Discover Devices

This section explains the following:

- Discover Devices, on page 1

Discover Devices

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

Discovery Life Cycle

Discovery involves three phases:

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

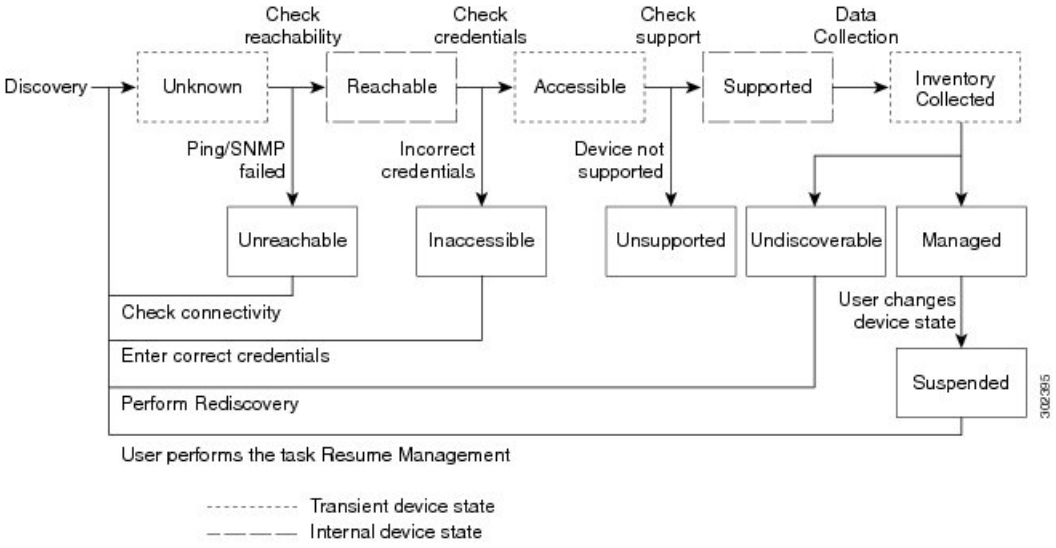
For Cisco Prime Collaboration Release 11.1 and earlier

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

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

The following diagram shows the device discovery lifecycle.

Figure 1: Device Discovery Lifecycle



Cisco Prime Collaboration Assurance displays the following device states:

Table 1: Discovery States

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

Discovery States	Description
Inventory Collected	Cisco Prime Collaboration Assurance is able to collect the required data using the mandated data collectors. This is part of the inventory discovery, which is an intermediate (transient) state during device discovery.
Undiscoverable	Cisco Prime Collaboration Assurance is not able to collect the required data using the mandated data collectors. The device state can be undiscoverable when: • Connectivity issues can be caused by SNMP or HTTP/HTTPS timeout. Also, if you use HTTP/HTTPS to collect data, only one HTTP/HTTPS user can log in at a time. If Cisco Prime Collaboration Assurance faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery. • There is no mandated data collection for Cisco Unified CM, CTS, CTMS, and other network devices. • Connectivity issues can be caused by SNMP or HTTP/HTTPS timeout. Also, if you use HTTP/HTTPS to collect data, only one HTTP/HTTPS user can log in at a time. If Cisco Prime Collaboration Assurance faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery.
Managed	Cisco Prime Collaboration Assurance has successfully imported the required device data to the inventory database. All conference, endpoints, and inventory data are available for devices in this state. **For Cisco Prime Collaboration Release 11.1 and earlier** You can troubleshoot a device only if it is in this state. **Note** Cisco Prime Collaboration Assurance supports third-party devices whose manageability depends on MIB-II support. If the Cisco Prime Collaboration Assurance inventory exceeds your device limit, you will see a warning message. For information on how many devices Cisco Prime Collaboration Assurance can manage, see the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide.

