameters
    ```

  - For Details View:

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

- NBI API documentation includes parameter descriptions and sample NBI URLs. To access the NBI API documentation, log in to the Cisco Prime Collaboration Analytics server with the administrator privilege and enter one of the following URL in the browser:
  - `https://<pc-server-ip>/emsam/nbi/nbiAnalyticsDoc/`

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

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

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

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

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

- Case insensitive parameter values are supported in the NBI API. For example, parameter *timePeriod* accepts *last7days*, *Last14Days*, *last7DAYS*, and so on as values.

  This feature is supported in the following dashboards:

  - Capacity Analysis
  - Video Conference Analysis
  - UC System Performance
  - License Usage

Note This feature is not supported in the following dashboards for Cisco Prime Collaboration Analytics 11.5 SP1:

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

- As part of Cisco Prime collaboration Release 11.5, NBI API is supported to query Call Detail Records(CDR) for the CDR based dashlets. For more information, refer Call Detail Records (CDR) NBI Support.

For Cisco Prime Collaboration Release 11.6 and later

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

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.

New and Changed Information

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

Table 2: New and Changed Information

Version	Date	Updates	Location
Cisco Prime Collaboration Assurance Guide - Advanced, 11.0			
11.0	October 19, 2015	Added a table with name fields and descriptions to generate the CSR.	Install CA Signed Certificate for Secure Data Transmission
	October 23, 2015	Added a note related to collecting switch port details.	Schedule IP Phone XML Discovery Schedule
	October 26, 2015	Updated information related to dual stack.	Cisco Prime Collaboration Assurance Support for IPv6
	October 29, 2015	Added a note related to Endpoint Name field.	CME Diagnostics
Cisco Prime Collaboration Assurance Guide - Advanced, 11.1			

Version	Date	Updates	Location
11.1	March 1, 2016	Added What's New in Cisco Prime Collaboration section.	What's New in Cisco Prime Collaboration
		Updated the information related to **Notes for Email**.	System
		Updated the information related to **Notes for Email**.	Add Dynamic Syslogs
		Updated the information related to **Notes for Email**.	Threshold Rules
	March 1, 2016	Updated the information related to **Notes for Email**.	Correlation Rules
		Updated the information related to e-mail notification.	Set up Destinations Field Descriptions
		Updated the information related to search option in Cluster or Device drop-down list in **UC Device Search**, **Performance**, and **Event Customization**.	
	May 30, 2016	Updated a note related to adding more alarm to an existing alarm set.	Add an Alarm Set
Cisco Prime Collaboration Assurance Guide - Advanced, 11.5			
11.5		Added What's New in Cisco Prime Collaboration section.	What's New in Cisco Prime Collaboration
11.5		Updated information related to Getting Started page.	Getting Started with Cisco Prime Collaboration Assurance
11.5		Updated the information related to PKCS12 format certificates.	Install CA Signed Certificate
11.5		Update a note related to the polling interval.	Create Custom Performance Dashboards

Version	Date	Updates	Location
11.5		Updated the information related to **Report Viewer** role.	Cisco Prime Collaboration Assurance-Advanced User Roles
11.5		Updated the information related to monitoring the Cisco Prime Collaboration Assurance Server health by using the Cisco Prime Collaboration Assurance application.	Monitor the Cisco Prime Collaboration Assurance Server
11.5		Update information related to enabling FIPS compliance in Cisco Prime Collaboration Assurance.	FIPS Setup
11.5		Updated the FIPS related information.	Overview of Backup and Restore
			Overview of Cisco Prime NAM/vNAM
			Credential Profiles Field Descriptions
			Import Devices
			SNMP Query
			View User 360 Details
11.5		• Updated a note that Auto Discovery is not supported in MSP deployment. • Renamed "Assurance Domain" to "Associate to Domain".	Automatic Discovery of Devices

