Discover Devices

Discover Devices

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

Discovery Life Cycle

Discovery involves three phases:

- Access-level discovery—Cisco Prime Collaboration does the following:

1. Checks whether the device can be pinged using ICMP. If ICMP is not enabled on the device, the device is moved to the Unreachable state. See Rediscover Devices for information on how to disable ICMP verification.
2. Gets all the defined credential profiles, based on the IP address. See Manage Device Credentials to understand how to define the credential profiles.
3. Checks whether the SNMP credentials match.

4 Identifies the device types.

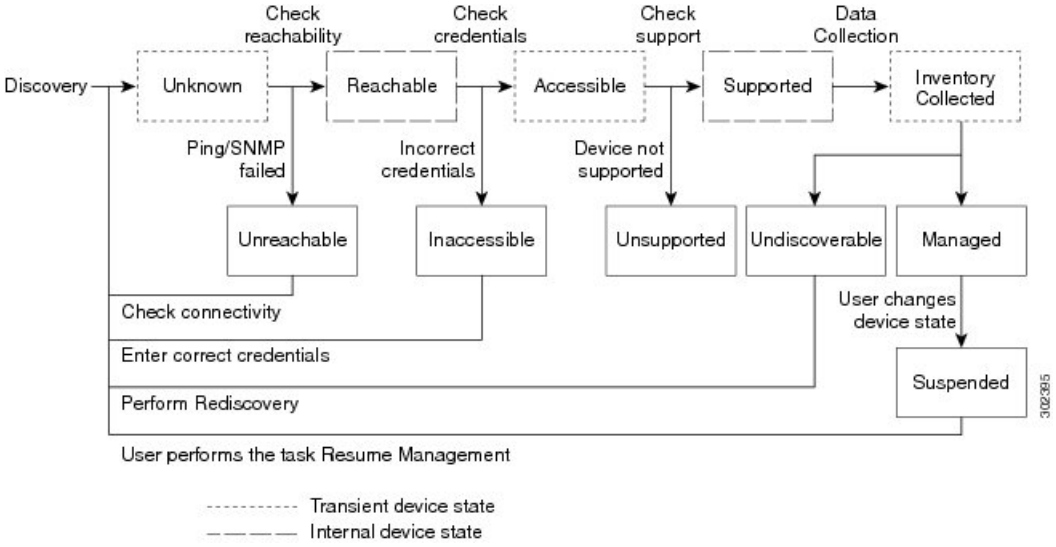
5 Verifies all other mandatory device credentials, based on the device type. If the mandatory credentials are not defined, discovery fails. See Manage Device Credentials for information on required device credentials.

- Inventory discovery—Cisco Prime Collaboration 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.
- Path trace discovery—Cisco Prime Collaboration verifies whether CDP is enabled on the device and discovers the topology, based on CDP. The links between the devices are computed using CDP and they are persisted in the Cisco Prime Collaboration database.

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

The following diagram shows the device discovery lifecycle.

Figure 1: Device Discovery Lifecycle



Cisco Prime Collaboration 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 is unable to ping the device using ICMP. If ICMP is not enabled on the device, the device is moved to the Unreachable state.

Discovery States	Description
Unsupported	Cisco Prime Collaboration compares the device with the device catalog. If the device does not match with the devices in the device catalog or the SysObjectID is not known, the device is moved to this state. For a list of devices supported by Cisco Prime Collaboration Assurance and Analytics—Business 11.5, see Supported Devices for Prime Collaboration Business 11.5
Accessible	Cisco Prime Collaboration is able to access the device through all mandated credentials. This is part of the access-level discovery, which is an intermediate (transient) state during the device discovery.
Inaccessible	Cisco Prime Collaboration is not able to access the device through any of the mandated credentials. You must check the credentials and discover the devices.
Deleted	The device is hidden from Inventory Management. However, the device is in the Cisco Prime Collaboration database and can be discovered.
Inventory Collected	Cisco Prime Collaboration is able to collect the required data using the mandated data collectors. This is part of the inventory discovery, which is an intermediate (transient) state during device discovery.
Undiscoverable	Cisco Prime Collaboration is not able to collect the required data using the mandated data collectors. Connectivity issues can be caused by SNMP or HTTP/HTTPS timeout. Also, if you use HTTP/HTTPS to collect data, only one HTTP/HTTPS user can log in at a time. If Cisco Prime Collaboration faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery.
Managed	Cisco Prime Collaboration has successfully imported the required device data to the inventory database. All conference, endpoints, and inventory data are available for devices in this state. **Note** Cisco Prime Collaboration supports third-party devices whose manageability depends on MIB-II support. If the Cisco Prime Collaboration inventory exceeds your device limit, you will see a warning message. For information on how many devices Cisco Prime Collaboration can manage, see the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide.
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.

Discovery States	Description
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. See Suspend and Resume Managed Devices for details on suspended devices.

