CHAPTER 12

Discovering Devices

The Cisco Prime Collaboration Manager discovery process involves three phases:

- Access-level discovery—Prime CM:
  a. Checks whether the device can be pinged (ICMP). If the ICMP is not enabled on the device, the device is moved to the Unreachable state. See Device States, page 12-2 for information on how to disable the ICMP verification.
  b. Gets all the defined credential profiles, based on the IP address. See Managing Credentials to understand how to define the credential profiles.
  c. Checks whether the SNMP credentials match.
  d. Identifies the device types.
  e. Verifies all other mandatory device credentials, based on the device type. If the mandatory credentials are not defined, discovery fails.

     See Setting Up the Network section in the *Cisco Prime Collaboration Manager 1.2 Quick Start Guide* to know the required device credentials.
- Inventory discovery—Prime CM 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 CM.
- Path trace discovery—Prime CM 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 CM database.

  Prime CM discovers both layer 2 and layer 3 paths.
  - For Cisco 500, 1000 and 3000 series TelePresence systems, Prime CM discovers the first-hop router and switch. See Discovery Life Cycle for a CTS-Manager.
  - For Cisco C and Ex series TelePresence systems, Prime CM does *not* discover the first hop router and switch. See Discovery Life Cycle for a TMS.

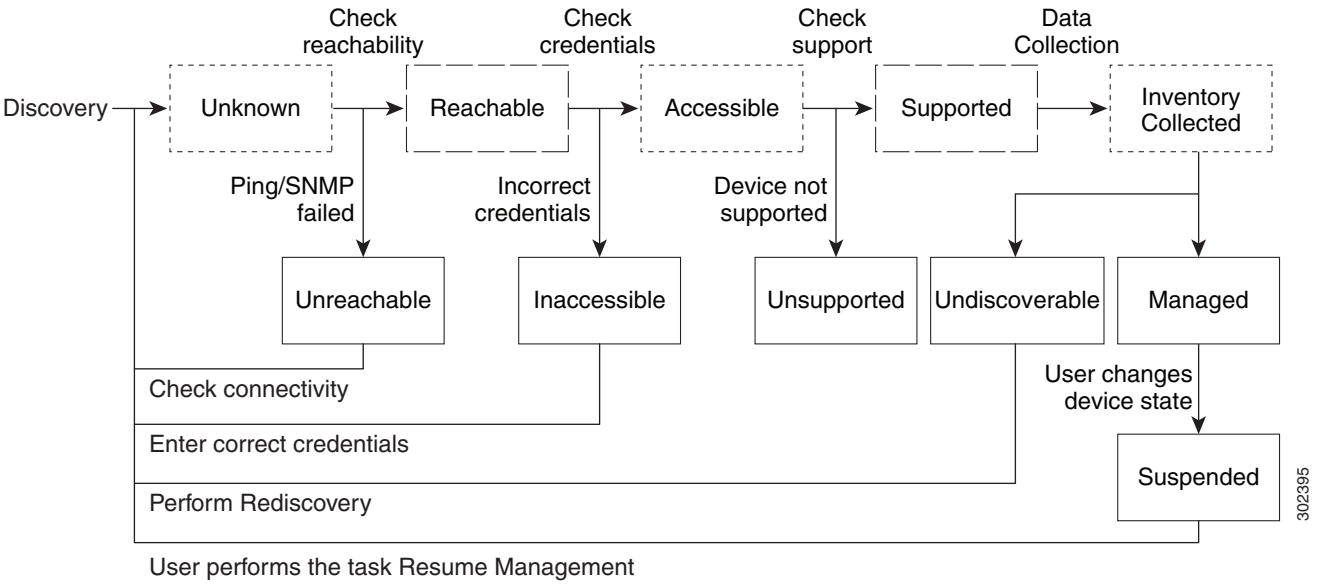
  The layer 3 path is discovered when a troubleshooting workflow is triggered either manually or automatically.

  For further details on the Troubleshooting workflow, see Troubleshooting Sessions, page 23-1.

See *Cisco Prime Collaboration Manager 1.2 Supported Devices Table* for list of devices that are supported in Prime CM.

Figure 12-1 shows the device discovery life cycle.

Figure 12-1 Device Discovery Life Cycle



Device States

A device state indicates that Prime CM 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.

Prime CM displays the following device states:

- **Unknown**—This is the preliminary state, when the device is first added.
- **Unreachable**—Prime CM is unable to ping the device, using ICMP.