Version	Date	Updates	Location
11.5		• Updated the information about the unsupported devices in Credential Profiles page. • Updated information related to CLI and MSI credentials. • Updated the renamed devices in Credential Profiles page.	Credential Profiles Field Descriptions
11.5		• Updated information related to software version of managed devices. • Updated the Location search parameter section.	Manage Inventory

Version	Date	Updates	Location
11.5		• Renamed “Discovery Methods” drop-down list to “Discover” and re-organized the discovery methods in Discover drop-down list. • Added “Any Device” as a new option in the Auto discovery row. • Updated content related to automatic configuration of syslog receiver and CDR billing application server in Unified Communications Manager. • Added information on the following new devices: Virtualized Voice Browser (VVB), Perimeta Session Border Controller (SBC), and Cisco Unified Attendant Console	Discovery Methods
11.5		Assurance Inventory Summary is renamed as Device Status Summary.	Device Status Summary
11.5		• Added two new sections: CUBE SIP Trunk, and T1/E1 Trunks • Updated information on the Route Group Utilization dashlet.	Utilization Monitor

Version	Date	Updates	Location
11.5		• Renamed “Session” to “Conference” in all the relevant sections. • Renamed “Assurance Domain” to “Associate to Domain” in all the relevant sections. • Troubleshooting workflow is not supported, updated all the relevant sections. • Medianet technology is not supported, updated all the relevant sections. • Merged the Phone and TelePresence search fields and renamed them to “Endpoint” in the Global Search option.	
Cisco Prime Collaboration Assurance Guide - Advanced, 11.6			
11.6		Added What's New in Cisco Prime Collaboration section.	What's New in Cisco Prime Collaboration
11.6		Updated the information related to PKCS12 format certificates.	Install CA Signed Certificate
11.6		Updated the information related to accessing NB API document.	Cisco Prime Collaboration Assurance NBI , on page 26
11.6		Updated the information related to the MAC Address and DB Server IP Address.	View License Details

Version	Date	Updates	Location
11.6		Updated the information related to ciscoDX70 and ciscoDX80 devices with Collaboration Endpoint (CE) image.	Prerequisites and Recommendations Endpoint Diagnostics Dashboard
11.6		Updated the information related to HTTP Download Synthetic Test.	Create an HTTP Download Synthetic Test
11.6		Updated the information related to task on Export and Import synthetic tests.	Manage Synthetic Tests
11.6		Updated the information related to the method of viewing the SIP trunk utilization.	UCM SIP Trunks
11.6		Updated the information related to the display of Ops View and list view.	Ops View
11.6		Updated the information related to the color codes in the Treemap view.	Ops View
11.6		Updated the information related to viewing the UCM SIP Trunk tab from Utilization Monitor page.	NA
11.6		Updated the information related to leaf creation for Trunks.	NA
11.6		Updated the information related to the graphical view of channel usage.	Trunk Group Utilization
11.6		Updated the information related to LDAP Configuration Parameters.	LDAP Configuration Parameters

What's New in Cisco Prime Collaboration

You can access the Cisco Prime Collaboration Assurance 11.0 features from Cisco Prime Collaboration Assurance Guide - Advanced, 11.0.

Table 3: Cisco Prime Collaboration 11.0 Features

Feature Name	Feature Description	Where Documented
User Interface Changes	• 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. • Navigation in Cisco Prime Collaboration Assurance Advanced - User Interface is changed.	NA

Feature Name	Feature Description	Where Documented
Dashboards	You can view Customer Voice Portal License Usage dashlet under License Usage dashboard to view license usage for CVP call servers.	Customer Voice Portal License Usage
	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.	Contact Center Enterprise License Usage
	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.	Overview of Voice Call Grade Settings
	The OpsView dashlet is enhanced to display the hard and soft unregistered endpoints count as a separate entity.	Ops View
	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.	Conductor Bridge Pool Utilization
	You can view a new set of performance counters loaded for Cisco SocialMiner devices until version 11.0.	NA