Discovery Methods

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

Discovery Type	Discover	Description
Auto discovery	Communications Manager (UCM) Cluster and connected devices	• Performs logical discovery of Cisco Unified CM. • 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. In such configuration, conductor with administrator IP must be managed first, before performing the logical discovery of Cisco Unified CM.
	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 codec, Cisco MCU, TPS, Cisco IP Video Phone E20, and Cisco MXP Series. For Cisco C and EX Series TelePresence systems, Cisco Prime Collaboration does not discover the first hop router and switch.
	Contact Center Customer Voice Portal (CVP) and connected devices	Performs logical discovery of Contact Center Customer Voice Portal (CVP) and connected devices.
		Performs logical discovery of VCenter and connected ESXi devices. For Cisco C and EX Series TelePresence systems, Cisco Prime Collaboration does not discover the first hop router and switch.

Discovery Type	Discover	Description
	VCenter and connected ESXi devices	
	UCS Manager	Performs logical discovery of UCS Manager.

Discovery Type	Discover	Description
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.
	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.
	Any Device	Discovers any other seed devices such as conductors. **Note** This option is not available in the Standard mode.

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.
-	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 can resolve the DNS name for that device. Check the DNS Server configuration to make sure it is correct. This is critical for Cisco Unified CM, Unified Presence Server, Unity Connection devices. Cisco Prime Collaboration needs to resolve the hostnames for MGCP gateways. This is because, the MGCP gateway hostnames are not added to the DNS server generally as the gateways and Cisco Unified CM are capable of operating together without DNS resolution. However, the Cisco Unified CM does not resolve the hostnames for MGCP gateways, considering it as a FQDN.
- CDP must be enabled on all 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 . These endpoints are discovered only with the discovery of the call processor with which they are registered.
- You must ensure that the device credentials that you have entered are correct. During the discovery process, based on the device that you want to discover, Cisco Prime Collaboration connects to the device by using HTTP/HTTPS, or SNMP.
- When you add devices, the HTTP (and HTTPS) port numbers are optional. These settings are automatically detected.
- Firewall devices are not supported.
- If HTTP is used to retrieve device details, disable the HTTP firewall.
- HSRP-enabled devices are not supported.
- When you add devices that have multiple interfaces and HTTP administrative access, you must manage the devices in Cisco Prime Collaboration using the same interface on which you have enabled HTTP administrative access.
- After discovering devices, if the IP address changes for network devices and infrastructure devices (such as 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 21 for information on rediscovering devices.
- If a managed device is removed from the network, it will continue to be in the Managed state until the next inventory collection occurs, even though the device is unreachable. If a device is unreachable, an Unreachable event for this device appears.
- Configuration changes on a device are discovered by Cisco Prime Collaboration only during the inventory collection process. Therefore, any changes to a device's configuration will not be shown by Cisco Prime Collaboration until the next inventory collection after the configuration change.
- To periodically update inventory, and synchronize the inventory with the Cisco Prime Collaboration database, you must perform inventory update. For more information, see Update and Collect Inventory Details.

Cisco Unified CM

- Cisco Prime Collaboration supports Unified Communications Manager cluster discovery. The Cluster IDs must be unique.
- The Access Control List (ACL) in Unified Communications Manager must contain all endpoints to be managed. If the Unified Communications Manager SNMP user configuration includes the ACL, all Unified Communications Manager nodes in the cluster must contain the Cisco Prime Collaboration server IP address.
- Cisco Prime Collaboration must discover and manage only the Unified Communications Manager publisher to manage a cluster. Subscribers are not discovered directly; they are discovered through the publisher. Cisco Prime Collaboration must manage the publisher to monitor a cluster. The Computer Telephony Integration (CTI) service must be running on all subscribers. You must ensure that the access control list in Unified Communications Manager contains all endpoints that need to be managed. If the Unified Communications Manager SNMP user configuration includes the use of the Access Control List, you must enter the Unified Communications Manager server IP address on all Unified Communications Manager nodes in the cluster.
- After you auto discover Unified Communications Manager publisher in Cisco Prime Collaboration (**Inventory** > **Inventory Management** > **Auto Discovery**), you can configure 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. It is recommended 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.

- The SNMP and HTTP credentials are mandatory for Cisco Unified CM publishers and subscribers.
- After discovering Cisco Unified CM, if you have registered any new endpoints, you must rediscover Unified CM Publisher node to add them to Cisco Prime Collaboration. See Rediscover Devices, on page 21 for information on rediscovering devices.

Note It is recommended that you should not add a subscribe node manually.

