Manage Inventory

This section explains the following:

Manage Inventory

This chapter provides information about managing inventory.

View Inventory Details

Cisco Prime Collaboration Assurance performs continuous, real-time discovery of inventory. You need to periodically update the inventory so that you have up-to-date information about your network. You can schedule how often you want to update inventory.

When you update inventory, the inventory synchronizes with the Cisco Prime Collaboration Assurance database. The Cisco Prime Collaboration Assurance inventory reflects every addition, deletion, and modification that occurs in the network after update.

In Cisco Prime Collaboration Assurance, devices are grouped based on the device type. The Device Group pane is available in the Inventory Management, Conference Diagnostics (as a filter), Endpoint Diagnostics, and Alarms and Events pages. You can select devices or endpoints from the groups you are interested in, to check inventory details.

Note Cisco Telepresence Endpoints discovered as TC/CE device type in Cisco Prime Collaboration Assurance should not be included in the JTAPI user controlled devices list. We recommend you to keep the IP Phones into the JTAPI user controlled list.

You can hover over the device host name column in the inventory table, and click the Device 360 ° view to see device details, such as alarms, interfaces, ports, environments, modules and other device-specific capabilities of that device. For more information, see Device 360° View. The inventory table also displays the software version of the devices that are managed and registered to Unified Communications Manager. The devices include soft phones, hard phones, and Jabber.

In addition to the inventory table, the Inventory Management page contains System Information, Access Information, Interface Information, and Event Settings panes that appear below the inventory table. All of these panes are populated based on the last polled data. A device must be in the Managed state at least once for these details to be displayed.

Inventory Pane

The current inventory table is available in the Inventory page.

Each device that is managed by Cisco Prime Collaboration Assurance is modeled to display the physical inventory of a device (interface and peripherals). To view the inventory details for a device, click on a row in the Current Inventory pane.

To select multiple devices (first 500 entries), use the check box available on the top left corner of the Current Inventory pane.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can assign a customer to a device or devices by selecting the device(s), and then clicking on the **Edit > Assign**. The Edit Device dialog box appears, from where you can select the customer name from the drop-down list. You can assign a customer to a cluster too, by selecting the cluster from the Device Group pane, select the Host Name check box (this selects all the devices of the cluster), and then click **Edit > Assign**. Similarly to unassign a customer, select the device(s), and then click **Edit > Unassign**.

You can modify the credentials and rediscover devices using the Modify Credentials option. Click on Job Progress in the confirmation message window and cross launch to the Jobs Management page to see the details of the discovery job.

For Cisco Prime Collaboration Release 11.1 and earlier

You can enable, disable or set different options for automatic troubleshooting using the Threshold Settings option.

You can suspend and resume the management of the device using the Suspend and Resume options. Inventory is not updated for devices in the Suspended state.

You can use the show drop-down list on the inventory table to filter devices based on the device type and state. For example, if you want to rediscover all deleted devices in your network, select Deleted from the show drop-down list. The inventory table will list all deleted devices. Perform rediscovery to discover these devices.

For example, if you want to rediscover all deleted devices in your network, select Deleted from the show drop-down list. The inventory table will list all deleted devices. Perform rediscovery to discover these devices.

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

The Total field in the upper right corner of the inventory table displays the device count. To view the number of devices in a group, select the group.

For example, to view the number of phone endpoints, select the Endpoints group in Device Group. The number of endpoints will be updated in the Total field. For more information on the device count, see the Field Descriptions for the Current Inventory table.

You can view the list of unknown endpoints by selecting Device Group Selector > Predefined > Unknown Endpoints.

For Cisco Prime Collaboration Release 12.1 and later

You can enable, disable or set different options for automatic troubleshooting using the Threshold Settings option.

You can suspend and resume the management of the device using the Suspend and Resume options. Inventory is not updated for devices in the Suspended state.

You can use the show drop-down list on the inventory table to filter devices based on the device type and state.

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

The Total field in the upper right corner of the inventory table displays the device count. To view the number of devices in a group, select the group.

For example, to view the number of phone endpoints, select the Endpoints group in Device Group. The number of endpoints will be updated in the Total field. For more information on the device count, see the table on "Field Descriptions for the Current Inventory Table".

You can view the list of unknown endpoints by selecting **Device Group Selector** > **Predefined** > **Unknown Endpoints**.

This table describes the fields on the Inventory table. Not all columns of the inventory table appear by default. To see all the columns, click the Settings option on the top right corner. You can export the inventory table as a CSV or a PDF file by clicking the Export icon at the upper right corner of the inventory table.

Table 1: Field Descriptions for the Current Inventory Table

Field	Description
Endpoint Name	Name assigned to the endpoint for ease of identification.
Extension	Directory Number of endpoints. This number helps to identify a device uniquely.
Phone Description	A unique description of the endpoints that you have added during configuring the devices on Cisco Unified Communications Manager (CUCM) or Cisco TelePresence Video Communication Server (VCS).
Host Name	Name assigned to the device for ease of identification.
Model	Device model, such as Catalyst3506G48PS.

Field	Description
IP Address	IP address used for managing the device. Click on the IP address to log into the device. This feature is not available in MSP mode. Click on the quick view icon to launch the Device 360 Degree View for that device. If that device is an endpoint the Endpoint 360 Degree View appears. If these devices are discovered by logical discovery then the IP Address and Private IP address will be same. For routers and switches, you must associate a terminal client application, such as Putty, to log into the device.
Mac Address	MAC Address of the devices.
Software Type	Software running on the device, such as IOS, CatOS.
Software Version	Software version running on the device. **Note** The Software Version field displays NA when the device is not registered to Unified Communications Manager.
Device Pool	Only for CUCM registered devices.
Partition	Only for CUCM registered endpoints.
Serial Number	Applicable only for endpoints.
State	Status of the device.
Status Reason	Reason for the device status.
Type	The most applicable role or service of the device.
Capabilities	All other roles or services of the device.
Last Discovered	Date and time when the device was last discovered. The time will be according to the time zone set in the Cisco Prime Collaboration Assurance server.
For Cisco Prime Collaboration Release 11.1 and earlier Customized Events	• Green check mark displayed—Event settings are customized for the device using Customize Events tab. • Green check mark not displayed—Event settings are not customized for the device. The device uses global settings.

Field	Description
For Cisco Prime Collaboration Release 11.1 and earlier Mediatrace Role	• Unsupported—Device does not support Cisco Mediatrace. • Transparent—Device supports Cisco Mediatrace but profile is not configured. • Responder—Cisco Mediatrace responder profile is enabled on the device. Enable this profile if you want to monitor and collect information on Cisco Mediatrace. • Initiator—Cisco Mediatrace initiator profile is enabled on the device. Enable this profile if you want to initiate Cisco Mediatrace session or polls. • Initiator/Responder—Cisco Mediatrace initiator and responder profiles are enabled on the device.
For Cisco Prime Collaboration Release 11.1 and earlier IP SLA Role	• Unsupported—Device does not support Video IP SLA. • Not Configured—Device supports the Video IP SLA but the device is not configured. • Responder—IP SLA Responder profile is configured on the device. The device that is configured with this profile processes measurement packets and provides detailed time stamp information. The responder can send information about the destination device's processing delay back to the source Cisco router.
For Cisco Prime Collaboration Release 11.1 and earlier Performance Monitor	• Unsupported—Device does not support Cisco Performance Monitor. • Not Configured—Device supports Cisco Performance Monitor but the device is not configured. • Configured—Cisco Performance Monitor is enabled to allow you to monitor the flow of packets in your network and become aware of any issues that might impact the flow.

