Discovering Devices

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

Discovery Life Cycle

Discovery involves three phases:

• Access-level discovery—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 Discovery Life Cycle for information on how to disable ICMP verification.

  2. Gets all the defined credential profiles, based on the IP address. See Managing 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 Managing Device Credentials for information on required device credentials.

• Inventory discovery—Prime Collaboration polls MIB-II and other device MIBs to collect information on the device inventory, neighboring switches, and default gateway. It also verifies whether the polled device is supported in Prime Collaboration.

• Path trace discovery—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 Prime Collaboration database.
Prime Collaboration 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 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**

Prime Collaboration displays the following device states:

**Table 1: Discovery States**

<table>
<thead>
<tr>
<th>Discovery States</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>This is the preliminary state, when the device is first added. This is a transient state.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>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.</td>
</tr>
<tr>
<td>Unsupported</td>
<td>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 Prime Collaboration, see Supported Devices for Prime Collaboration Assurance.</td>
</tr>
</tbody>
</table>
## Discovery States

<table>
<thead>
<tr>
<th>Discovery States</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible</td>
<td>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.</td>
</tr>
<tr>
<td>Inaccessible</td>
<td>Prime Collaboration is not able to access the device through any of the mandated credentials (see Managing Device Credentials). You must check the credentials and discover the devices.</td>
</tr>
<tr>
<td>Deleted</td>
<td>The device is hidden from the Device Work Center. However, the device is in the Prime Collaboration database and can be discovered.</td>
</tr>
<tr>
<td>Inventory Collected</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Undiscoverable      | Prime Collaboration is not able to collect the required data using the mandated data collectors. The device state can be undiscoverable when:  

  - Prime Collaboration collects the endpoint data from CTS-Manager. If data is not collected, CTS-Manager is moved to Undiscovered state. 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 Prime Collaboration faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery. |
| Managed             | Prime Collaboration has successfully imported the required device data to the inventory database. All session, endpoints, and inventory data are available for devices in this state. You can troubleshoot a device only if it is in this state.  

  **Note**  
  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 Prime Collaboration can manage, see the Cisco Prime Collaboration Quick Start Guide |
| Suspended           | User has suspended monitoring of the device. Session 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 Suspending and Resuming Managed Devices for details on suspended devices. |

## Discovery Methods

Choose one of the following discovery methods to manage devices in Prime Collaboration Assurance:
<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Discovery Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto discovery| Logical Discovery| - Discovers management applications, conferencing devices, and call processors such as CTS-Manager, Cisco TMS, Cisco VCS, and Cisco Unified CM.  
- All endpoints and infrastructure devices registered with CTS-Manager, Cisco TMS, Cisco Unified CM, and Cisco VCS are discovered automatically during logical discovery.  
  - Logical discovery of CTS-Manager discovers Cisco TMS, Cisco Unified CM, CTS, Cisco Cius, IP phones, routers, and switches.  
  - Logical discovery of CTS-Manager discovers the first-hop router and switch for Cisco 500, 1000 and 3000 series TelePresence systems.  
  - For Cisco C and Ex series TelePresence systems, Prime Collaboration 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.  
- 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.  
- Deleted devices are not discovered again through Logical Discovery, you have to rediscover them. You can filter deleted devices using the quick filter in Device Work Center. |
<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Discovery Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| 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. |
## Discovery Methods

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Discovery Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| -              | 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, SRST 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
- 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.

### Prerequisites and Recommendations
Before performing the discovery, you must review the following and configure the devices as required:
Discovering Devices

All devices

- If DNS is configured on a device, ensure that 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. 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 CTS endpoints, CTMS, and network devices (routers and switches).

- You can discover the devices, such as endpoints, TelePresence server, and so on individually, except for mass endpoints (phones, Cisco Cius, and Cisco Jabber). 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, Prime Collaboration 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 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 CTS-Manager, Cisco Unified CM, CTMS, Cisco MCU, Cisco VCS, Cisco TS, and so on), you must rediscover these devices by providing the new IP address or hostname.

- 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 Prime Collaboration database, you must perform inventory update. For more information, see Updating and Collecting Inventory Details.
Cisco Unified CM

- Prime Collaboration supports Cisco Unified CM cluster discovery. The Cluster IDs must be unique.

- The access control list (ACL) in Cisco Unified CM must contain all endpoints to be managed. If the Cisco Unified CM SNMP user configuration includes the ACL, all Cisco Unified CM nodes in the cluster must contain the Prime Collaboration server IP address.

