



## Using Device Management

---

These topics explain how to use IP Communications Operations Manager (Operations Manager) Device Management:

- [Getting Started with Device Management, page 15-1](#)
- [Understanding the Device Summary and Device States, page 15-7](#)
- [Importing Devices into Operations Manager, page 15-8](#)
- [Editing Device Configuration and Credentials, page 15-15](#)
- [Using Default Device Credentials, page 15-15](#)
- [Performing Inventory Collection, Viewing Details, and Deleting Devices, page 15-16](#)
- [Viewing Discovery Status, page 15-24](#)
- [Editing SNMP Timeout and Retries, page 15-24](#)
- [Configuring LDAP, page 15-25](#)
- [Understanding Cisco CallManager Security Certificates, page 15-27](#)

## Getting Started with Device Management

For Operations Manager to monitor a device, you must first add the device to the CiscoWorks Common Services Device and Credentials Repository (DCR). Use the DCR to perform the following operations:

- Adding devices
- Importing devices
- Exporting devices
- Changing device credentials

Once a device is added to the DCR, you can then add it to the Operations Manager inventory, which is separate from the DCR. You can add devices from the DCR to Operations Manager automatically by activating automatic synchronization (the default), or you can add them selectively by deactivating using the Device Selector. For more information on how Operations Manager is affected by the DCR, see [Understanding the Device Summary and Device States, page 15-7](#).

Operations Manager is the front-end for performing the following operations on devices in the Operations Manager inventory:

- Deleting devices (*local delete*)
- Viewing device details

- Performing inventory collection on devices
- Suspending and resuming Operations Manager device management

As Operations Manager performs inventory collection on devices, they pass through various *device states* until they are fully recognized by Operations Manager (see [Verifying Device Import, page 15-14](#) for details). Once a device is in Operations Manager inventory, Operations Manager monitors the device and its components according to the polling and threshold settings that apply to the device group (when it is added to the DCR, the DCR assigns the device to a device group).

**Note**

When working with device management, remember the following:

- If a monitored device is removed from the network, it will continue to be in the Monitored state until the next inventory collection occurs, even though the device is unreachable. The only way that you will know that this device is unreachable, is when an Unreachable alert appears for this device in the Alerts and Events display.
- Configuration changes on a device are discovered by Operations Manager only during the inventory collection process. Therefore any changes to a device's configuration will not be shown by Operations Manager until the next inventory collection after the configuration change.
- If Cisco Discovery Protocol (CDP) is not enabled on a Media Server (either it is disabled or not responding) Operations Manager will not discover the device correctly and the device will be moved to the Unsupported state.
- If the Operations Manager server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to [Device-Based Filtering, page 19-469](#).

Operations Manager manages a device when the device's *management state* is set to True; conversely, Operations Manager is not managing a device when its management state is set to False. A device with a management state set to False is called a *suspended device*. You can also selectively unmanage device components (see [Suspending/Resuming a Device Component, page 3-81](#)).

For information on how many devices Operations Manager can manage, refer to *Installation Guide for IP Communications Operations Manager*. If the Operations Manager inventory exceeds your device limit, you will see a warning message. For more information, see [Responding to Messages About Device Limits, page 1-24](#).

## Types of Devices that Operations Manager Monitors

When devices are added to the DCR, they are assigned to Common Services System Defined Groups. The group to which the DCR assigns the device depends on the device type users specify when they add the device. If a user does not select a device type, or selects the wrong device type, the DCR designates the device as Unsupported, and it is assigned to the Common Services Unsupported group. (For devices with no specified device type, Operations Manager assigns a device type when it performs inventory collection on the device.)

For examples of the types of devices that Operations Manager monitors, see [Table 16-1 on page 16-344](#).

**Note**

For a detailed list of devices that Operations Manager supports, see *Supported Device Table for IP Communications Operations Manager* on Cisco.com at [http://cisco.com/en/US/partner/products/ps6535/products\\_device\\_support\\_table09186a0080552d07.html](http://cisco.com/en/US/partner/products/ps6535/products_device_support_table09186a0080552d07.html).

## Ports and Interfaces that Operations Manager Monitors

The following describes the default ports and interfaces that Operations Manager monitors or does not monitor:

- Ports (switches)—By default, Operations Manager monitors trunk ports but does not monitor access ports.
  - An access port is a switch port that is connected to a host or device that Operations Manager does not monitor; that is, an end-station port.
  - A trunk port is a port that connects to a Cisco network device running Cisco Discovery Protocol (CDP). In other words, a trunk port connects to a router, or to a switch that the same Operations Manager server manages.
- Interfaces (routers)—By default, Operations Manager monitors all interfaces listed in the ifTable.