Note

- To update the unknown phones in inventory, trigger Cluster Data Discovery. This is triggered automatically at midnight.
- If you change the IP address or swap IP addresses, the device type is not identified. In such a case:
  - Navigate to the */opt/emms/emsam/conf/* folder and edit the *emsam.properties* file.
  - Find the line *com.cisco.nm.emms.devicetype.rediscovery = false* and change the value from 'False' to 'True'.
  - Restart Cisco Prime Collaboration Assurance Server by logging in as admin user and execute the following commands:
    - **application stop cpcm**
    - **application start cpcm**
  - Rediscover the device.

The Mobile Remote Access (MRA) clients (such as Cisco Jabber, Cisco TelePresence MX Series, Cisco TelePresence System EX Series, and Cisco TelePresence SX Series) have the same IP address as that of the Cisco Expressway-Core device in Cisco Unified Communications Manager, however in Cisco Prime Collaboration Assurance the IP Address is shown as NA.

Note Device 360° View is available for MRA clients.

Related Topics

Conference Diagnostics Dashboard
Manage Device Groups
Unified CM Cluster Data Discovery

Device 360° View

You can get a concise summary information regarding any device through its 360° view. Rest your mouse over a device IP address, then click the quick view icon to launch the Device 360° View window. You can also do a global search for a device to see the device details in the Device 360° View.

In addition to viewing device information such as status, location, you can also view modules, alarms, and interfaces on the device, invoke tools like ping, and traceroute for that device.

If the device belongs to a cluster, you can cross launch to the cluster view of the cluster the device belongs to, by clicking on the Cluster ID value.

Note If you are using Internet Explorer 10 and 11, ensure that you have the recommended browser settings to view the Device 360° View window. Press F12 in your browser and set the following:

- For Internet Explorer 10:
  - **IE10 Browser Mode**: IE10 or IE10 Compatibility View
  - **Document Mode**: Standards (Default) or Quirks
- For Internet Explorer 11:
  - **Browser Profile**: Desktop
  - **Document Mode**: Edge (Default)

Launch the browser again to view the Device 360° view window.

The 360° Device View window contains the following device details:

Table 2: Field/Buttons and their Description

Field	Descriptions
State	You can hover on the State icon to know the state of the device. Different colors of the icon represent different states.
Status Reason	You can hover over the icon to know the status reason of the device and any additional activities you need to perform to make all features work. Different colors of the icon correspond to the state the device is in.
Host Name	—
Host IP /Global IP Address	You can click the IP address to launch the device management page. To log into routers and switches, ensure that you click on the IP address and associate a terminal client application, such as TELNET or SSH. This feature is not available in MSP mode.
MAC Address	MAC address of the device.
Type	The device type or primary role or capability of the device is mentioned on the right corner below the hostname row. For example, Finesse, Unified CM or Unity Connection.
Host Name	If you have deployed Cisco Prime Collaboration Assurance in MSP mode in a NAT environment, you will see the host name of the device.
Customer	If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to.

Field	Descriptions
Version	Software version of the device.
Last discovered	Time stamp of last successful discovery.
Cluster ID	Cluster ID of the cluster the device belongs to. You can click on the cluster ID to launch the Cluster Details page.
—	Click the support community icon to open the Cisco Support Community Dialog box which has the related posts and discussions filtered for the device. You can post a question for that device. You can go to the support pages of other devices, and also visit the support community page of Cisco Prime Collaboration Assurance. To visit the Cisco Prime Collaboration Assurance page, click **Visit the Cisco Support Community**, click on Navigate to a Community Topic and Post pane, then click **Collaboration, Voice and Video**. In the Collaboration, Voice and Video Communities table, click **Prime Collaboration Management**. You can post questions in the Cisco Prime Collaboration Community forum, and look for related questions or information in existing discussions, videos, and additional documents for your issues. For business impacting technical issues, we recommend that you open a service request with Cisco TAC for timely support.
—	Click the ping icon to ping the device and get ping statistics, such as the number of packets transmitted and received, packet loss (in percentage), and the time taken to reach the device by ping in milliseconds (ms).
—	Click the traceroute icon to know the route to reach the device, the number of hops to reach the device, and the time elapsed at each hop in milliseconds (ms).
—	Click the tasks icon, and select from the drop-down list to perform multiple tasks such as launching performance graphs and managing thresholds. **Note** The options available depend on the device you have selected.

Other device-specific information is as follows:

Table 3: Device 360° View - Tabs Description

Tabs	Description
Alarms	It includes the following: • Severity — Severity of the alarm • Status — Status of the alarm • Name — Name of the device • Component — Name of the component that has alarms • Last Updated — Time stamp of the last alarm generation.
Interfaces	It includes details on interfaces, voice interface and port (whichever applicable for the device). It specifies the card is playing on a particular port, and the capability of the card. The following information is available for the interface, voice interface and port: • Operation Status (Oper Status) — Operational state of the device • Admin Status — Administrative status of the interface • Name — Description of the device • Address — Physical address of the device • Type — Device type
Card/Services	It includes the following: • Name — Description of the voice/service • Version — Version of the card/service • Status — Status of the card/service
Port	—
Environment	It includes: • Power supply • Fan • Temperature sensor • Voltage sensor
Device-specific details	—

You can view the Differentiated Services Code Point (DSCP) values (both in decimal format and its meaning) for Cisco TelePresence TX Series under the Connectivity Details tab of the Endpoint 360° View of the devices.

Choose **Inventory Management**, and click on the IP Address column to launch the Endpoint 360° View.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **Inventory Management**, and click on the IP Address column to launch the Endpoint 360° View.

For more information on Differentiated Services Code Point (DSCP) values, see RFC 2474.

Note The fields displayed depend on the device you have selected.

Click the **View More** button on top to:

- View the Device 360° View pop up in window size.
- Create performance dashboards for Cisco Unified Communication applications/devices by selecting specific counters. For more information, see Create Custom Performance Dashboards.

Metric Charts

You can view metric charts for voice devices (excluding phones) and CTS. These charts appear only for devices in managed state and for which at least one poling cycle is over.

Note It will take time for the chart to appear after the device is in managed state. This is because polling has to be completed to fetch data for these charts.

These charts display values for CPU, Memory and Hard Disk utilization etc. You can view maximum, minimum and current value (in percentage or bytes in MB) of the last hour. Each bar on the metric chart denotes a period of four minutes, thus there are 15 bars, each denoting the value for four minutes. The figures in brown represent the minimum value, and the figures in blue represent the maximum value for the last hour.