  If the ICMP is not enabled on the device, the device is moved to the Unreachable state.
- **Unsupported**—Prime CM compares the device with the device catalog, if the device does not match or the SysObjectID is not known, the device is moved to this state.
- **Accessible**—Prime CM is able to access the device through all mandated credentials. This is part of the access-level discovery, which is an intermediate state during the device discovery.
- **Inaccessible**—Prime CM is not able to access the device through any one of the mandated credentials (see Managing Credentials). You must check the credentials and discover the devices.
- **Inventory Collected**—Prime CM is able to collect the required data, using the mandated data collectors. This is part of the inventory discovery, which is an intermediate state during device discovery.

- **Undiscoverable**—Prime CM is not able to collect the required data, using the mandated data collectors.
  - CTS-Manager—Prime CM must collect the endpoints data from CTS-Manager. If it not collected, CTS-Manager is moved to Undiscovered state. There is no mandate data collection for Cisco Unified CM, CTS, CTMS, and other network devices.
  - Connectivity issues can be caused by SNMP and/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 CM faces any of these problems, the device state is moved to the Undiscoverable state.

  You must perform a rediscovery.
- **Managed**—Prime CM 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.
- **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, page 14-12 for details on suspended devices.

Sequence for Discovering Devices

You must follow this sequence to discover devices in Prime CM:

1. Enter the device credentials using the Manage Credentials page (**Inventory > Device Inventory > Manage Credentials**).

   You must enter credentials for all video collaboration devices that you plan to monitor, using Prime CM. See Managing Credentials for details.
2. Discover the devices using the Inventory page (**Inventory > Device Inventory > Discover Devices**).

   If you have management and call and session control devices, such CTS-Manager, TMS, Cisco Unified CM, or VCS deployed in your network, you can discover these devices first. All registered video collaboration devices will be discovered when you discover the application managers and/or call processors.

Note

- If you have installed a licensed version of Prime CM, it is mandatory to configure the CTS-Manager Reporting API. If this feature is not configured on the CTS-Manager 1.7, or 1.8, Prime CM will not manage the CTS-Manager.
- If you are using Cisco TMS 13.0 or 13.1, it is mandatory to configure the Cisco TMS Booking API feature. If this feature is not configured, the sessions will not be monitored.

  For Cisco TMS 13.2 and above, the Cisco TMS Booking API feature need not be configured.
- If the Cisco VCS expressway is configured within the DMZ, Prime CM should be able to access the Cisco VCS expressway through SNMP. If it cannot, then this device is moved to the Inaccessible state.

You can also discover the devices (endpoints, telepresence server, and so on) individually, except for the Cisco Unified IP Phone 8900 and 9900 series, Cisco Cius, and Cisco TelePresence Movi endpoints. These endpoints are discovered only with the discovery of the call processor with which they are registered.

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

If you have Cisco MSE Supervisor, ensure that it is registered with the TMS.

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 CM connects to the device, using CLI, HTTP (HTTPS), or SNMP. CDP must be enabled on all CTS endpoints, CTMS, and network devices (routers and switches).

Cisco Unified CM Cluster Discovery

Prime CM supports Cisco Unified CM clusters. You must ensure that the cluster IDs are unique. For Cisco Unified CM publisher, a JTAPI application user account must be created with the required roles.

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 CM server IP address on all Cisco Unified CM nodes in the cluster.

Prime CM must discover and manage only the Cisco Unified CM publisher to manage a cluster. All subscribers must be discovered only through the publisher. You must not discover the subscribers directly.

Prime CM must manage the cluster publisher to monitor a cluster. The JTAPI must be configured on the cluster publisher and the computer telephony integration (CTI) service must be running on all subscribers.

Cisco VCS Cluster Discovery

Prime CM supports Cisco VCS clusters. You must ensure that the cluster names are unique. All the endpoints that need to be managed in Prime CM should be registered in the Cisco VCS master.

Figure 12-2 shows the discovery life cycle for a Cisco TelePresence Manager (CTS-Manager).