Discovery States	Description
Partially Managed	Devices which are in managed state but have some credentials missing. These credentials are not mandatory for managing inventory, but required for all other features, such as conference monitoring to work. You can click on the corresponding number to cross launch to see a list of all devices in the inventory table which are managed but with insufficient credentials. This count is updated only when you perform rediscovery after adding the credentials. **For Cisco Prime Collaboration 12.1 SP4 and later** **Note** When Cisco Prime Collaboration Assurance is in MSP mode, and NAT environment, mention the public IP of Assurance in `/opt/emms/emsam/conf/mspconfig.properties` file. Steps to update mspconfig.properties file: 1. Login to Assurance CLI using root user. 2. Edit `/opt/emms/emsam/conf/mspconfig.properties` file. 3. Add the Assurance public IP address at the end of the file. `PCA_PUBLIC_IP=<PCA public IP>`
Suspended	User has suspended monitoring of the device. Conference and endpoint data are not displayed for devices in this state. Periodic polling is also not performed for devices in this state. You cannot update inventory for these devices. To do so, you will need to perform Resume Management.

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

Related Topics

- Manage Device Credentials
- Add a Device Credentials Profile
- Credential Profiles Field Descriptions
- Suspend and Resume Managed Devices

Removal of Devices from Cisco Prime Collaboration Assurance on Deletion

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

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

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

Discovery Methods

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

For Cisco Prime Collaboration Release 11.1 and earlier

Discovery Type	Discovery Method	Description

Auto discovery	Logical Discovery	• Discovers management applications, conferencing devices, and call processors such as Cisco TMS, Cisco VCS, and Cisco Unified CM.
		• All endpoints and infrastructure devices registered with , Cisco TMS, Cisco Unified CM, and Cisco VCS are discovered automatically during logical discovery.
		  • For Cisco C and Ex series TelePresence systems, Cisco Prime Collaboration Assurance does not discover the first hop router and switch.
		  • Logical discovery of Cisco TMS discovers VCS, codec, Cisco MCU, TPS, Cisco IP Video Phone E20, and Cisco MXP Series.
		• Logical discovery of the Cisco Unified CM publisher discovers other Cisco Unified CMs (subscribers) in the network, Cisco Unity, Cisco MGCP Voice Gateways, H.323 Voice Gateways, Gatekeepers, CTI applications.
		• Cisco Unified CM logical discovery for SIP devices includes the discovery of Conductor. The SIP configured conductor IP is not SNMP enabled, so it is not managed in Cisco Prime Collaboration Assurance. In such configuration, Conductor with admin IP must be managed first, before performing the logical discovery of Cisco Unified CM.
		• Endpoints and infrastructure devices that are not registered with any of the management applications, conferencing devices, or call processors cannot be discovered using logical discovery. Use ping sweep or direct discovery to discover these devices.
		• Cisco CTX cluster is discovered using logical discovery.
		• Unified Contact Center devices are discovered using logical discovery.
		• Logical Discovery rediscovers the deleted devices, if they are logically associated to seed devices or clusters.

Auto discovery	CDP	• Discovers devices independently of media and protocol used. This protocol runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. • This discovery method queries the CDP Neighbor Table to find neighboring devices. When CDP is enabled, discovery queries the CDP cache on each seed device (and its peers) via SNMP. After CDP discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by CDP discovery, then all endpoints and infrastructure devices registered with it are also discovered. • CDP must be enabled on the devices to perform CDP discovery. • There is no limit on the number of seed devices that can be used for CDP discovery. However, for a large network, it is advised to perform this on limited chunks of seed devices rather than all at once.

Discovery Type	Discovery Method	Description
Auto discovery	Ping Sweep	• Discovers devices within a range of IP addresses from a specified combination of IP address and subnet mask. • This method pings each IP address in the range to check the reachability of devices. If a device is reachable, you must specify a list of subnets and network masks to be pinged. After ping sweep discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by ping sweep discovery, then all endpoints and infrastructure devices registered with it are also discovered. • If no call processors are deployed, or if no devices are registered to call processors, use ping sweep discovery. This method discovers all new infrastructure devices, new network devices, and new locations of devices in the target network. You must provide a list of subnet and network masks of the target network. During a scheduled ping sweep discovery, all devices in the network are identified and matched with their credential profiles. If a new device is discovered, it is added to the inventory. • Ping Sweep discovery does not require seed devices. Instead, you must specify a list of subnets and network masks to be pinged. • Ping Sweep discovery may take longer than usual to discover devices if the IP ranges are large. • You must create an “Any” credential profile for ping sweep and CDP discovery. • Ping Sweep does not work for devices with IPv6 addresses.
-	Add Devices	• Discovers the device directly using the IP address. • Discovers individual devices in your network. • If the discovery of a device fails because of incorrect credentials during a scheduled discovery, then you can discover the failed device alone using the direct discovery method. • SIP devices and Presence server cannot be discovered using logical discovery. You must add these devices manually, or perform direct discovery. • To discover the seed or publisher devices without discovering the network devices or video endpoints registered to them. • To discover infrastructure devices, which have not been discovered after a fresh installation. • For MSP mode - To discover a single device without auto discovery of network devices.