Cisco Unified CM Express and Cisco Unity Express

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

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

  where type is equal to the phone model type. If you are unsure of your model type, see Cisco.com for details on all phone model types, or enter type?. For information on how phone counts are displayed, see the window in the Inventory Management page.
- If a UC500 Series router is running Cisco Unified CM Express, you must configure "type" under ephone config for each phone so that the cmeEphoneModel MIB variable of CISCO-CME_MIB will return the correct phone model. This enables Cisco Prime Collaboration to discover the phones registered with Cisco Unified CM Express.
- For a Cisco Unity Express that is attached to a Cisco Unified CM Express to display in the Service Level View, you must use the following configuration:

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

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

Cisco VCS and Cisco VCS Expressway

- You can discover Cisco VCS clusters. Cluster names must be unique, and all endpoints that Cisco Prime Collaboration should manage must be registered in the Cisco VCS. During VCS discovery, the endpoints registered to it are also discovered. All the VCSs in a cluster need to be in managed state so that all related features work, for example 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 detects the IP address change automatically.
- If the Cisco VCS Expressway is configured within the DMZ, Cisco Prime Collaboration must be able to access the Cisco VCS Expressway through SNMP. If it cannot, then this device is moved to the Inaccessible state. For more information on setting up devices for Cisco Prime Collaboration 11.5, see the Configure Devices for Prime Collaboration Assurance wiki page.

Cisco TMS

- If you login to Cisco TMS using the <domain/username> format, then ensure that you add the same <domain/username> value for the HTTPS credentials in the HTTP(s) Username field. In case the HTTP(s) Username does not match, discovery of that Cisco TMS will fail.
- If you have Cisco MSE Supervisor, ensure that it is registered with the Cisco TMS.
- Cisco Prime Collaboration cannot manage two standalone Cisco TMS. If you are using more than one Cisco TMS, you must configure in a cluster for the Cisco Prime Collaboration application to manage. Before performing the discovery, enter the IP address of the primary active server and the secondary active or passive server details in .

Cisco TelePresence Conductor

Cisco Prime Collaboration supports Cisco TelePresence Conductor XC in the standalone model. The cluster model is not supported.

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 the Configure Devices for Prime Collaboration Assurance 11.6.

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

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

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 clusters, you need to enter specific application details.

Step 1 Choose **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, on page 8.

Note 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 Communications Manager (UCM) Cluster and connected devices, Video Communications Server (VCS) / Expressway Cluster and connected devices, Telepresence Management Suite (TMS) 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 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 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 enables the CDR and CMR flags on both publishers and subscribers of Unified Communications Manager. However Cisco Prime Collaboration performs automatic configuration of CDR billing server only on managed Unified Communications Manager publishers.

Step 8 (Optional) If you have selected "Communications Manager (UCM) Cluster and connected devices" from the **Discover** drop-down list in 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 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 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 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.

Troubleshooting

1 **Issue**: Cisco Prime Collaboration 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 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.

2 **Issue**: Cisco Prime Collaboration 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 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.

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	
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.
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 manually by using the Add Device option in the 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 Recommendations: Configure the required settings on the devices and review the recommendations.

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

Step 2 In the 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 table.

Import Devices

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

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

- Hostname
- IP address
- Protocol credentials

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

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

Step 2 Click **Import**.

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

Step 4 Click **Import**.

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

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

After discovery, the imported devices appear in the inventory. You can also look at the Device Status Summary window 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:

Step 1 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.

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.

Troubleshooting

Step 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.

Step 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.

Unified CM Cluster Data Discovery

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

- Cluster configuration data including Redundancy group, Devicepool, Location, Region, RouteList, RouteGroup, RoutePattern, Partition, and so on. This also includes the entities provisioned in the cluster such as phones, voice mail endpoints, media resources, gateways, and trunks.

- Registration information about all the entities which register with the Unified CM cluster. This includes Device IP, Registration status, the Unified CM server to which the entity is registered currently, the latest registration or unregistration time stamp, and the status reason.

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

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

Note

- Only endpoints registered to Unified CM are discovered. The endpoints registered to Cisco VCS are discovered separately.
- SIP devices are not discovered.

Schedule Cluster Data Discovery

Before You Begin

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

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

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

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

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

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

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

If changes are limited to a specific cluster, you can rediscover the publisher of the cluster by using .

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 takes more time than expected in case there is any other phone sync up operation in progress.

Rediscover Devices

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

Perform rediscovery when:

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

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

Note Accessibility information is not checked during rediscovery.

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

Rediscover Deleted Devices

To rediscover deleted devices:

Step 1 From the Inventory Management page, choose the Deleted quick filter to get a list of devices that are in the Deleted state in the Current Inventory table.

Step 2 Select the devices you want to rediscover. Click **Rediscover**.

Step 3 In the confirmation message box that appears, click **OK**.

Step 4 From the Inventory Management page, click the Discovery Jobs button to check the progress and the status of the job in the Job Management page. For more information, see Verify Discovery Status.

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

Verify Discovery Status

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

To verify discovery status:

Step 1 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, do 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.

Troubleshoot Device Discovery

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 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 Auto Discovery option. Ensure that the credentials are added for all the associated devices.

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

   Recommended Action: DX 80 and other phones are only discovered as part of Phone Sync, CDT, or Cisco Unified Communications Manager publisher cluster discovery. Other than Registration/Un-Registration status, any configuration change in phones is updated in the Cisco Prime Collaboration inventory only after the Cluster Data Discovery.

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

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

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

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

   Recommended Action: Enable the Cisco Unified Communications Manager SNMP service on the Cisco Unified Communications Manager. See the Configure Devices for Prime Collaboration Assurance 11.5 wiki page for more information.