You can click **See More** to launch performance graphs for some devices.

For an Multipoint Controller (MCU) you can see the absolute values and percentage of Audio and Video Port utilization in the performance graphs. You can select these options near the top right of the chart.

Performance graph is available for TP Server. You can see the absolute values and percentage.

Note The metric charts and performance graphs availability depend on the device you have selected.

Global Search Options for Cisco Prime Collaboration Assurance

For Cisco Prime Collaboration Release 11.6 and 12.1

The following table describes the Global Search options for Cisco Prime Collaboration Assurance.

Table 4: Global Search Options for Cisco Prime Collaboration Assurance

Search	Variable	Sample String Format	Exceptions and Allowed Search Strings
Endpoint	DN	10002|1000*| 100*| 1*| *0002	Alphanumeric characters, dash, period, and underscore.
	IP	10.64.101.162 | 10.64.101.* | * 10.78.22.77| . | 10.78.22.*| 10.78.*.*| 10.*.*.*| *.	Alphanumeric characters, dash, period, and underscore. The special character % does not retrieve results. Ampersand (&) and blank space are not allowed.
	MAC	00260bd75cf8| 00260bd75cf*| 00260bd*| 0*| 00*	Dash, period, underscore, are not allowed. Alphanumeric and blank space are allowed. **Note** When you search for phones using the MAC address in the global search option, do not use colon or hyphen or dots in between.
	Endpoint Name	San Jose	-
Device	IP	10.78.22.129| 10.78.22.*| 10.*	Alphanumeric characters, dash, period, underscore, and space.
	DNS	cussmtest-15.cisco.com	If the domain name is not resolvable, the IP address is displayed in the search results.
User	First Name or Last Name or User Name	HS John	Alphanumeric characters, dash, underscore, and blank space are not allowed.

For Cisco Prime Collaboration Release 11.6 and 12.1

Search Results

Search Parameter	Search Result
Endpoint	Endpoint Name, Directory Number, IP Address, IPv6 Address, MAC Address, Model, Cluster Name, Software Version, Registration Status, and Status Reason. When you perform an endpoint search, all phones and Cisco TelePresence endpoints are also included in the search. You can click on the icon next to the IP address to launch the Endpoint 360° View for that endpoint.
Device	Name, IP Address, Status, and Device Type. When you perform a device search, all phones and Cisco TelePresence endpoints are also included in the search. You can click on the icon next to the device name to launch the Endpoint or Device 360° View for that device. **Note** The information displayed depends on the device you have searched for.
User	First Name, Last Name, and User Name. You can click on the icon next to the user name to launch the User 360° View for that user.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you can also see the customer to which the searched device belongs to. If the device belongs to multiple customers, then all the customers to which it belongs are mentioned. If the device is not associated with any customer or is associated with all customers, it is part of the default customer domain - All Customers, but shows a blank for customer details in the search result. You can click on the customer name to launch the home page filtered for that customer.

Search Use Cases

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

Table 5: Search Use Cases

To search for...	Perform/Use
All devices belonging to a particular customer.	Select the customer from the global customer selection drop-down list at the top right of your screen, select Device search, and then enter the search string *.
Cisco Jabber	Endpoint Search
E20	Endpoint Search
Infrastructure devices	Device Search
IP address of a device with a partial IP address.	Device Search - For example search with a string such as 10.*
List of all users associated with a particular customer.	Select the customer from the global customer selection drop-down list at the top right of your screen, select User search, and then enter the search string *.

Inventory Summary

The Inventory Summary lists the count of devices based on the device state. The Total column displays the total number of devices in a particular state. The device count is available as a cross-launch to the Inventory table in Inventory Management. When you click on any count, you will be directed to the Inventory table, where you can see all the devices in that particular state.

The Inventory Summary is available as a slider at the bottom of your user interface browser. You can view the details when you scroll down. The Inventory Summary data is refreshed every 30 seconds.

Table 6: Inventory Summary - Field Descriptions

Field	Descriptions
Unknown Endpoints	Total number of unknown endpoints. You can click on this number to launch the filtered list of unknown endpoints in the Endpoint Diagnostics page.
Partially Managed	Devices which are in managed state but have some credentials missing. These credentials are not mandatory for managing inventory, but required for all other features, such as troubleshooting to work. You can click on the corresponding number to cross launch to see a list of all devices in the inventory table which are managed but with insufficient credentials. This count is updated only when you perform rediscovery after adding the credentials.

Note Although the Total Count column contains the sum of the Infrastructure Devices, Endpoints columns combined for each device state, you may see some inconsistency in the number of devices in the Total Count column. This difference can happen when the computation includes device types in Unknown state from the inventory.

Device Status Summary

For Cisco Prime Collaboration Release 11.5 and later

The Device Status Summary lists the count of devices based on the device state. The counts does not include Phones & Unknown devices. The device count is available as a cross-launch to the Inventory table in Inventory Management. When you click on any count, you will be directed to the Inventory table, where you can see all the devices in that particular state. You can filter count based on Customer/Assurance Domain.

The **Device Status Summary** is available under **Inventory** > **Device Status Summary**. The **Devices** column displays the total number of devices in a particular state. The **Status** column displays the status of the devices. When you click on **Discovery Jobs**, you will be directed to **Job Management** page and where you can see the status of the discovery job.

You can view the following device status. For more information on status, see “Discovery Life Cycle” section in *Cisco Prime Collaboration Assurance Guide- Advanced*.

- Managed

- Partially Managed
- Inaccessible
- Unreachable
- Suspended
- Unsupported
- Undiscoverable

When you hover your mouse over Partially Managed, Inaccessible, or Undiscoverable states, you can view a tool tip with an explanation.

You can view Unmanaged device count in the global summary bar, adjacent to **Inventory Summary**. When you click on the count, you will be directed to **Device Status Summary** page.

Table 7: Device Status Summary - Field Descriptions

Field	Descriptions
Device Discovery Status	Displays the device discovery status.
Devices Discovery In-Progress <count>	Displays the number of devices for which discovery is in progress. Devices Discovery In-Progress <count> is not displayed, if there are no discovery in progress.

For Cisco Prime Collaboration Release 12.1 and later

The Device Status Summary lists the count of devices based on the device state. Devices, as referred to in this table, include Infrastructure components and Video/TelePresence endpoints. Phones are not counted (which includes DX series). When you click on any count, you will be directed to the Inventory table on the **Inventory Management** page, where you can see all the devices in that particular state. You can filter count based on Customer/Assurance Domain.

The Device Status Summary is available under **Inventory** > **Device Status Summary**. The **Devices** column displays the total number of devices in a particular state. The **Status** column displays the status of the devices.

When you click on **Discovery Jobs**, you will be directed to **Job Management** page from where you can see the status of the discovery job.

You can view the following device status. For more information on status, see "Discovery Life Cycle" section in Cisco Prime Collaboration Assurance Guide- Advanced.

Device Status Summary data is divided into 2 categories: Managed and Unmanaged.