Discovery Type	Discovery Method	Description
-	Import	Use this option to add: • Devices in bulk. • A subset of devices, within a subnet, from a larger group.

Note

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

For Cisco Prime Collaboration Release 11.5 and later

Discovery Type	Discover	Description
Auto discovery	Communications Manager (UCM) Cluster and connected devices	• Performs logical discovery of Cisco Unified CM by using the **Inventory** > **Inventory Management** > **Auto Discovery** path. • All endpoints and infrastructure devices registered with Cisco Unified CM are discovered automatically during the discovery. • Endpoints and infrastructure devices that are not registered with any call processors cannot be discovered using logical discovery. Use ping sweep or direct discovery to discover these devices. • Communications Manager and its connected devices discovery rediscovers the deleted devices, if they are associated to seed devices or clusters. • Logical discovery of the Cisco Unified CM publisher discovers other Cisco Unified CMs (subscribers) in the network, Cisco MGCP Voice Gateways, H.323 Voice Gateways, Gatekeepers, CTI applications. • Cisco Unified CM logical discovery for SIP devices includes the discovery of Conductor. The SIP configured conductor IP is not SNMP enabled, so it is not managed in Cisco Prime Collaboration Assurance. In such configuration, Conductor with administrator IP must be managed first, before performing the logical discovery of Cisco Unified CM. • During CUCM logical discovery (Communications Manager Publisher) no SIP trunks are discovered. • In the MSP mode, if you are changing the customer name for publisher then update all other Infrastructure devices under that cluster with the new customer name. • When you autodiscover Unified Communications Manager (**Inventory** > **Inventory Management** > **Auto Discovery**), you can choose to add Cisco Prime Collaboration Assurance server as a CDR billing application server and syslog receiver in Unified Communications Manager servers by using the **Auto-Configuration** option.
	Video Communications Server (VCS) / Expressway Cluster and connected devices	Performs logical discovery of Video Communications Server (VCS) or Expressway Cluster and connected devices.
	Telepresence Management Suite (TMS) and connected devices	Performs logical discovery of Telepresence Management Suite (TMS) and connected devices. Logical discovery of Cisco TMS discovers , Cisco MCU, TPS, and TP conductor.

Discovery Type	Discover	Description
	Contact Center Customer Voice Portal (CVP) and connected devices	Performs logical discovery of Contact Center Customer Voice Portal (CVP) and connected devices.
	VCenter and connected ESXi devices	Performs logical discovery of VCenter and connected ESXi devices. For Cisco C and EX Series TelePresence systems, Cisco Prime Collaboration Assurance does not discover the first hop router and switch.
	UCS Manager	Performs logical discovery of UCS Manager.
Auto discovery	Network devices using CDP	• Discovers devices independently of media and protocol used. This protocol runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. • This discovery method queries the CDP Neighbor Table to find neighboring devices. When CDP is enabled, discovery queries the CDP cache on each seed device (and its peers) by using SNMP. After CDP discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by CDP discovery, then all endpoints and infrastructure devices registered with it are also discovered. • CDP must be enabled on the devices to perform CDP discovery. • There is no limit on the number of seed devices that can be used for CDP discovery. However, for a large network, it is advised to perform this on limited chunks of seed devices rather than all at once.