## Understanding the Device and Credentials Repository

The DCR is a centralized device repository for sharing device information across applications. It provides a single place for managing device credentials and attributes, ensuring consistency across applications. Individual applications can query the DCR for a device list, device attributes, and device credentials. Changes to the DCR are propagated to all applications. Thus, you should use the DCR to add, import, and export devices, and to change device credentials. For details on how you can add devices to the DCR, see the Common Services online help.

**Note**

A device must be added to the DCR before it can be added to the Operations Manager inventory.

Once a device is added to the DCR, you can add it to the Operations Manager inventory (the Operations Manager inventory is separate from the DCR). When a device is added to the DCR, the DCR assigns a DCR ID to every managed component. The DCR maps components to devices using either the device name or IP address. When the DCR device is added to Operations Manager, Operations Manager maps the DCR ID to a device name during inventory collection (see [Table 15-2 on page 15-9](#)).

Operations Manager also uses the DCR ID to verify if the device or component already exists in the Operations Manager inventory. (Further information on how Operations Manager identifies devices—such as whether Operations Manager uses an IP address or DNS name as the device name—is provided in [Importing Devices from the DCR, page 15-9](#).)

You can add devices from the DCR to Operations Manager automatically by activating automatic synchronization (which is the default), or you can add them selectively by deactivating using the Device Selector. When a device is deleted locally (from the Operations Manager inventory), the DCR is not affected. The device is added to the Device Selector list, which shows which devices are in the DCR but not in Operations Manager. (In this way, you can easily add the device back to Operations Manager, if desired.)

If a device is deleted from the DCR (*global delete*), it is deleted from Operations Manager (and all other applications that use that DCR). (For information on deleting components of aggregate devices, see [How Operations Manager Handles Containing and Contained Devices, page 15-10](#).)

All synchronization between the DCR and the Operations Manager inventory is controlled from the Device Management: Summary page.

- For automatic synchronization, the Device Selection field in the Device Management: Summary page must be set to automatic. See [Automatically Importing DCR Devices, page 15-10](#).
- For manual synchronization (in which you selectively add devices from the DCR to the Operations Manager inventory), see [Manually Importing DCR Devices, page 15-11](#). (However, if a device is deleted from the DCR, it is deleted from Operations Manager.)

**Note**

Do not confuse the Operations Manager physical discovery process (which adds devices to the DCR) or the Operations Manager inventory collection process (which probes devices and updates components in Operations Manager inventory) with the DCR synchronization process. Operations Manager inventory collection is a process that affects only the Operations Manager inventory.

## Adding Devices to the DCR From Operations Manager

Operations Manager adds devices to the DCR through physical discovery.

**Note**

To add devices to the DCR using bulk import (importing from an NMS or from a file), use the instructions in the Common Services online help.

## Running Operations Manager Physical Discovery

- Step 1** Select **Devices > Device Management**. The Device Management: Summary page appears.
- Step 2** Click the **Configure** button next to the Last Discovery and Next Discovery fields. The Discovery page appears.

**Note**

Discovery requires SNMP and/or SNMPv3 credentials. If the credentials are not configured, when you click the **Configure** button, you will be redirected to the Default Credentials Page. Enter the default credentials. When you click **Save**, the Discovery page appears.

- Step 3** Enter data described in the following table.

Field	Action/Description
Seed Devices	Enter a comma-separated list of IP addresses, or select the Use all devices currently in Device and Credentials Repository check box.
Ping Sweep	(Optional) This is an alternative to using seed device-based discovery. Select the Use Ping Sweep check box and specify a comma-separated list of IP address ranges using the <i>/netmask</i> specification. For example, 172.20.57.1/24 to specify a ping sweep range starting from 172.20.57.1 and ending at 172.20.57.255.