- Managed category includes the following:
  - Discovered successfully
  - Partially Managed
- Unmanaged category includes the following:
  - Inaccessible
  - Unreachable

- Suspended
- Unsupported
- Undiscoverable
- Unknown

When you hover your mouse over Partially Managed, Inaccessible, Unreachable, or Undiscoverable state, you can view a tool tip with an explanation.

The count for both categories (Managed and Unmanaged) should match the sum of count of devices in the respective categories.

You can view Unmanaged device count in the global summary bar, adjacent to **Inventory Summary**. This count must match the Unmanaged device count in the **Device Status** table. When you click on the count, you will be directed to **Device Status Summary** page.

Table 8: Device Status Summary - Field Descriptions

Field	Descriptions
Device Discovery Status	Displays the device discovery status.
Devices Discovery In-Progress <count>	Displays the number of devices for which discovery is in progress. Devices Discovery In-Progress <count> is not displayed, if there are no discovery in progress.

Troubleshooting

Issue: CUCM rediscovery causes Pub to disappear from Cisco Prime Collaboration Assurance Inventory. This is due to the co-resident ELM/PLM configuration on CUCM. Since Cisco Prime Collaboration Assurance is case sensitive the ELM/PLM configuration should match the hostname of CUCM.

For example, if the co-resident ELM/PLM configuration on CUCM has a hostname lax-ccm-px.apl.com whereas the hostname of CUCM is LAX-CCM-PX.apl.com then, when you perform a re-discovery of the CUCM Pub, the CUCM Pub disappears from the inventory or gets deleted.

Recommended Action: Modify the file **/etc/hosts** of Cisco Prime Collaboration Assurance to re-discover the CUCM pub. Add an entry to the host file like the one mentioned below.

10.8.2.20	LAX-CCM-PX.apl.com

Inventory Status Error Messages

The credential verification error messages are tabulated below.

Table 9: Credential Verification Error Messages

Error Message	Condition	Possible Solutions
SNMP_ERROR	Failed for one of the following reasons: • SNMP service is enabled in the device • SNMP credentials do not match. • Firewall settings blocking the port.	• Verify if SNMP service is enabled in the device • Verify and reenter the device SNMP credentials in the credential profile. • Verify if firewall settings blocks the port, and unblock the port using the correct port. For more information on required port, see Required Ports for Prime Collaboration.
UNKNOWN_ERROR	Error in discovering the device.	Perform a re-discovery. If issue persists, contact TAC for assistance.
INSUFFICIENT_INV_COLLECTION	The device is taking a longer time to respond than expected, may be due to the network latency.	Verify the the SNMP/HTTP(S) response time and perform a rediscovery. If the issue persists, contact TAC for assistance.
HTTP_ERROR	HTTP access has failed. Failed for one of the following reasons: • HTTP(S) credentials do not match • Firewall settings blocking the port.	• Verify and reenter the device HTTP credentials in the credential profile. • Verify if firewall settings blocks the port, and unblock the port using the correct port. For more information on required port, see Required Ports for Prime Collaboration.

Error Message	Condition	Possible Solutions
JTAPI_ERROR	JTAPI access has failed. Firewall settings blocking the port.	• Verify and reenter the device JTAPI credentials in the credential profile. **Note** Password must not contain a semicolon (;) or equals symbol (=). • Verify if firewall settings blocks the port, and unblock the port using the correct port. For more information on required port, see Required Ports for Prime Collaboration. • Verify if JTAPI user is configured in Cisco Unified CM. For more information to enable JTAPI, see Configure Devices for Prime Collaboration Assurance
UNSUPPORTED_DEVICE	Device is unsupported	Verify the supported devices from Supported Devices for Cisco Prime Collaboration Assurance.
UNDISCOVERABLE	Error while persisting	Perform a re-discovery. If issue persists, contact TAC for assistance.
DISCOVERY_FAIL_TOO_MANY_DB_CONNECTIONS	Error while persisting	Perform a re-discovery. If issue persists, contact TAC for assistance.

Device-Specific Inventory Details

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

- Table 10: Cisco Codec, MX, E20, and MXP
- Table 11: Cisco TelePresence Movi
- Table 12: Cisco Unified IP Phone 8900 and 9900 Series
- Table 13: CTMS
- Table 14: Cisco TMS
- Table 15: Cisco Unified CM
- Table 16: Cisco MCU and MSE
- Table 17: Cisco VCS

- Table 18: Cisco TelePresence Conductor

Table 10: Cisco Codec, MX, E20, and MXP

Field		Description
TelePresence Endpoint (Data displayed based on selected endpoint type CTS, Cisco Codec, MX, E20, MXP, .)	Endpoint Name	Name assigned to the endpoint for ease of identification.
	Directory Number	IP phone details as defined in the endpoint.
	Call Controller	
	CUCM Address	Hostname or IP address of the Cisco Unified CM server where the endpoint is registered.
	CUCM Cluster ID	Identification of the Cisco Unified CM cluster where the Cisco Unified CM server is registered.
	VCS Address	Hostname or IP address of the VCS server where the endpoint is registered.
	VCS Cluster ID	Identification of the VCS cluster where the VCS server is registered.
	Registration Status	Registration status of the endpoint with call processor (Cisco Unified CM or VCS). If Cisco Unified CM or VCS is not managed, the information displayed is N/A.
	H323 ID	H.323 ID configured on the Cisco Codec device.
	E164 No	E164 number configured on the Cisco Codec device.
	H323 Gatekeeper Address	Network address of the gatekeeper to which the Cisco Codec device is registered.
	SIP URI	Registered SIP URI on the Cisco Codec device.
	SIP Proxy Address	SIP proxy address that is configured manually on the Cisco Codec device.

Field		Description	
	Application Manager		
	TMS	Hostname or IP address of the application manager where the Cisco Codec device is integrated.	
	Switch Details		
	Connected To Switch	Details of the switch to which the endpoint is connected.	
	Port Connected	Details of the switch port to which the endpoint is connected.	
	Peripherals	Name	Peripheral type, such as uplink, phone, camera, display, touch screen monitor, microphone.
Position		Position of the peripheral, such as *front_center* for a microphone.	
MAC Address		MAC address of the peripheral.	
Software Version		Software version running on the peripheral.	
Model		Model of the peripheral.	
Serial		Serial number of the peripheral.	
Make		Manufacturer's details for the peripheral.	
Firmware Version		Firmware version of the peripheral.	
Hardware Version		Hardware version of the peripheral.	
Midlet Version			

Field		Description
		Midlet version running on the peripheral.

Note Cisco Prime Collaboration Assurance does not support peripheral details for Cisco TelePresence 150 MXP.

Table 11: Cisco TelePresence Movi

Field		Description
Movi	Endpoint Name	Name assigned to the endpoint for ease of identification.
	SIP URI	Registered SIP URI on the Cisco TelePresence Movi endpoint.
	VCS Address	Hostname or IP address of the VCS where the endpoint is registered.
	VCS Cluster ID	Identification of the VCS cluster where the VCS is registered.