- Prime Collaboration must discover and manage only the Cisco Unified CM publisher to manage a cluster. Subscribers are not discovered directly; they are discovered through the publisher. 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 Cisco Unified CM contains all endpoints that need to be managed. If the Cisco Unified CM SNMP user configuration includes the use of the access control list, you must enter the Prime Collaboration server IP address on all Cisco Unified CM nodes in the cluster.

- 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.

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.

- To enable 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 Inventory Summary slider window in the Device Work Center page.

- If a UC500 Series router is running Cisco Unified CM Express, 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 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>
  session protocol sipv2
  session 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 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 session 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, Prime Collaboration detects the IP address change automatically.

- If the Cisco VCS Expressway is configured within the DMZ, 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.

CTS-Manager

- If you have installed a licensed version of Prime Collaboration, 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, Prime Collaboration will not manage the CTS-Manager.

- Prime Collaboration cannot manage two standalone CTS-Manager. If you are using more than one CTS-Manager, you must configure in a cluster for the Prime Collaboration application to manage. Before performing the discovery, enter the Primary Server IP address and hot standby or secondary server details in **Operate > Device Work Center > Manage CTS-MAN/TMS** and/or **CTX Cluster**.

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.

- 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 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 **Operate > Device Work Center > Manage CTS-MAN/TMS** and/or **CTX Cluster**.
**CTX Cluster**

- Prime Collaboration 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. Prime Collaboration 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.

- Before performing the discovery, enter the IP address of the primary and secondary admin server details in **Operate > Device Work Center > Manage CTS-MAN/TMS/CTX Cluster**.

**Cisco TelePresence Conductor**

Prime Collaboration supports Cisco TelePresence Conductor XC 1.2 and later in the standalone model. The cluster model is not supported.

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

**Media Server**

If Cisco Discovery Protocol (CDP) is not enabled on a media server (it is either disabled or not responding), Prime Collaboration will not discover the device correctly and the device will be 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, and Cisco TelePresence System EX 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 Prime Collaboration. 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 DWC.
Cisco Unified Contact Center Enterprise (Unified CCE)

- 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.
- Prime Collaboration 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 ([ ]).

Auto Discovery

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

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.

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 CTS-Manager, Cisco TMS and CTX clusters, you need to enter specific application details.

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Work Center 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.

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 Ping Sweep 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 Prime Collaboration 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 Prime Collaboration 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.

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

Step 8 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 on Job Progress to view the job status on the job management page. Or, if you have run the discovery immediately, click Job Progress in the message confirmation window to verify discovery status. See Verifying Discovery Status for more information.

---

**Discovery Filters and Scheduling Options**

**Discovery Filters**

The following table describes the filters that are available when you run discovery.
Table 2: Discovery Filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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). |

**Scheduling Options**

The following table describes the scheduling options that are available
Table 3: Scheduling Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>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.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Click None, Hourly, Daily, Weekly, or Monthly to specify the job period.</td>
</tr>
<tr>
<td>Settings</td>
<td>Specify the details of the job period.</td>
</tr>
<tr>
<td>End Time</td>
<td>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.</td>
</tr>
</tbody>
</table>

Adding Devices

You can add single or multiple devices to Prime Collaboration manually using the Add Device option on the Device Work Center 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Operate &gt; Device Work Center</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Device Work Center page, click <strong>Add Device</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Add Device window, enter the necessary information. For information regarding different credentials, see the <strong>Credential Profiles Field Descriptions</strong> table. Based on your deployment, you can select either the Customer or Assurance Domain for which you want to add the devices in the Device Information pane:</td>
</tr>
<tr>
<td></td>
<td>• NAT - If the devices you want to discover are in a NAT environment, select this check box.</td>
</tr>
<tr>
<td></td>
<td>• Customer - You can select the customer for which you want to discover the devices.</td>
</tr>
<tr>
<td></td>
<td>• IP Address - Enter the Public IP address or the Managed IP. You can enter an IPv4 or IPv6 address.</td>
</tr>
</tbody>
</table>
• 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 Prime Collaboration in MSP mode, you must provide FQDN in the Private Host Name field, while configuring endpoints registered with CUCM or ELM.

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. See Verifying Discovery Status for more information.

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.

---

## Importing Devices

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

If you have deployed Prime Collaboration 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 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.

• If the devices are in a NAT environment, ensure that you add the Customer name, Private IP and Public IP address, and Private host name of the devices.