Discovery Type	Discover	Description
Auto discovery	Network devices using Ping	• Discovers devices within a range of IP addresses from a specified combination of IP address and subnet mask. • This method pings each IP address in the range to check the availability of devices. If a device is reachable, you must specify a list of subnets and network masks to be pinged. After ping sweep discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by ping sweep discovery, then all endpoints and infrastructure devices registered with it are also discovered. • If no call processors are deployed, or if no devices are registered to call processors, use ping sweep discovery. This method discovers all new infrastructure devices, new network devices, and new locations of devices in the target network. You must provide a list of subnet and network masks of the target network. During a scheduled ping sweep discovery, all devices in the network are identified and matched with their credential profiles. If a new device is discovered, it is added to the inventory. • Ping Sweep discovery does not require seed devices. Instead, you must specify a list of subnets and network masks to be pinged. • Ping Sweep discovery may take longer than usual to discover devices if the IP ranges are large. • You must create an “Any” credential profile for ping sweep and CDP discovery. • Ping Sweep does not work for devices with IPv6 addresses.
Auto discovery	Any Device	Discovers any other seed devices such as conductors.

Discovery Type	Discover	Description
-	Add Devices	• Discovers the device directly using the IP address. • Discovers individual devices in your network. • If the discovery of a device fails because of incorrect credentials during a scheduled discovery, then you can discover the failed device alone using the direct discovery method. • SIP devices and Presence server cannot be discovered using logical discovery. You must add these devices manually, or perform direct discovery. • To discover the seed or publisher devices without discovering the network devices or video endpoints registered to them. • To discover infrastructure devices, which have not been discovered after a fresh installation. • For MSP mode - To discover a single device without auto discovery of network devices.
-	Import	Use this option to add: • Devices in bulk. • A subset of devices, within a subnet, from a larger group.

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

Prerequisites and Recommendations

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

All devices

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

- You can discover the devices, such as endpoints, TelePresence server, and so on individually, except for IP Phones/Software Clients. These endpoints are discovered only with the discovery of the call processor with which they are registered.
- You must ensure that the device credentials that you have entered are correct. During the discovery process, based on the device that you want to discover, Cisco Prime Collaboration Assurance connects to the device using CLI, HTTP/HTTPS, or SNMP.
- When you add devices, the HTTP (and HTTPS) port numbers are optional. These settings are automatically detected.
- If you have both voice and video endpoints deployed in your network, do not discover all clusters in your network at the same time, as discovery could take a long time.
- Firewall devices are not supported.
- If HTTP is used to retrieve device details, disable the HTTP firewall.
- HSRP-enabled devices are not supported.
- When you add devices that have multiple interfaces and HTTP administrative access, you must manage the devices in Cisco Prime Collaboration Assurance using the same interface on which you have enabled HTTP administrative access.
- After discovering devices, if the IP address changes for network devices and infrastructure devices (such as CTMS, Cisco Unified CM, Cisco MCU, Cisco VCS, Cisco TS, and so on), you must rediscover these devices by providing the new IP address or hostname. See Rediscover Devices, on page 33 for information on rediscovering devices.
- If a managed device is removed from the network, it will continue to be in the Managed state until the next inventory collection occurs, even though the device is unreachable. If a device is unreachable, an Unreachable event for this device appears.
- Configuration changes on a device are discovered by Cisco Prime Collaboration Assurance only during the inventory collection process. Therefore, any changes to a device's configuration will not be shown by Cisco Prime Collaboration Assurance until the next inventory collection after the configuration change.
- To periodically update inventory, and synchronize the inventory with the Cisco Prime Collaboration Assurance database, you must perform inventory update. For more information, see Update and Collect Inventory Details.

Cisco Unified CM

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

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

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

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

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

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

- The JTAPI credential is optional for Cisco Unified CM clusters. However, the SNMP and HTTP credentials are mandatory for Cisco Unified CM publishers and subscribers.
- After discovering Cisco Unified CM, if you have registered any new endpoints, you must rediscover Unified CM Publisher node to add them to Cisco Prime Collaboration Assurance. See Rediscover Devices, on page 33 for information on rediscovering devices.