Figure 12-2 Discovery Life Cycle for a CTS-Manager

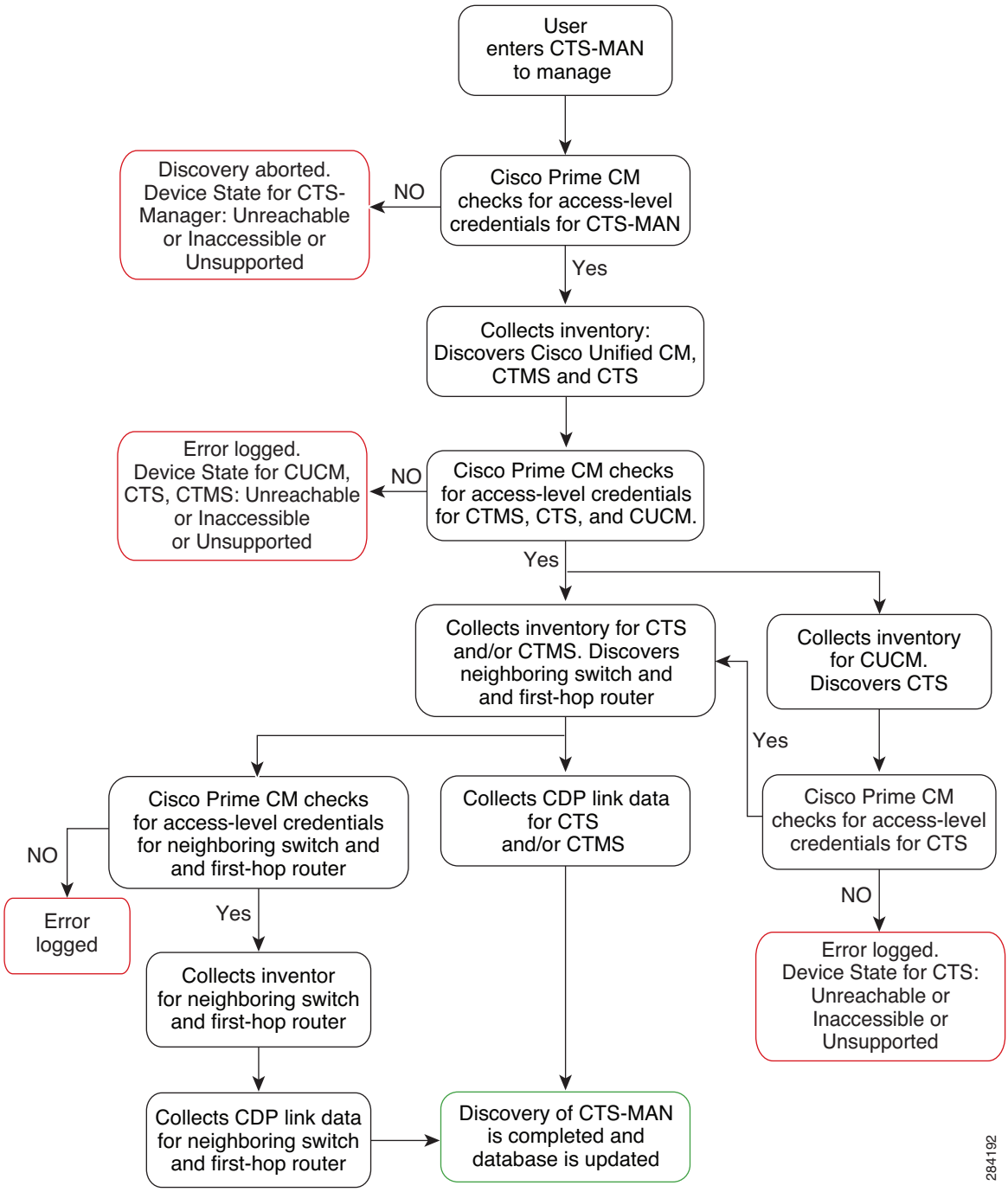
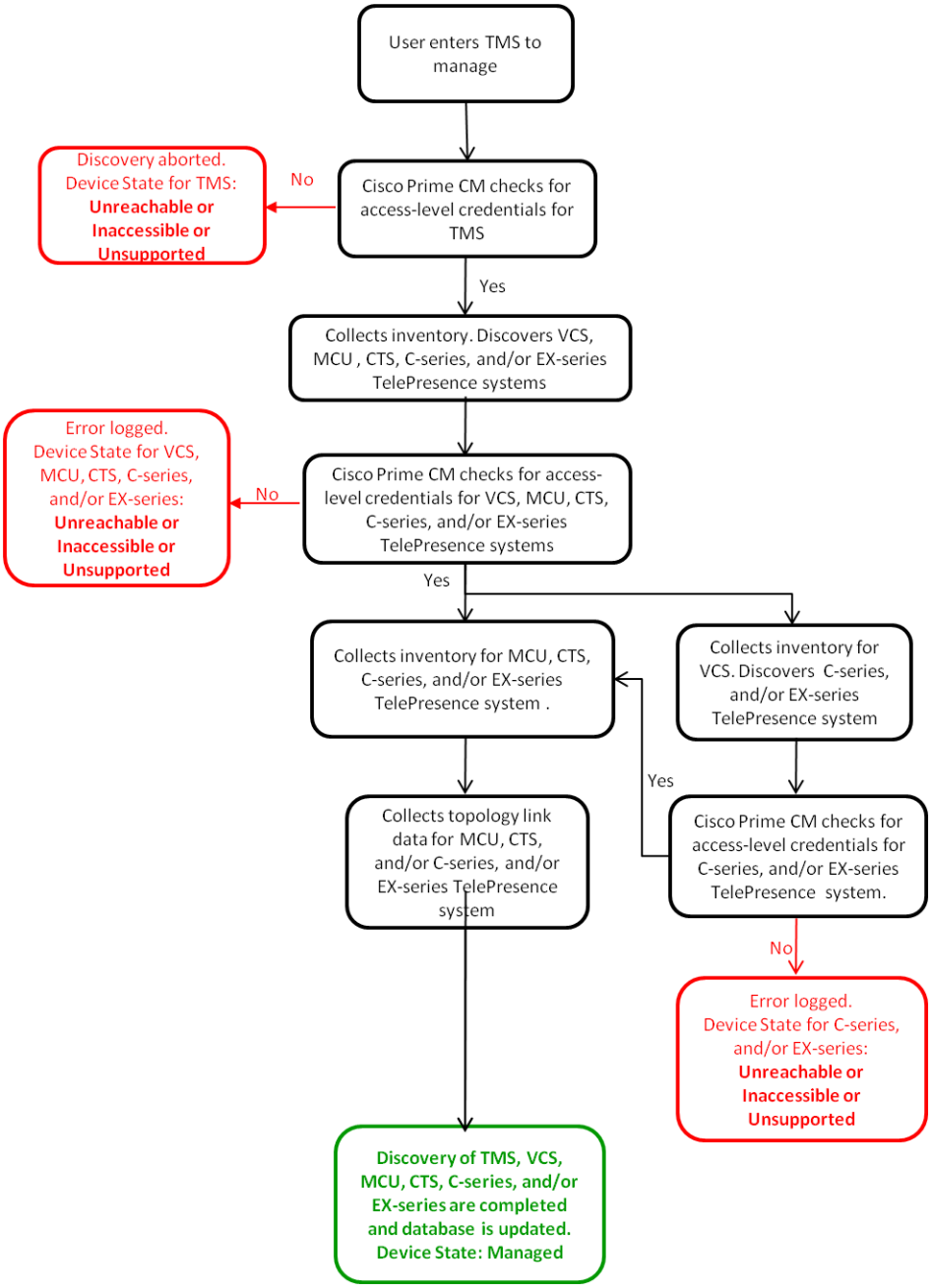