Feature Name	Feature Description	Where Documented
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	Overview of Voice Call Grade Settings
	CDR & CMR Report is simplified to enhance the user experience. You can filter the CDR & CMR Report by using the **Display** filter panel.	CDR & CMR Call Report
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.	Session Monitoring
	Cascading of Cisco TelePresence Servers allows you to monitor TelePresence servers during ad hoc conference calls over Cisco TelePresence Conductor.	Session Diagnostics Dashboard
	New alarm is generated - CDRNotReceived.	Supported Alarms and Events for Cisco Prime Collaboration
	The VXML Server alert trap is supported from CVP devices.	Supported Alarms and Events for Cisco Prime Collaboration
	You can cross launch to CMR report from **Last Call Quality** column under 360 User View.	NA
	The Cisco Integrated Management Controller Hardware Fault trap is generated to troubleshoot any fault in the hardware components of Cisco Integrated Management Controller device.	NA

Feature Name	Feature Description	Where Documented
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.	NA
	Cisco SocialMiner and Cisco Integrated Management Controller (CIMC) devices are supported for this release. **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.	Supported Devices for Cisco Prime Collaboration Assurance.
	CDR Report now reports the following video codecs: H.264 and H.265.	NA
	Log Collection Center and Call Signaling Analyzer features are now supported in MSP mode also.	NA
	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.	Cisco Prime Collaboration 11 Ordering Guide
	Cisco Prime Collaboration supports Geo-Redundancy from this release.	Cisco Prime Collaboration Geo-Redundancy, on page 28

Feature Name	Feature Description	Where Documented
Features or Devices Not Supported From This 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. • Contacting Cisco Technical Assistance Center (TAC) by using the user interface is not supported.	NA

You can access the Cisco Prime Collaboration Assurance 11.1 features from Cisco Prime Collaboration Assurance Guide - Advanced, 11.x.

Table 4: Cisco Prime Collaboration 11.1 Features

Feature Name	Feature Description	Where Documented
Notes for Email	You can add, edit, or delete any additional information about alarms or events in **Notes for Email** under the **System** tab.	System
	You can add, edit, or delete any additional information about alarms or events in **Notes for Email** under the **Syslog Rules** tab.	Add Dynamic Syslogs
	You can add, edit, or delete any additional information about alarms or events in **Notes for Email** under the **Threshold Rules** tab.	Threshold Rules
	You can add, edit, or delete any additional information about alarms or events in **Notes for Email** under the **Correlation Rules** tab.	Correlation Rules
Notification Setup	You receive an e-mail notification with the subject line in the following format: [PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME :SEVERITY.	Set up Destinations Field Descriptions
Event Customization	You can view **Custom Rules** instead of **Exception Indicator** on **Event Customization** page.	Threshold Rules
Cluster search	You can search for a device easily from the search option in Cluster or Device drop-down list in **UC Device Search**, **Performance**, and **Event Customization**.	NA
User Interface Changes	**Monitor** > **UC Cluster Status** is changed as **Device Inventory** > **UC Device Search** in Cisco Prime Collaboration Assurance User Interface.	Unified CM Device Search

Table 5: Cisco Prime Collaboration 11.5 Features

Feature Name	Feature Description	Where Documented
Getting Started Page	You can view the end to end work flow of the product on Getting Started page. You should perform the tasks in the sequence mentioned on this page.	Get Started with Cisco Prime Collaboration Assurance
Certificate Management	• Cisco Prime Collaboration accepts only PKCS12 format certificates with .pfx or .p12 extension. • Generating Certificate Signing Request (CSR) is not supported.	Install CA Signed Certificate