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

For Cisco Prime Collaboration Release 11.5 and earlier

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

Cisco Unified CM Express and Cisco Unity Express

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

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

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

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

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

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

Cisco VCS and Cisco VCS Expressway

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

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

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

For Cisco Prime Collaboration Release 11.1 and earlier

CTS-Manager

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

For Cisco Prime Collaboration Release 11.1 and earlier

CTX Cluster

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

Cisco TelePresence Conductor

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

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

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

Media Server

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

Mobile and Remote Access (MRA) Clients

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

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

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

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

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

Cisco Unified Contact Center Express (Unified CCX)

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

- Setting Up Devices for Cisco Prime Collaboration Assurance
- Configure Devices for Cisco Prime Collaboration Assurance

Cisco SocialMiner

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

- Setting Up Devices for Cisco Prime Collaboration Assurance
- Configure Devices for Cisco Prime Collaboration Assurance

Cisco Integrated Management Controller (CIMC)

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

  The system cannot auto-discover a CIMC device. You must manually add the device by using the **Add Device** button under **Inventory** > **Inventory Management**.

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

For Cisco Prime Collaboration Release 11.5 and later

Cisco Unified Attendant Console

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

For Cisco Prime Collaboration Release 11.6 and later

ciscoDX70 and ciscoDX80 with CE image

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

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

Automatic Discovery of Devices

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

Note

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

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

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

For Cisco Prime Collaboration Release 12.1 SP2 and later

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

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

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

To auto discover devices:

Before you begin

You must review the following sections before performing auto discovery:

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

Procedure

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

For Cisco Prime Collaboration Release 11.1 and earlier

Choose **Device Inventory** > **Inventory Management**.

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

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

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

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

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

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

Example:

- For Logical Discovery, Cisco Discovery Protocol and Direct Discovery, you can enter multiple IP addresses or hostnames using one of the supported delimiters: comma, colon, pipe, or blank space.
- **For Cisco Prime Collaboration Release 11.5 and later**

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

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

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

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

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

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

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

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

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

Troubleshooting

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

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

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

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

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

Recommended Action:

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

Discovery Filters and Scheduling Options

Discovery Filters

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

Table 2: Discovery Filters

Filter	Description
IP Address	Comma-separated IP addresses or IP address ranges for included or excluded devices. For the octet range 1-255, use an asterisk (*) wildcard, or constrain using [xxx-yyy] notation; for example: • To include all devices in the 172.20.57/24 subnet, enter an include filter of 172.20.57.*. • To exclude devices in the IP address range of 172.20.57.224 to 172.20.57.255, enter an exclude filter of 172.20.57.[224-255]. You can use both wildcard types in the same range; for example, 172.20.[55-57].*. If both include and exclude filters are specified, the exclude filter is applied before the include filter. After a filter is applied to an auto-discovered device, no other filter criterion is applied to the device. If a device has multiple IP addresses, the device is processed for auto-discovery as long as it has one IP address that satisfies the include filter.
Advanced Filters	

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

Schedule Options

The following table describes the scheduling options that are available

Table 3: Schedule Options

Field	Descriptions
Start Time	Click Start Time to enter the start date and time in the yyyy/MM/dd and hh:mm AM/PM formats, respectively. Click the date picker if you want to select the start date and time from the calendar. The time displayed is the client browser time. The scheduled periodic job runs at this specified time.
Recurrence	Click None, Hourly, Daily, Weekly, or Monthly to specify the job period.
Settings	Specify the details of the job period.

Field	Descriptions
End Time	If you do not want to specify an end date/time, click No End Date/Time. Click Every number of Times to set the number of times you want the job to end in the specified period. Enter the end date and time in the yyyy/MM/dd and hh:mm AM/PM formats, respectively.

Manual Discovery of Devices

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

To add a new device and perform discovery:

Before you begin

You must review the following sections before adding devices:

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

Procedure

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

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

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

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

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

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

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

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

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

For Cisco Prime Collaboration Release 11.5 and later

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

Import Devices

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

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

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

- Hostname
- IP address
- Protocol credentials

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

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

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

To import a device from a file:

Before you begin

You must review the following sections before importing devices:

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

Procedure

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

For Cisco Prime Collaboration Release 11.5 and later

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

Step 2 Click **Import**.