• If you have deployed Prime Collaboration in MSP mode, you must provide Host Name as FQDN, while configuring endpoints registered with CUCM 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:
- Managing 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.

---

**Exporting 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 Operate > Device Work Center > 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.

**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.
Discovery of Cisco Unified Computing System (UCS)

Prerequisites

- VMware vCenter Server (vCenter), VMware ESX Server (ESX), and Cisco UCS Manager (UCS Manager) devices are supported in a non-NAT deployment.
- The Virtual Machines (VMs) must be powered on during 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.
- Create credential profiles for the following. Choose Operate > Device Work Center, and click the Manage Credentials button:
  - VMware vCenter Server (vCenter) - The HTTP credentials for the vCenter credential profile must be same as the vCenter device admin login credentials.
  - Cisco UCS Manager (UCS Manager) - Create the credentials as follows:
    - 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. Use the virtual IP address of the Cisco UCS Manager as the seed IP address for Logical Discovery.
    - 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. Use the IP address of Fabric Interconnect device as the seed IP address for Logical Discovery.
  - VMware ESX Server (ESX) - Add the following:
    1. The HTTP credentials for the VMware ESX Server credential profile must be the same as the VMware ESX Server device login credentials.
    2. Configure SNMP credentials on the VMware ESX Server. For more information, see the Setting up Devices for Prime Collaboration Assurance wiki page.

Note: The Virtual Machines are supported both in a NAT and non-NAT deployment.

To discover the Cisco UCS and associated Virtual Machine(s) in a non-NAT deployment, do the following:

- Choose Operate > Device Work Center > Auto Discovery, and then select Logical Discovery in the Discovery Methods 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.
- (Optional) Discover the ESX host separately which is not configured in vCenter. You can use the Add Device (Operate > Device Work Center > Add Device) or Import (Operate > Device Work Center > Import) feature, however you need to perform Logical Discovery to get the association between ESX and VM /UC applications.
• (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.

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

To discover Cisco UCS in a NAT deployment, you must use the Add Device or Import feature to discover
the vCenter, ESX or UCS Manager individually. Ensure that you use the Rediscover feature, and select the
Enable Logical Discovery check box to get the association between ESX and VM/UC applications.

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.

Unified CM Cluster Data Discovery

After the Unified CM publisher is managed in Prime Collaboration, you can 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.

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.
Scheduling 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 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 Prime Collaboration server. Otherwise, an entry must be configured for this name in the host files for the data collection to proceed further.
- For 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.

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 Setting Up Devices for Prime Collaboration for Assurance.

---

**Step 1**
Choose Administration > System Setup > Assurance Setup > Cluster Data Discovery Settings. The Cluster Device Discovery window displays the information tabulated in the following table:

**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 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 **Operate > Device Work Center > 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 Prime Collaboration Assurance will take more time than expected in case there is any other phone sync up operation in progress.

---

## Rediscovering Devices

You can rediscover devices that have already been discovered. The credentials previously entered are already available in the 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 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.

When you perform rediscovery of a device (router, switch, or voice gateway) that has become unreachable with its earlier managed IP address in Device Work Center, 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.

---

**Note**

Accessibility information is not checked during rediscovery.

The workflow for rediscovery is the same as for discovery. See **Discovery Life Cycle** for details.
Rediscovering Deleted Devices

To rediscover deleted devices:

Step 1  Choose Operate > Device Work Center.
Step 2  From the Device Work Center page, choose the Deleted quick filter to get a list of devices that are in the Deleted state in the Current Inventory table.
Step 3  Select the devices you want to rediscover. Click Rediscover. If you want to perform logical discovery (discovery of all registered devices) select the Enable Logical Discovery check box, else deselect it.
Step 4  In the confirmation message box that appears, click OK.
Step 5  From the Device Work Center, click the Discovery Jobs button to check the progress and the status of the job in the Job Management page. For more information, see Verifying Discovery Status.

Note: Deleted endpoints are not discovered as part of Unified CM, Cisco VCS, or CTS-MAN seed device discovery.

Verifying 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 Operate > Device Work Center > 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 (see Verifying Discovery Status, on page 22), and run the discovery again.

- For CTS-Manager discovery failure with the error UNDISCOVERABLE Exception:: null, perform the discovery again. (This issue occurs if multiple users are accessing CTS-Manager at the same time.)

- To discover the same devices more than once, use the Rediscover option. For more information, see Rediscovering Devices.