Table 12: Cisco Unified IP Phone 8900 and 9900 Series

Field		Description
CUCM Endpoint	Endpoint Name	Name assigned to the endpoint for ease of identification.
	Model	Model of the endpoint, such as CP-8945 or CP-9971.
	Directory Number	IP phone details as defined in the endpoint.
	Serial Number	Serial number of the endpoint.
	Description	Description of the endpoint as defined in the call processor.
	Call Controller	
	CUCM Address	Hostname or IP address of the Cisco Unified CM server where the endpoint is registered.
	CUCM Cluster ID	Identification of the Cisco Unified CM cluster where the Cisco Unified CM server is registered.
	Registration Status	Registration status of the endpoint with call processor (Cisco Unified CM). If Cisco Unified CM is not managed, the information displayed is N/A.
	Switch Details	
	Connected To Switch	Details of the switch to which the endpoint is connected.
	Port Connected	Details of the switch port to which the endpoint is connected.
Status	Displays the status of the wi-fi connection, such as connected or not connected.	
IP Address	IP address used to manage the endpoint when connected using a wi-fi network.	
Default Router	IP address of the default router to which the endpoint is connected.	

Field		Description
Access Point Name	Name of the access point to which the endpoint is connected.	
Ethernet Details		
Status	Displays the status of the Ethernet connection, such as connected or not connected.	
IP Address	IP address used to manage the endpoint when connected using Ethernet.	

Note For discovery of Cisco Unified IP Phone 8900 and 9900 series, you must enable the HTTP interface. If the HTTP interface is not enabled, these devices will not appear in the inventory table.

Table 13: CTMS

Field		Description
Multipoint Switch	Timezone	Time zone configured on the multipoint switch.
	SKU	—
	Hardware Model	Model number of the media convergence server on which the multipoint switch is running.
	Software Version	Version of multipoint switch administration software currently installed.
	OS Version	Operating System version.
	Hostname	Hostname configured for the multipoint switch.
	IP Address	IP address used to manage the multipoint switch.
	Subnet Mask	Subnet mask used on the IP address.
	MAC Address	MAC address of the media convergence server on which the multipoint switch software is running. This MAC address belongs to Ethernet interface 0 (the eth0 network interface card [NIC]). With failover, this MAC address persists, although another Ethernet interface becomes active.
	Switch Details	
	Connected To Switch	Details of the switch to which the multipoint switch is connected.
	Port Connected	Details of the switch port to which the multipoint switch is connected.
	Ad hoc Segments	Maximum number of segments that are available for impromptu meetings. The maximum number is 48.
	Maximum Segments	

Field		Description
		Total number of segments (individual video displays) that this multipoint switch can handle. The maximum number is 48.
	Schedulable	Number of segments available at any one time for scheduled meetings. The multipoint switch automatically derives this value by subtracting the defined number of ad hoc Segments from the defined number of maximum segments.

Table 14: Cisco TMS

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

Field		Description
System Connectivity (see note following this table)	Status	Whether the exchange server is running or down.
	IP Address	IP address assigned to the exchange server.
	Software Version	Version of software currently installed on the exchange server.
	Status	Whether the LDAP server is running or down.
	IP Address	IP address assigned to the LDAP server.
	Software Version	Version of software currently installed on the LDAP server.

Table 15: Cisco Unified CM

Field		Description
Call Processor	Cluster ID	Parameter that provides a unique identifier for the cluster. This parameter is used in Call Detail Records (CDRs), so collections of CDR records from multiple clusters can be traced to their sources. The default is StandAloneCluster.
	Publisher Hostname	Hostname configured for the cluster publisher.
	Registered CTS Endpoints	Number of registered endpoints on the call processor.
	Total CTS Endpoints	Total number of endpoints.

Table 16: Cisco MCU and MSE

Field		Description
MCU or MSE Details (Data displayed based on selected conferencing device: MCU or MSE.)	Hardware Model	Model number of the media convergence server on which the multipoint switch is running.
	Serial Number	Serial Number of the Multipoint Control Unit (MCU).
	Software Version	Version of multipoint switch administration software currently installed.
	MCU Type/Device Type	Type of the MCU or device.
	Build Version	Build version of the installed software.
	Manufacturer	Manufacturer's name.
	Hostname	Hostname configured in the device (MCU or Media Service Engine).
	IP Address	Local IP address of the MCU or Media Service Engine (MSE) network interface used to access the MCU or MSE web user interface.
	Subnet Mask	Subnet mask used on the IP address.
	MAC Address	Fixed hardware MAC address of the Ethernet port.
	Connected To Router	IP address of the router to which the MCU or MSE is connected.
	Cluster Type	Whether the cluster is a master or slave. If the cluster is configured, *Not Configured* is displayed.
	Total Video Ports	Number of video ports configured in MCU. (Data displayed only for MCU devices.)
	Total Audio Ports	Number of audio ports configured in MCU. (Data displayed only for MCU devices.)
	SIP (Data displayed only for MCU devices.)	
	Status	

Field		Description
		Whether the SIP registration is enabled or disabled.
	Proxy	Network address of the SIP proxy.
	Domain	Network address of the SIP registrar to which the MCU has registered.
	H.323 (Data displayed only for MCU devices.)	
	Status	Whether the H.323 gatekeeper registration is enabled or disabled.
	Gatekeeper ID	Identifier used by the MCU to register with the H.323 gatekeeper.
	Gatekeeper Address	Network address of the gatekeeper to which the MCU has registered.
MSE Blades (Data displayed only for MSE.)	Type	Type of the blade.
	Slot	Slot number. Slot 1 is MSE Supervisor; slots 2-10 are blades.
	Software Version	Version of the software used.
	Status	Status of the blade: OK or absent.
	Port A IP Address	IP address of Port A.
	Port B IP Address	IP address of Port B.

Table 17: Cisco VCS

Field		Description
Call Processor	Cluster ID	Cluster Name that is used to identify one cluster of VCSs from another.
	Master	Name of the VCS peer that is configured as the cluster master.
	Registered Endpoints	Number of endpoints registered to the VCS.
	Peers	Number of VCS peers configured within the cluster.

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

Note Cisco Prime Collaboration Assurance manages both the Cisco VCS application and appliance.

Table 18: Cisco TelePresence Conductor

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

Note Only Cisco TelePresence Conductor-controlled MCU cascading is supported.

For Cisco Prime Collaboration Release 11.5 and later

Note The following devices are not supported:

- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence-Manager (CTS-MAN)

Update and Collect Inventory Details

Updating and collecting inventory details depend on the type of network deployed: voice, video or both. It also depends on the data you want to collect at a given point. The following table recommends when to update inventory based on your network.