Feature Name	Feature Description	Where Documented
Device Certificate Management	Device Certificate Management is no longer available in Cisco Prime Collaboration Assurance.	
User Roles and Tasks	**Report Viewer** role helps you to view and export the reports only.	Cisco Prime Collaboration Assurance-Advanced User Roles
Monitor the Cisco Prime Collaboration Assurance Server	You can monitor the Cisco Prime Collaboration Assurance Server health using the Cisco Prime Collaboration Assurance application. You can get information on CPU, memory, disk utilization, logical storage areas, and process details.	Monitor the Cisco Prime Collaboration Assurance Server
FIPS Compliance	You can enable FIPS compliance, only if you enable Cisco Prime Collaboration Assurance in ENT mode.	FIPS Setup
Auto Discovery	• Auto Discovery is not supported in MSP deployment. • “Assurance Domain” is renamed to “Associate to Domain”.	Add Devices—Auto Discovery
Manage Device Credential	• You do not need to add credentials for Cisco Device, Polycom, Cisco Unified Communications Manager Express (Cisco Unified CME), and UC500 Series devices in Credential Profiles page. • You do not need to add MSI credentials in Credential Profiles page. • You do not need to add CLI credentials in Credential Profiles page for troubleshooting. • Several devices are renamed on Credential Profiles page.	Credential Profiles Field Descriptions

Feature Name	Feature Description	Where Documented
Discovery Methods	• Renamed "Discovery Methods" drop-down list to "Discover" and re-organized the discovery methods in the Discover drop-down list. Also, added "Any Device" as a new option under the Discover drop-down list. You can view the following device options in the Discover drop-down list: • Communications Manager (UCM) Cluster and connected devices • Video Communications Server (VCS) / Expressway Cluster and connected devices • Telepresence Management Suite (TMS) and connected devices • Contact Center Customer Voice Portal (CVP) and connected devices • VCenter and connected ESXi devices • UCS Manager • Network devices using CDP • Network devices using Ping/Sweep • Any Device • You can enable or disable automatic configuration of syslog receiver and CDR billing server, when Unified Communications Manager is in managed state in Cisco Prime Collaboration.	Discovery Methods

Feature Name	Feature Description	Where Documented
Dashboard	• The cross launch to the UCM Troubleshoot and VCS Troubleshoot pages are not supported and are not available in the Endpoint Health Troubleshooting window. • Cisco TelePresence Exchange (CTX) dashboard is no longer available in Cisco Prime Collaboration Assurance. • Troubleshoot icon is not available in Conference Diagnostics Dashboard. • The Endpoint Diagnostics dashboard also displays the endpoints that are in Inaccessible state (registered, unregistered, or unknown). • CUBE SIP Trunk dashlet is added as a tab on the Utilization Monitor page. The dashlet provides information on utilized CUBE-connected SIP trunks in terms of channel usage. • The Trunks tab is updated and is renamed to T1/E1 Trunks on the Utilization Monitor page. • In the Route Group Utilization tab, you can select a route group to view the Associated Gateways/Trunks table. The table contains information on the trunk, gateway name, and gateway IP.	NA
Backup and Restore	You must perform backup and restore from FIPS-compliant setup to FIPS-compliant setup and non-FIPS compliant setup to non-FIPS compliant setup only. Backup and restore from non-FIPS compliant setup to FIPS-compliant setup or FIPS-compliant setup to non-FIPS compliant setup is not supported.	Overview of Backup and Restore
Device Status Summary	“Assurance Inventory Summary” is renamed to “Device Status Summary”.	Device Status Summary

Feature Name	Feature Description	Where Documented
General	• Exporting the device credentials from one Cisco Prime Collaboration server and importing it to another server is not supported. • In the Global Search option, the Phone and TelePresence search fields are merged and renamed as Endpoint. • The Inventory table does not display the software version that is running on the device, when the device is not registered to Unified Communications Manager. • The Inventory status reasons are modified for better understanding of the issues. • Session is renamed as Conference in Cisco Prime Collaboration Assurance. • Assurance domain is renamed as Domain in Cisco Prime Collaboration Assurance. • Cisco Prime Collaboration does not support Cisco Unified CM cluster in Mixed mode. • When you configure the SFTP credentials in Cisco Prime Collaboration Assurance, you can update the same SFTP credentials across all the managed Unified Communications Manager publishers. • The Location field displays the location that is configured on a device pool for the following features: • CDR & CMR Reports • Top 5 Poor Voice Call Quality Locations • Top 5 Call Failure Locations • In a NAT environment, the Private IP address of one customer may overlap with the Public IP address of another customer.	NA
Device support	Virtualized Voice Browser (VVB), Perimeta Session Border Controller (SBC), and Cisco Unified Attendant Console devices are supported and managed in Cisco Prime Collaboration Assurance.	Prerequisites and Recommendations