Figure 12-3 shows the discovery life cycle for a Cisco TelePresence Management System (Cisco TMS).

Figure 12-3 Discovery Life Cycle for a TMS



Adding Devices

You must perform discovery:

- When you want to add new devices to the Prime CM database.
- When you have changed the IP address of the devices.

  The endpoints registered to Cisco VCS are discovered automatically when the IP address is changed.

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

  – The endpoints by providing the new IP address or hostname.

  – The Cisco Unified CM instance to which the endpoint is registered.

  – The CTS-Manager to which the endpoint is registered.

  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 discover these devices by providing the new IP address or hostname.
- After discovering Cisco Unified CM, if you have registered any new endpoints, you must manually add these new endpoints to the Cisco Prime CM database. For Cisco VCS, the newly registered endpoints are automatically discovered.

You can either discover devices immediately or schedule a discovery job.

To discover devices:

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

The Inventory page appears.

Step 2 Click **Discover Devices**.

The Discovery Setup window appears.

Step 3 Enter the job name.

Step 4 Click **True** to enable device accessibility verification during device discovery.

Prime CM verifies device accessibility, using SNMP, CLI, HTTP (HTTPS), and JTAPI.

Step 5 Enter the IP address or hostname of the device.

You can enter multiple IP address or hostname using one of the supported delimiters: comma, colon, pipe, or blank space.

To manage a cluster, enter only the IP address of the call processor publisher. All subscribers must be discovered only through the publisher. You must not discover subscribers directly.

You can either schedule a periodic discovery job or run the discovery job immediately. To run the job immediately, go to Step 7.

Step 6 Enter the scheduling details to schedule a discovery job:

- 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**, **Hourl**y, **Daily**, **Weekl**y, 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.