Table 19: Recommendations to Update Inventory

Description	Task
If you have both voice and video endpoints deployed in your network, and want to collect data on both.	Perform Update Inventory (choose **Device Inventory** > **Inventory Management** > **Update Inventory**). For more information, see Update Inventory. **For Cisco Prime Collaboration Release 11.5 and later** Choose **Inventory** > **Inventory Management** > **Update Inventory**
If you have both voice and video endpoints deployed in your network, and you want to collect data on video endpoints only.	Perform Update Inventory (choose **Device Inventory** > **Inventory Management** > **Update Inventory**). For more information, see Update Inventory. **For Cisco Prime Collaboration Release 11.5 and later** Choose **Inventory** > **Inventory Management** > **Update Inventory**
If you have both voice and video endpoints deployed in your network, and you want to collect data on voice endpoints only.	Perform Cluster Data Discovery (choose **Assurance Administration**). For more information, see Inventory Details Collection. **For Cisco Prime Collaboration Release 11.5 and later** Choose **Alarm & Report Administration**.

Description	Task
If you have only a voice network	Perform Cluster Data Discovery (choose **Assurance Administration**). For more information, see Inventory Details Collection. **For Cisco Prime Collaboration Release 11.5 and later** Choose **Alarm & Report Administration**.
If you have only a video network	Perform Update Inventory (choose **Device Inventory** > **Inventory Management** > **Update Inventory**). For more information, see Update Inventory. **For Cisco Prime Collaboration Release 11.5 and later** Choose **Inventory** > **Inventory Management** > **Update Inventory**

Update Inventory

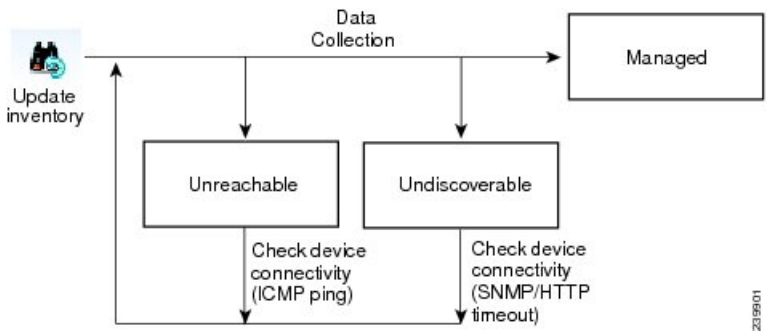
The Update Inventory task helps you to synchronize the Cisco Prime Collaboration Assurance Inventory database with the network. During this task, accessibility verification is not performed (see the Update Inventory Lifecycle chart).

Perform the Update Inventory task when:

- You want to synchronize the database for all devices managed in your network. However, you can update the configuration details for specific devices based on the device status criteria.
- You want to define a periodic Update Inventory job to keep the Cisco Prime Collaboration Assurance database up-to-date.
- There are any changes in the network devices' interfaces.

Note The new devices that are added to the network will not be identified.

Figure 1: Update Inventory Lifecycle



We recommend that you define a periodic Update Inventory job to keep the Cisco Prime Collaboration Assurance database up-to-date.

To update inventory:

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

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **Inventory Management**

Step 2 In the **Inventory Management** page, click **Update Inventory**.

Step 3 If you want to update the inventory based on device status, check the Update devices based on device criteria check box in the Update Inventory window and select the desired device criteria from the drop-down list.

If you choose to update the inventory based on device status, an accessibility information check is performed. If you do not, the inventory is updated with all devices in the Managed state. Device accessibility is not checked.

To schedule a periodic update inventory job, go to add **step 4**. To run the job immediately, go to **step 5**.

Step 4 Enter the job name and the scheduling details. See Job Schedule - Field Descriptions for field descriptions.

Step 5 Click **Run Now** to immediately run the update inventory job, or click **Schedule** to schedule the periodic update inventory job at a later time.

Step 6 To check the status of your job, perform any one of the following :

- If you click **Run Now**, click the progress details in the progress window that appears.
- Click the **Discovery Jobs** button on the Inventory Management page.

Job Schedule - Field Descriptions

Table 20: Job Schedule - Field Descriptions

Field	Description
Start Time	Select Start Time to enter the start date and time in the *yyyy/MM/dd* and *hh:mm AM/PM* format, respectively. Alternatively, click the date picker to select the start date and time from the calendar. The displayed time is the client browser time. The scheduled periodic job runs at this specified time.
Recurrence	Select None, Hourly, Daily, Weekly, or Monthly to specify the job period.
Settings	Details of the job period.
End Time	If you do not want to specify an end date/time, click **No End Date/Time**. Click End at to enter the end date and time in the *yyyy/MM/dd* and *hh:mm AM/PM* format respectively.

Inventory Details Collection

Cisco Prime Collaboration Assurance supports on-demand inventory update for managed devices by collecting and updating data about the devices and the phones registered to them.

All additions, deletions, and modifications of phones, XML phones, and clusters are reflected in the inventory. There are separate inventory collection schedules for phones and clusters. For details on cluster discovery, see Cluster Data Discovery Settings.

You cannot create additional schedules; you can only edit an existing schedule. For phones, you can create multiple inventory collection schedules.

Note You can schedule periodic discovery of Cisco Unified CM clusters only. Phones registered with other clusters are not discovered. For more information, see Cluster Data Discovery Settings.

As Cisco Prime Collaboration Assurance performs inventory collection of phones and Cisco Unified CM clusters, these phones and clusters pass through various device states until they are fully recognized by Cisco Prime Collaboration Assurance (see Device States for details).

You can specify how often to collect information about the phones and clusters that are managed in Inventory Collection. To schedule Inventory Collection, choose **Assurance Administration**.

For Cisco Prime Collaboration Release 11.5 and later

To schedule Inventory Collection, choose **Alarm & Report Administration**.

For an overview of inventory collection tasks, see the following table.

Table 21: Overview of Inventory Collection Tasks

Task	Description
Schedule inventory collection of cluster devices	**For Cisco Prime Collaboration Release 12.1 and later** **Inventory** > **Cluster Device Discovery Schedule** to add, edit, or delete the cluster device discovery schedules (For more information, see Schedule Cluster Device Discovery)

Suspend and Resume Managed Devices

You can suspend a device that is in the Managed state. After the device is moved to the Suspended state, Cisco Prime Collaboration Assurance does not monitor this device. That is, conference, endpoint, and inventory details are not updated and alarms are not triggered for this device.

The following are behaviors for a device in the Suspended state:

- If a device is in the Suspended state, Cisco Prime Collaboration Assurance does not poll the devices.
- If a suspended endpoint joins a new conference, the endpoint is shown as Unknown in the Conference Topology pane.
- If a suspended endpoint is already in an in-progress conference, the endpoint icon (in the Conference Topology pane) changes to Unknown immediately after the endpoint state is changed to Suspended.