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

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

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

Step 4 Click **Import**.

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

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

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

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

Export Device Lists and Credentials

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

To export device list and credentials:

Procedure

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

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

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

Troubleshooting

1. **Issue**: Devices are not getting discovered while trying to import the device credential from one server to other.

   Recommendation: You can import the exported device credentials file on the same server only.

2. **Issue**: Devices are not getting discovered while trying to use the exported credential from the previous release to import in current release.

   Recommendation: You can import the exported device credentials file on the same server only.

Discovery of Cisco Unified Computing System (UCS)

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

Before you begin

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

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

- VMware Tools must be installed on the VMs before performing the discovery. This ensures the tools are discovered during the VMware ESX server discovery.
- In a NAT deployment, the VM name in the managed ESX server must be same as the private host name of the VM in Cisco Prime Collaboration Assurance.
- Check the Event and Alarm correlation rules with UCS blades by configuring vCenter. See Configure vCenter, on page 30 for more information.
- Enable and configure SNMP on Cisco UCS Manager to create the relationship between the SNMP manager and the SNMP agent:
  1. In Cisco UCS Manager, navigate to the **Admin** tab and expand it to select the **Communication Services** tab.
  2. Configure the fields in the SNMP window and save the changes.

Procedure

Step 1 Login to Cisco Prime Collaboration Assurance server and navigate to **Device Inventory** > **Inventory Management**.

For Cisco Prime Collaboration Release 11.5 and later

Login to Cisco Prime Collaboration Assurance server and navigate to **Inventory > Inventory Management**.

Step 2 Click the **Manage Credentials** button to create credential profiles for VMware ESX Server (ESX), Cisco UCS Manager (UCS Manager), and VMware vCenter Server (vCenter).

Note

- You must configure SNMP credentials on the VMware ESX Server. For more information on setting up devices and configure devices for Cisco Prime Collaboration Assurance, see the list at the following locations:
  - Setting Up Devices for Cisco Prime Collaboration Assurance
  - Configure Devices for Cisco Prime Collaboration Assurance
- The HTTP credentials for the VMware ESX Server credential profile must be same as the VMware ESX Server device login credentials.
- In a clustered scenario, the HTTP credentials for the Cisco UCS Manager credential profile must be the same as the primary Fabric Interconnect device login credentials.
- In a standalone scenario, the HTTP credentials for the Cisco UCS Manager credential profile must be the same as the Fabric Interconnect device login credentials.
- The HTTP credentials for the vCenter credential profile must be same as the vCenter device admin login credentials.
- The virtual machines are supported both in a NAT and non-NAT deployment.

Step 3 Perform logical discovery of the following:

- **ESX Logical Discovery** - Use the ESX Server IP address as the seed device to discover all the VMs running on it.
- **UCS Manager Logical Discovery** - In a clustered scenario, use the virtual IP address of the Cisco UCS Manager as the seed IP address for logical discovery. This discovers the UCS Chassis managed by the UCS Manager, and also associates the managed ESX Server to the right UCS Chassis. In a standalone scenario, use the IP address of Fabric Interconnect device as the seed IP address for Logical Discovery.
- **vCenter Logical Discovery** - Use the vCenter IP address as the seed device to discover the vCenter and the ESX servers managed in the vCenter server.

Note

- The VM name in the managed ESX server must be same as the private host name of the VM in Cisco Prime Collaboration Assurance to ensure proper grouping of the VMs.
- Logical Discovery is not supported in MSP deployment.