Step 7 Click **Run Now** to immediately run the discovery job, or click **Schedule** to schedule the periodic discovery job to run at a later time.

The device discovery may take a few minutes to appear on the Current Inventory table, based on the device that you have entered.

You can check the progress and the status of the job, using the **List Discovery Jobs** button on the Inventory page. The Job Management page appears with the list of discovery jobs.

After the discovery job is complete, check the status of the job. There may be devices that are not discovered because of incorrect credentials. Verify the credentials for these devices (see Testing the Credentials, page 11-7) and run the discovery again.

If the CTS-Manager discovery has failed with the error `UNDISCOVERABLE Exception:: null`, perform the discovery again. This issue occurs because multiple users may be accessing CTS-Manager at the same time.

If you are discovering devices for the first time, after the discovery job has completed, you must import the sessions, using the **Import Sessions** link in the Sessions Monitoring (**Monitoring > Session Monitoring**) page.

See Import Sessions from CTS-Manager and Cisco TMS, page 15-8 for details.

If you are discovering the same devices more than once, use the rediscover option. See Rediscovering Devices, page 12-8 for details.

You can check the visibility settings of the devices added. The visibility feature for an endpoint determines to what level Prime CM monitors the operations of the endpoint. See Realtime Visibility of an Endpoint, page 15-11 for details.

Rediscovering Devices

You can rediscover devices that have already been discovered. The credentials previously entered are already available in the Prime CM database, and the system updates the new changes. Devices in any state can be rediscovered.

You can perform the rediscovery task:

- When a deleted device must be rediscovered. See Rediscovering Deleted Devices, page 12-9 for details.
- When there are changes in first hop router configuration, and for software image updates. You can perform rediscovery of a single device using the **Rediscover** button.
- When there are changes to the credentials, location, time zone, and device configurations such as IP address or hostname, SIP URI, H323 gatekeeper address, and so on. See Rediscovering Devices After Updating Credentials, page 12-9 for details.

The workflow for rediscovery is the same as for discovery. See Figure 12-1 for details.

Rediscovering Deleted Devices

To rediscover the devices listed in the Current Inventory table, you can use the **Rediscover** button available in the Current Inventory pane. You can select a single device and perform the rediscovery.

To rediscover deleted devices:

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

The Device Inventory page appears.

Step 2 Filter the devices in the Deleted state from the Current Inventory table.

You can use the quick filter Deleted to get the list of devices in this state.

Step 3 Choose the devices you want to Rediscover.

Step 4 Click **Rediscover**.

A message appears, `Are you sure you want to Rediscover the selected devices?`

Step 5 Click **OK.**

A message appears, `Selected devices Rediscovered successfully.`

You can check the progress and the status of the job, using the **List Discovery Jobs** button on the Inventory page. The Job Management page appears with the list of discovery jobs.

Rediscovering Devices After Updating Credentials

To rediscover devices after the credentials (see Managing Credentials) have been changed:

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

The Inventory page appears.

Step 2 Click **Discover Devices**.

The Discovery Setup window appears.

Step 3 Click **True** to enable device accessibility verification while discovering devices.

Prime CM verifies device accessibility, using SNMP, CLI, HTTP (HTTPS), and JTAPI. To rediscover devices using IP address/ Host name, go to Step 5.

Step 4 If you want to rediscover devices based on device type or device status, check the **Re-discover devices based on a criteria** check box. (If you select this option, you will not be able to rediscover devices by entering their IP address or hostname).

- Device type—You can rediscover all the devices except for the Cisco Unified IP Phone 8900 and 9900 series, Cisco Cius, and Cisco TelePresence Movi endpoints.
- Device status—You can rediscover devices that are in inaccessible, unreachable, undiscoverable, unknown, deleted, and unsupported states.

Note For rediscovering the Cisco Unified IP Phone 8900 and 9900 series, Cisco Cius, and Cisco TelePresence Movi endpoints, enter the IP address of the endpoint (Step 5).

Step 5 Enter the IP address of the device.

You can enter multiple IP address or host name using one of the supported delimiters: comma, colon, pipe, or blank space.

Step 6 Click **Run Now** to immediately run the rediscovery job, or click **Schedule** to schedule the periodic rediscovery job to run at a later time.

For scheduling periodic rediscovery jobs (which is same as scheduling periodic discovery jobs), go to Step 6 of Adding Devices, page 12-7.

You can check the progress and the status of the job, using the **List Discovery Jobs** button on the Inventory page. The Job Management page appears with the list of discovery jobs.