- If Cisco Unified CM publisher is suspended, Cisco Prime Collaboration Assurance does not poll the registered endpoints that belong to that corresponding Cisco Unified CM cluster.
- If there are any active alarms, they are not cleared immediately. You can either manually clear the alarms; otherwise, they are cleared automatically after they expire (by default, in 24 hours). No new alarms are triggered for a suspended device.
- You are not allowed to Suspend CUCM devices if any background job (like endpoint sync, phone XML, and so on) is running for the current cluster.
- **For Cisco Prime Collaboration Release 11.1 and earlier**

  If a suspended endpoint is already in a troubleshooting job, you cannot troubleshoot from the suspended endpoint. However, you can troubleshoot up to the suspended endpoint.
- If a device is suspended, the Endpoint Utilization report does not contain any data for this device.
- **For Cisco Prime Collaboration Release 12.1 SP2 and later**

  When the TC/CE endpoint management status changes from Managed to Suspend, it should Unsubscribe.

To suspend or resume managed devices:

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

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **Inventory Management**

Step 2 From the Current Inventory table, select managed or suspended devices.

Step 3 Click **Suspend** or **Resume**.

Step 4 In the confirmation message box, click **OK**.

Note You cannot delete phones directly from the inventory using the delete option. Phones are deleted automatically when the clusters with which they are registered are deleted. The inventory is updated only after a rediscovery is performed.

Delete Devices

You can delete devices that are in the Unknown, Unreachable, Inaccessible, Undiscoverable, Suspended, and Unsupported states. You cannot delete devices in the Managed state.

After a device is deleted, it is not listed in the Current Inventory table. , but the details are available in the Cisco Prime Collaboration Assurance server. To rediscover a deleted device, see Rediscover Devices. You can access the deleted device's details as part of the past conference data.

For Cisco Prime Collaboration Release 12.1 and later

You can delete devices that are in the Unknown, Unreachable, Inaccessible, Undiscoverable, Suspended, and Unsupported states. You cannot delete devices in the Managed state.

After a device is deleted, it is not listed in the Current Inventory table.

Endpoint with old IP entry must be deleted as part of DEVICE_REMOVED feedback and new IP entry (considered as a new endpoint on VCS) must be added separately.

For Cisco Prime Collaboration Release 12.1 SP2 and later

If the TC/CE endpoint is deleted from Inventory, the HTTPS feedback subscription will be removed from the endpoint.

The following are behaviors for a device in the Deleted state:

1. You are not allowed to Delete CUCM devices if any background job (like endpoint sync, phone XML, and so on) is running for the current cluster.
2. Cisco Prime Collaboration Assurance allows only 1 delete request at a time for all concurrent sessions. If you try deleting device(s)/endpoint(s) from other sessions, a message indicating that "Concurrent delete operation is running in background, please try after sometime" appears.
3. Cisco Prime Collaboration Assurance will not keep any device information once they are removed or deleted. There is no more DELETED state for device management status.

To delete a device:

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

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **Inventory Management**

Step 2 From the Current Inventory table, select devices to delete.

You can use the quick filter to get a list of devices in the desired state.

Step 3 Click **Delete**.

Step 4 In the confirmation message box, click **OK**.

Note You cannot delete phones directly from the inventory using the delete option. Phones are deleted automatically when the clusters with which they are registered are deleted. The inventory is updated only after a rediscovery is performed.

Troubleshooting

Issue: Unable to delete a device that is in Managed state.

Recommended Action: Ensure that you suspend the device first, and then delete the device.

Performance Graphs

Cisco Prime Collaboration Assurance enables you to select and examine changes in network performance metrics. You can select, display, and chart network performance data using real time, as well as collected data.

You can access the performance graphs through the Alarm & Events page, Device 360° view, and Diagnostic Summary pages. You can create performance graphs from the current or real-time data when:

- Voice utilization polling is enabled for devices.
- Device is in managed state.

Note You can view performance graphs for voice devices (excluding phones) only. These graphs appear only for devices in managed state and for which at least one polling cycle is over.

Performance Graphing Notes

This section contains information you should be aware of when working with performance graphs.

Summary	Explanation
Cisco recommends following these guidelines for optimal performance graph viewing.	The following guidelines are recommended: • No more than five metrics be selected for one graph. • No more than ten graphs on the user interface. • No more than ten items selected for merge.
An MGCP gateway on a Catalyst 6000 switch. When you have all three capabilities (voice gateway, switch, and MGCP) performance graphing cannot graph all the data. Only the common metrics are available for graphing.	When graphing performance metrics for a device that has these three capabilities (voice gateway, switch, and MGCP) you will only be able to graph the common metrics. In the Event Details page you cannot graph HighUtilization events.
A voice gateway, MGCP, and H323 on a router. When you have all these capabilities on one device, each metric displays two graphs.	When graphing performance metrics for a device that has these capabilities (voice gateway, MGCP, H323, and router), each metric displays two graphs. Also, when graphing multiple devices or devices that have multiple polling intervals, the least common multiple is used to plot the x axis. Real-time graphs will refresh at this common polling interval.
Cisco Unity Express servers (CUES) graph real-time data and update in real-time. You can switch from line to bar charts and zoom in on specific data to troubleshoot and find peak utilization periods.	Ensure Cisco Prime Collaboration Assurance is collecting data and is configured properly to receive this data.

Launch a Performance Graph

The performance graphs are available through the following:

- Device 360 degree View - Click on the Launch Tools icon, and then click on Performance Graph.
- Event Details page
- Diagnostics views - UCM Cluster Call Usage Summary in Server and Cluster views, UCM Resource Utilization Summary and UCM Cluster Location Summary in Cluster view, and trunk utilization can be accessed through the UCM Resource Utilization Summary portlet. in the Cluster view.

Before you Begin

- Verify that Cisco Prime Collaboration Assurance is monitoring the devices for which you want to collect utilization statistics. This includes the Cisco Unified Communications Manager that the ports are registered to.
- Verify that voice utilization polling settings are enabled. Cisco Prime Collaboration Assurance uses the statistics gathered during voice utilization polling for charting network performance.
- Review the Performance Graphing Notes.

Performance Graph Window

Performance graphs provide real-time information and historical information.

When you launch a performance graph, one line graph is displayed for each metric that you select. Each line graph contains 16 data points displayed in real time. The following table provides details on the data options.

Graph Data Option	Description
Real Time	When you launch a performance graph, it shows real time data by default.
Hourly Average	When you select Hourly Average, the performance graph shows average data for the hour.
Hourly Max	When you select Hourly Max, the performance graph shows peak data for the hour.
Hourly Min	When you select Hourly Min, the performance graph shows minimum data for the hour.
History	When you select History, the performance graph shows hourly average data for seven days.
All	Displays all data. Graphs display up to a maximum of 130 points. If data ranges in the Zoom/Pan view contain more than 130 points, then Cisco Prime Collaboration Assurance selects points at regular intervals and plots them in the graph.

Troubleshooting Performance Graphs

This section contains information that will help you if you encounter problems generating performance graphs. If you encounter an error, it will likely appear either when you select Performance Graphing from the menu, or when Cisco Prime Collaboration Assurance is checking for the data file to graph. In the first case (when selecting Performance Graphing), you will see an error message that describes the problem and an action to take. The following table describes the errors and their possible causes, for both of these types of cases.