Feature Name	Feature Description	Where Documented
Features or Devices Not Supported From This Release	• Cisco TelePresence Exchange (CTX), Cisco TelePresence Multipoint Switch (CTMS), Cisco TelePresence-Manager (CTS-MAN), Cisco Unified MeetingPlace Express, Cisco Unity, Cisco Unified Expert Advisor, Wireless, and UC500 Series devices are not supported. • AES 128 and DES are the supported Authentication Privacy Protocols to enable SNMP V3. AES Authentication Privacy Protocol is not supported. • The Inventory table does not display Mediatrace Role, IP SLA Role, and Performance Monitor columns. • Cross launch of Cisco Prime Infrastructure and Cisco Prime NAM Setup from 360 Integration page is not supported. • Cross launch to device log in page from the IP address link is not supported in MSP mode. • Medianet technology is not supported. • Troubleshooting is not supported.	

Table 6: Cisco Prime Collaboration 11.6 Features

Feature Name	Feature Description	Where Documented
Certificate Management	To install CA signed certificate for secure data transmission, you must import a PKCS12 (.pfx or .p12) format signed certificate, and the certificate must contain primecollab alias.	Install CA signed certificate
NB API Support	You can access the NB API documentation by logging in to the Cisco Prime Collaboration Assurance server and select **Assurance NB API documentation** under Settings drop-down at the top right corner of the user interface.	Cisco Prime Collaboration Assurance NBI , on page 26
License Management	You can view the MAC Address and DB Server IP Address information in **License Management** page instead of System Information in the **About** page.	View License Details

Feature Name	Feature Description	Where Documented
General	After you perform an upgrade from Cisco Prime Collaboration Assurance 11.1, 11.5, and 11.5 SP1 to Cisco Prime Collaboration Assurance 11.6, the system reboots automatically.	
Device Support	Cisco Prime Collaboration Assurance supports both DX70 and DX80 devices with 7800/8800 image and ciscoDX70 and ciscoDX80 devices with Collaboration Endpoint (CE) image.	Prerequisites and Recommendations
HTTP Download Test	This feature allows you to download a configuration file from the HTTP server using a HTTP get-file operation on the HTTP server.	Create an HTTP Download Synthetic Test
Export Synthetic tests	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.	Manage Synthetic Tests
UCM SIP Trunks	You can view information about utilization (audio and video maximum calls, and total active calls), default value of the maximum concurrent calls, SIP trunk status and flag, running nodes, remote destination, and the associated trunk details of the SIP trunks connected to the Unified Communications Manager cluster. UCM SIP Trunk is added as a tab on the Utilization Monitor page. Choose **Monitor** > **Utilization Monitor** > **UCM SIP Trunk** in Cisco Prime Collaboration Assurance User Interface.	UCM SIP Trunks

Feature Name	Feature Description	Where Documented
Ops View and list view	The OpsView dashlet is enhanced to display the details of SIP trunks that are connected to a Unified Communications Manager cluster.	Ops View
Color Codes in the Treemap View	The OpsView dashlet is enhanced to provide a color coded Treemap view of the devices in a cluster, their status and the severity of the alarms.	Ops View
Leaf creation for Trunks	The Network Health View dashlet displays the count of trunks and their status in a SIP Cluster.	NA
Trunk Group Utilization	You can graphically view channel usage of the most utilized trunks against time, their gateway IP and name, and other route group details.	Trunk Group Utilization
LDAP Configuration Parameters	Cisco Prime Collaboration Assurance supports login to PCA with CN or sAMAccountName or uid attributes of an LDAP user as applicable and should be unique.	LDAP Configuration Parameters