Field	Action/Description
IP Address	<p>(Optional) Enter comma-separated IP addresses or IP address ranges for devices that you want to:</p> <ul style="list-style-type: none"> <li>• Include—In the auto-discovery process.</li> <li>• Exclude—From the auto-discovery process.</li> </ul> <p>You can use wildcards when specifying the IP address range.</p> <p>An asterisk (*) denotes the octet range of 1-255. Also, the octet range can be constrained using the [xxx-yyy] notation.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• To include all devices in the 172.20.57/24 subnet in the auto-discovery process, enter an include filter of 172.20.57.*.</li> <li>• To exclude devices in the IP address range of 172.20.57.224 - 172.20.57.255 from the auto-discovery process, enter an exclude filter of 172.20.57.[224-255].</li> </ul> <p>Both types of wildcards can be used in the same range specification; for example, 172.20.[55-57].*. If both include and exclude filters are specified, the exclude filter is applied first before the include filter. Once a filter is applied to an auto-discovered device, no other filter criterion will be applied to the device. If a device has multiple IP addresses, the device will be processed for auto-discovery as long as it has one IP address that satisfies the include filter.</p>
DNS Domain	<p>(Optional) Enter comma-separated DNS domain names for devices that you want to:</p> <ul style="list-style-type: none"> <li>• Include—In auto-discovery processing.</li> <li>• Exclude—From auto-discovery processing.</li> </ul> <p>The DNS names can be specified using wildcards. An asterisk (*) matches any combination of mixed uppercase and lowercase alphanumeric characters, along with the hyphen (-) and underscore (_) characters, of an arbitrary length. A question mark (?) matches a single uppercase or lowercase alphanumeric character or a hyphen or an underscore character.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• *.cisco.com matches any DNS name ending with .cisco.com.</li> <li>• *.?abc.com matches any DNS name ending with .aabc.com, or .babc.com, etc.</li> </ul>

Field	Action/Description
SysLocation	<p>(Optional) Enter comma-separated strings that will match the string value stored in the sysLocation OID in MIB-II, for devices that you want to:</p> <ul style="list-style-type: none"> <li>• Include—In auto-discovery processing.</li> <li>• Exclude—From auto-discovery processing.</li> </ul> <p>The location strings can be specified using wildcards. An asterisk (*) matches, up to an arbitrary length, any combination of mixed uppercase and lowercase alphanumeric characters, hyphen (-), underscore (_), and, white space (spaces and tabs). A question mark (?) wildcard matches a single occurrence of any of the above characters. For example, a SysLocation filter of <i>San *</i> will match all SysLocation strings starting with <i>San Francisco, San Jose, etc.</i></p>
Run	<p>Select a radio button and enter the schedule:</p> <ul style="list-style-type: none"> <li>• Now—Select to run immediately.</li> <li>• Daily—Enter time and select days on which to run (Sun, Tue...Sat).</li> <li>• Weekly—Enter the weekly frequency (every N weeks), the time and day on which to run.</li> </ul>

- Step 4** Click **OK**. Physical discovery starts to run and takes some time to complete. (Check the status of discovery on the Device Management: Summary page.)

## Events that Trigger DCR and Operations Manager Synchronization

The following events will trigger synchronization between the Operations Manager inventory and the DCR:

- Devices are added or deleted, or their credentials (IP address, SNMP credentials, MDF type) are changed in the DCR. (This also triggers a device inventory collection in Operations Manager).
- DCR is changed from:
  - Master to slave
  - Standalone (single server) to slave
- DCR is restored from a different domain.

See these topics for more information:

- [Importing Devices from the DCR, page 15-9](#)
- [Determining the Media Server Account to Use for Cisco CallManager Access, page 15-24](#)

## DCR Masters and Slaves

By default, the DCR mode is standalone (single server), and CiscoWorks supports one DCR per CiscoWorks server. However, you can configure the DCR to use a master/slave model. In this model, the master DCR is the primary repository residing on a CiscoWorks server. Slave DCRs reside on other CiscoWorks servers, and replicate the DCR master. Any change in the master DCR is propagated to slave DCRs. This allows applications on different servers to use a synchronized device inventory. Using the master/slave model is transparent to Operations Manager.

If the DCR used by your instance of Operations Manager is changed from master to slave, or from standalone to slave, the DCR device list is synchronized with the Operations Manager inventory. First, all devices are removed from the Operations Manager inventory (regardless of DCR synchronization mode). If Operations Manager is configured to use manual synchronization, all DCR devices will appear in the Device Selector (as devices not in Operations Manager). For automatic synchronization, all DCR devices are added to the Operations Manager inventory.

For more information on the DCR master/slave model, refer to the Common Services online help

## Understanding the Device Summary and Device States

The Device Management: Summary page lists the device states for all devices in the Operations Manager inventory. The Device Management: Summary page appears when you select **Devices > Device Management**. Figure 15-1 shows an example of the Device Management: Summary page.