Error	Possible Causes

Cannot collect data	• Account and credentials are not the same on all Cisco Unified Communications Managers in the cluster.
	• HTTP server problems:
	  • HTTP server on the device is down.
	  • HTTP server is operational, but the Cisco Unified Communications Manager is down.
	• Device unreachable because of a network problem.
	• **For Cisco Prime Collaboration Release 11.1 and earlier**
	  Performance Monitor process on the media server is down.
	• The Cisco Unified Communications Manager that the MGCP gateway is registered to, is not in Cisco Prime Collaboration Assurance Inventory.
	• Device capability is not supported. Performance graphing supports the following: Cisco Unity, Cisco Unity Express, Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, H.323 devices, and Voice Mail Gateways.
	• Device is suspended or deleted.
	• Device platform is not support.
	For a list of supported devices, see Supported Devices for Cisco Prime Collaboration Assurance.

Cannot collect data because of the following: • The username or password for the device is empty. • The system has the wrong credentials for the device. • The device does not have credential information.	• No credentials in Cisco Prime Collaboration Assurance. • Incorrect credentials in Cisco Prime Collaboration Assurance. To add credentials, see **Adding a Device Credential Profile.** .

Error	Possible Causes
Cannot collect data from the device because of the following: • A processing error occurred. • Parsing or processing errors occurred. • Internal initialization errors occurred. • Initialization problems occurred in the device data collector.	Incorrect Cisco Unified Communications Manager version. Check the following: • The version of the Cisco Unified Communications Manager that is running on the device. • The Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance. • If the Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance is incorrect, add the device again. For a list of supported devices, see Supported Devices for Cisco Prime Collaboration Assurance.
Cannot collect data from the device. The certificate hostname/IP Address cannot be mapped to the URL hostname/IP Address.	The device is not in DNS.
Incomplete data collected because an error occurred in communicating with the device.	Incorrect Cisco Unified Communications Manager version. Check the following: • The version of the Cisco Unified Communications Manager that is running on the device. • The Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance. • If the Cisco Unified Communications Manager version number that is stored in Cisco Prime Collaboration Assurance is incorrect, add the device again. For a list of supported devices, see Supported Devices for Cisco Prime Collaboration Assurance.
Cannot collect data because of the following: • The device returned no data from a required MIB. • The device received no MIB data.	• No data from a required MIB. • A required MIB is not populated on the device. • No MIBs returned data. • Device is unreachable due to a network problem. • Device credentials do not contain a valid SNMP community read string. • SNMP response slow; data collection timed out.
• The rate of queries on the Cisco Unified Communications Manager exceeds the limit. • An error has occurred in the data processing stage.	Too many queries on a Cisco Unified CM 6.0 or later. Check the polling settings; they should not be less than three minutes.

Error	Possible Causes
• The Cisco Unified Communications Manager did not have enough time to handle the query requests. • An error has occurred in the data processing stage.	Query exceeded time limit on Cisco Unified CM 6.0 or later.
Cisco Unity or Unity Express trunk utilization graphs are not working.	Cisco Prime Collaboration Assurance must be configured properly using the maximum capacity.

When working with performance graphs, remember the following:

- If you are not able to collect performance data and you do not see an error message (either a popup message or a message in the log file) indicating the problem, you should verify the status of the device. To do so, use the View/Rediscover/Delete Devices page. If the device is in the Unreachable state, verify that the device's credentials are correct and rediscover the device.
- If a gray line or a gray area appears in a graph, hover your mouse over it to obtain a tool tip with an explanation.

Unified CM Device Search

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

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

For Cisco Prime Collaboration Release 11.5 and later

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

Note The table displays only 200 entries. Therefore, we recommend that you use the filter criteria to the best use to ensure that you get the desired result.

To create a new search criteria:

Step 1 **For Cisco Prime Collaboration Release 11.5 and later**

Choose **Inventory** > **UC Device Search**.

Step 2 Select the Cluster from **Cluster** drop-down list.

You can also search for a device in the Cluster drop-down list.

Step 3 Click **New Search**.

Step 4 Enter the Criteria Name, Device Type, and Polling Interval

If you choose the devices only configured in the DB option, you cannot specify the polling interval or the other parameters, except the device type. This option displays the devices in the Unknown state.

The same user cannot use the same search criteria name for the same cluster. The same user can have the criteria name for a different cluster.

Step 5 For Custom Search, specify the status within call Manager, Device Model, and the Search with Name parameters.

The search criteria available vary based on the device type you chose.

Step 6 Click **Search**.

The search results are displayed in the page. The results get refreshed based on the polling interval you specify. You can launch the Unified CM from the IP address link available in the IP Address column.

The search results also provides the following information:

- App Info— The information about the application.
- Configuration— This applies to H.323 Gateways.
- Port/Channel Status— Shows all the configured port or channels and their status. You can set the polling interval to refresh this view.

This search does not get saved in the database and cannot be retrieved after you log out, unless you save the search. To save the search, click the **Save** icon.

You can also edit a search that you had saved. You can delete a search that you had created, even if it is unsaved. Use the edit or delete icon to edit/delete the search. Fields that you cannot edit are disabled.

You can also view the destination status for SIP trunks. Select **SIP Trunk** from the Device Type drop-down list, enter the Criteria Name, Polling Interval and click **Search**. Hover your mouse over the **Name** column and click the quick view icon to launch the Destination Details pop-up window.

Note If you want to save the search criteria in Internet Explorer 10 or 11, you must enable Always Refresh from Server option in the browser. To enable this option, press the F12. In the Internet Explorer tool bar menu, choose **Cache > Always refresh from server**.

SNMP Query

The SNMP query feature helps you to troubleshoot devices in your network.

You should perform SNMP query when:

- Devices in your network do not get into a managed state in Cisco Prime Collaboration Assurance.
- Devices in your network are not listed in Inventory Management.
- SNMP Polling is not happening successfully.

Prerequisite - Devices should be supported by Cisco Prime Collaboration Assurance.

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

To perform SNMP query:

1. Choose **Device Inventory** > **SNMP MIB Query Tool**.

   For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **SNMP MIB Query Tool**.

2. Enter the IP Address, select and OID type from the OID drop-down list, and then do one of the following:
   - Click the GET button - To know the return value of a particular OID. For example to know the Interface Name or Interface Status.

     Credentials are required to perform this task. If the device information is available in the Cisco Prime Collaboration database, the details are auto-populated on the screen. Otherwise, check the Enter the Credentials check box, select an SNMP version from the version drop-down list, and enter the details on the fields that appear.
   - Click the Walk button - To get detailed information on the MIB of that device.

     Credentials are required to perform this task. If the device information is available in the Cisco Prime Collaboration database, the details are auto-populated on the screen. Otherwise, check the Enter the Credentials check box, select an SNMP version from the version drop-down list, and enter the details on the fields that appear.

   The information about the IOD appears as a table on the page.

Troubleshooting - SNMP credentials are not auto populated when:

- Discovery is not completed so credentials may not have been added in the Cisco Prime Collaboration database yet.
- If device is in Unknown or Inaccessible state in Inventory Management.
- SNMP Credentials have not been configured on the device.