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

a. For Cisco Prime Collaboration Release 11.1 and earlier

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

b. For Cisco Prime Collaboration Release 11.1 and earlier

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

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

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

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

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

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

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

Configure vCenter

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

Procedure

Step 1 **Configure SNMP in vCenter**

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

Step 2 **Configure the triggers and alarms in vCenter**

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

Unified CM Cluster Data Discovery

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

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

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

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

Note

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

Schedule Cluster Device Discovery

Before you begin

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

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

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

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

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

  - Setting Up Devices for Cisco Prime Collaboration Assurance
  - Configure Devices for Cisco Prime Collaboration Assurance

Procedure

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

For Cisco Prime Collaboration Release 11.5 and later

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

For Cisco Prime Collaboration Release 12.1 and later

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

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

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

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

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

Related Topics

Setting Up Devices for Cisco Prime Collaboration Assurance

Rediscover Devices

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

For Cisco Prime Collaboration Release 12.1 SP2 and later

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

Perform rediscovery when:

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

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

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

For Cisco Prime Collaboration Release 11.1 and earlier

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

For Cisco Prime Collaboration Release 11.5 and later

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

Note Accessibility information is not checked during rediscovery.

The workflow for rediscovery is the same as for discovery. See Discovery Life Cycle for details.

Verify Discovery Status

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

To verify discovery status:

Procedure

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

For Cisco Prime Collaboration Release 11.5 and later

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

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

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

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

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

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

Troubleshooting

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

   Recommended Action: You must discover the Cisco VCS Core and Cisco VCS Edge before discovering the Cisco Unified Communications Manager. This ensures that all the IP addresses of Cisco VCS - Edge external and internal interfaces are known in the Cisco Prime Collaboration Assurance inventory. When the Cisco Unified Communications Manager publisher is discovered, the interface IP address is matched with the collected inventory and does not cause unreachable alarms.

2. **Issue**: Cisco TelePresence Management Suite (TMS) - The associated devices are not discovered.

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

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

3. **Issue**: Cisco TelePresence Touch Panels are not capable of sending syslog event without being directly connected to a Codec Endpoint.

   Recommended Action: Ensure that the Cisco TelePresence Touch Panels are connected to the Codec and the Codec is rediscovered in Cisco Prime Collaboration Assurance.

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

   Recommended Action: DX80 and other phones are only discovered as part of Phone Sync, CDT, or Cisco Unified Communications Manager publisher cluster discovery. Other than Registration/Un-Registration status, any configuration change in phones is updated in the Cisco Prime Collaboration Assurance inventory only after the Cluster Data Discovery.

   You should not discover the DX80 device separately by adding DX IP address.

5. **For Cisco Prime Collaboration Release 11.6 and later**

   Issue: CiscoDX80/DX70 devices with CE image are not discovered successfully.

   Recommended Action: Ensure that the CiscoDX80/DX70 devices are present in Cisco Unified Communications Manager.

   For more information, see Configure Devices for Cisco Prime Collaboration Assurance.

6. **For Cisco Prime Collaboration Release 11.6 and later**

   Issue: CiscoDX80/DX70 devices with CE image are discovered successfully and it is in Inaccessible state.

   Recommended Action: Add credential profile for CiscoDX80/DX70 devices and also verify that Cisco Prime Collaboration Assurance can ping the device from the Device360 view ping option.

   For more information, see Configure Devices for Cisco Prime Collaboration Assurance.

7. **For Cisco Prime Collaboration Release 11.6 and later**

   Issue: CiscoDX80/DX70 devices with CE image are in the Unsupported state.

   Recommended Action: Ensure Cisco Prime Collaboration Assurance is above the 11.6 version, if it is below 11.6 version then CiscoDX80/DX70 devices with CE image is not supported.

For more information, see Configure Devices for Cisco Prime Collaboration Assurance.

8. **For Cisco Prime Collaboration Release 11.6 and later**

   Issue: CiscoDX80/DX70 devices with CE image are not displaying in Conference Diagnostics page.

   Recommended Action: Ensure that proper JTAPI credentials are added for the managed Unified CM where these phones are registered.

   For more information, see Configure Devices for Cisco Prime Collaboration Assurance.

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

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

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

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

    - Setting Up Devices for Cisco Prime Collaboration Assurance
    - Configure Devices for Cisco Prime Collaboration Assurance

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

    Recommended Action: Check the following:

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

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

    Recommended Action: Check that the following conditions are met:

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

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

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

    Recommended Action: Check that the following conditions are met:

    - Ensure that the Cisco Finesse device is up and running and is in Managed state on the **Inventory Management** page.

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

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