Figure 15-1 Device Management: Summary Page

The screenshot displays the 'Device Management: Summary' page in the IP Communications Operations Manager interface. The page includes a navigation menu on the left, a breadcrumb trail, and a main content area with a table of device states and summary statistics. The table lists states and their corresponding numbers. Below the table are sections for Device Selection, Last Discovery, and Next Discovery, each with a 'Configure' button.

State	Number
Monitored:	72
Partially Monitored:	12
Monitoring Suspended:	0
Inventory Collection in Progress:	0
Unreachable:	55
Unsupported:	1
<b>Total Devices:</b>	<b>140</b>
<b>Total Phones:</b>	<b>16</b>

**Device Selection:** Automatic

**Last Discovery:** Completed at Mon 19-Dec-2005 10:01:44 PST.  
80 devices discovered.

**Next Discovery:** Scheduled to run on Tue 20-Dec-2005 10:00:00 PST

Table 15-1 describes the information displayed on the Device Management: Summary page.

**Table 15-1** Device Management: Summary Page

Heading/Button	Description
State	Lists the state the devices are in, from the following possibilities:
Monitored	The device has been successfully imported, and is fully managed by Operations Manager.
Partially Monitored	The device has been successfully imported by some of the data collectors <sup>1</sup> in Operations Manager, but not all. If a device is in this state, you should take action to ensure that the device becomes monitored.
Monitoring Suspended	Monitoring of the device is suspended.
Inventory Collection in Progress	Operations Manager is probing the device. This is the beginning state, when the device is first added; a device is also in this state during periodic inventory collection. Some of the data collectors may still be gathering device information.
Unreachable	Operations Manager cannot manage the device. See <a href="#">Troubleshooting Device Import and Inventory Collection, page 15-14</a> .
Unsupported	The device is not supported by Operations Manager.
Number	The number of devices that are in each device state. The blue numbers are links to device reports. When you click a blue number a device report for that specific device state opens. See <a href="#">Understanding a Device Report, page 15-19</a> .
Device Selection (Configure)	You can configure how you want Operations Manager to select devices from the DCR.
Last Discovery	The date and time when Operations Manager last performed physical discovery.
Next Discovery (Configure)	The date and time when Operations Manager will next perform physical discovery. You can configure physical discovery using the Configure button. See <a href="#">Adding Devices to the DCR From Operations Manager, page 15-4</a> .

1. *Data collector* is a term used to refer to all back-end applications that are involved in device discovery and device data collection.

## Importing Devices into Operations Manager

A device must be in the DCR before you can add it to the Operations Manager inventory. Operations Manager supports two methods of device import from the DCR:

- Using automatic synchronization between the DCR and Operations Manager (see [Automatically Importing DCR Devices, page 15-10](#))
- Using manual synchronization between the DCR and Operations Manager (see [Manually Importing DCR Devices, page 15-11](#))

## Importing Devices from the DCR

Once a device has been added to the DCR, it can be added to the Operations Manager inventory:

- Automatically (whenever there is an addition or change), if Device Selection is set to Automatic in the Device Management: Summary page.
- Manually (on a device-by-device basis), if Device Selection is set to Manual in the Device Management: Summary page.

To verify which setting you are using, select **Devices > Device Management**, and check the Device Selection setting.



**Note**

Your login determines whether you can import devices into Operations Manager.

## How Operations Manager Identifies Devices Imported from the DCR

When a device is added to Operations Manager from the DCR, Operations Manager attempts to resolve the DNS name (hostname). Operations Manager does not use the DCR Display Name. [Table 15-2](#) shows how Operations Manager names devices, depending on how the devices are added to the DCR.

**Table 15-2** How Operations Manager Determines Device Names

When device is added to DCR with...	Operations Manager does the following:
IP address and hostname (DNS name)	<ul style="list-style-type: none"> <li>• Uses the DNS name, if Operations Manager can resolve it</li> <li>• Uses the IP address, if Operations Manager cannot resolve the DNS name</li> </ul>
IP address only	<ul style="list-style-type: none"> <li>• Uses the DNS name, if Operations Manager can resolve the IP address</li> <li>• Uses the IP address, if Operations Manager cannot resolve the DNS name</li> </ul>
DNS name only	Uses the DNS name, even if not resolvable
IP address, and the IP address was already added to the DCR (this is allowed in the DCR)	Chooses one IP address and the other becomes a duplicate. For details on how to determine if you have duplicate devices, see <a href="#">Viewing the IP Address Report Page, page 15-12</a> .
IP address, and the IP address corresponds to two interfaces of the same physical device	Chooses one IP address and the other becomes a duplicate. For details on how to determine if you have duplicate devices, see <a href="#">Viewing the IP Address Report Page, page 15-12</a> .



**Note**

Once a device is added to the DCR with a specified MDF type and sysObjectID, no one can overwrite it, even if it is incorrect. The only exception is if no sysObjectID is supplied, as described in the previous table.

For information on how Operations Manager performs polling and discovery, see [Appendix F, “Polling—SNMP and ICMP.”](#)

## How Operations Manager Handles Containing and Contained Devices

Operations Manager supports contained and containing devices (also referred to as aggregate devices). These are devices that have a parent/child relationship with another device, such as a Catalyst switch (parent) containing an MSFC (child). The switch is considered the containing device, and the MSFC is the contained device.

**Table 15-3 How Operations Manager Handles Containing and Contained Devices**

Action	Effect on Device	
	Containing	Contained
<b>Adding to Operations Manager (regardless of DCR synchronization mode)</b>		
Containing	Added	Added <sup>1</sup>
Contained	N/A	N/A
<b>Inventory Collecting in Operations Manager</b>		
Containing	Inventory collected	Inventory collected
Contained	No effect	Inventory collected
<b>Removing from Operations Manager</b>		
Containing	Deleted	Deleted from Operations Manager (but not deleted from DCR)
Contained	No effect	Deleted
<b>Removing from DCR</b>		
Containing	Deleted	Deleted
Contained	No effect	Deleted
<b>Suspending in Operations Manager</b>		
Containing	Suspended	Suspended
Contained	No effect	Suspended
<b>Resuming in Operations Manager</b>		
Containing	Resumed	Resumed
Contained	No effect	Resumed only if containing device is resumed

1. When a containing device is added to the DCR, the DCR does not recognize the contained devices. However, when the device is added to Operations Manager, the contained devices are probed by Operations Manager and added to the Operations Manager inventory.

## Automatically Importing DCR Devices

Operations Manager uses automatic synchronization by default. Use the following procedure to change manual synchronization to automatic synchronization.



### Note

If you are running the synchronization process for the first time, it may take several hours for Operations Manager to collect inventory for all of the devices, depending on how many devices are being added to Operations Manager.

**Step 1** Select **Devices > Device Management**. The Device Management: Summary page appears.

**Step 2** Click the **Configure** button next to the Device Selection field. The Device Selection page appears.

- Step 3** Activate the Automatic radio button.
- Step 4** Click **Apply**. Operations Manager will be synchronized with the DCR; any DCR devices currently not in Operations Manager will be added. Operations Manager will perform inventory collection for the new devices that are being added.
- Step 5** Verify whether any duplicate devices exist, by selecting **Devices > Device Management > IP Address Report**.



**Note** If you do not require the duplicate device for your deployment, remove it using **Devices > Device Credentials**. This takes you directly to CiscoWorks Common Services Device Management.



**Note** If you exceed your device limit, Operations Manager will continue to operate, but you will notice that devices are not being added to Operations Manager. Check the license log as described in [Accessing and Deleting Log Files, page 19-461](#). For information on device-based licensing, see [Responding to Messages About Device Limits, page 1-24](#).

For information on the inventory collection schedule, see [Scheduling Inventory Collection, page 15-22](#).

## Manually Importing DCR Devices

Use the following procedure to change automatic synchronization to manual synchronization.

- Step 1** Select **Devices > Device Management**.
- Step 2** Click the **Configure** button next to the Device Selection field. The Device Selection page appears.
- Step 3** Select the Manual radio button. All devices that are not in Operations Manager inventory are available through the device selector.
- Step 4** Select devices the following ways:
- Entering device names or IP addresses in the Device Display Name, and clicking **Filter**.
  - Using the group selector.
- Step 5** If you want to see the devices you have selected, click the Selection tab, and a list of devices appears.
- Step 6** Click **Select**. Operations Manager will perform inventory collection on the devices that are being added.
- Step 7** Verify whether any duplicate devices exist, by selecting **Devices > Device Management > IP Address Report**.



**Note** If you do not require the duplicate device for your deployment, remove it using **Devices > Device Credentials**. This takes you directly to CiscoWorks Common Services Device Management.

**Note**

If you exceed your device limit, Operations Manager displays a warning message. You can get more information from the license log as described in [Accessing and Deleting Log Files, page 19-461](#). For information on device-based licensing, see [Responding to Messages About Device Limits, page 1-24](#).

For information on how to handle duplicate devices, refer to [Viewing the IP Address Report Page, page 15-12](#).

## Determining Which Devices Are in the DCR But Not in Operations Manager

To identify devices that are in the DCR but not in Operations Manager, use the Device Selection page. In the Device Selection page with the Manual radio button selected, the device selector lists the devices that are not in Operations Manager. Devices may not be in Operations Manager for these reasons:

- The devices have not been added to Operations Manager because Operations Manager is using manual DCR synchronization.
- The devices were deleted from Operations Manager. (Devices you delete from Operations Manager are not deleted from the DCR.)

**Note**

Devices you delete can only be added back into Operations Manager using manual import.

See [Manually Importing DCR Devices, page 15-11](#) on how to access the Device Selection page.

For information on moving devices from the DCR into Operations Manager, see [Manually Importing DCR Devices, page 15-11](#). For information on duplicate devices, see [Viewing the IP Address Report Page, page 15-12](#).

## Viewing the IP Address Report Page

The IP Address Report page lists all the IP addresses of the devices that are added to Operations Manager. The IP address list includes both the IP addresses of the devices in the DCR (including devices that are not monitored by Operations Manager) and the IP addresses of all the devices in Operations Manager inventory.

The IP Address Report page displays the following:

- The IP addresses for all the devices in the DCR, but not in Operations Manager inventory. The IP Address Report may only display the IP address (if added) and the DCR display name.
- The IP addresses for all the devices in Operations Manager inventory.
- All the IP addresses known for each of the devices in Operations Manager inventory. If there is more than one IP address for a monitored device, all the IP addresses are displayed. The DCR Display Name column displays N/A and the Device Name and Managed IP Address columns will have the same entries for the corresponding device.

- Duplicate device entries from the DCR. If there is more than one entry for the same device in the DCR (this can occur by varying the DCR display name), the IP Address Report identifies the duplicate entries and appends the display names with the corresponding IP address entry in the DCR Display Name column.



**Note** The duplicate entries in the DCR are identified by having more than one display name in the DCR Display Name column of the IP Address Report.

**Step 1** Select **Devices > Device Management > IP Address Report**. The IP Address Report page appears. [Figure 15-2](#) shows an example of the IP Address Report page.



**Note** If you want to delete a duplicate device, use **Devices > Device Credentials**. This takes you directly to CiscoWorks Common Services Device Management.

**Figure 15-2 IP Address Report Page**

IP Address Report			
Showing 84 records			
	IP Address	DCR Display Name	Device Name
1.	172.20.119.19	172.20.119.19	vegas-vg200-2.cisco.com
2.	192.168.1.1	N/A	vegas-vg200-2.cisco.com
3.	161.44.250.19	161.44.250.19	161.44.250.19
4.	11.11.11.9	N/A	172.20.118.49
5.	172.20.118.49	172.20.118.49	172.20.118.49
6.	172.20.118.81	172.20.118.81	SW-PUB
7.	172.20.121.168	172.20.121.168	172.20.121.168
8.	172.20.118.24	172.20.118.24	nm-sol-server.cisco.com
9.	172.20.119.17	172.20.119.17	vegas-3640.cisco.com
10.	192.168.20.1	N/A	vegas-3640.cisco.com
11.	172.20.121.41	172.20.121.41	1-skate-7845h.cisco.com

**Table 15-4 IP Address Report Page**

Heading	Description
IP Address	IP address known to Operations Manager.
DCR Display Name	Display name used when the device was added to the DCR.
Device Name	Device name as seen in Operations Manager. Clicking the device name opens the Detailed Device View page for the device.
Managed IP Address	IP address of the device through which Operations Manager manages the device.

## Verifying Device Import

After adding a device, you can verify that it has been imported by using the View/Rediscover/Delete Devices page.

- 
- Step 1** Select **Devices > Device Management > View/Rediscover/Delete**. The View/Rediscover/Delete Devices page opens. [Figure 15-3](#) shows an example of the View/Rediscover/Delete Devices page.
- Step 2** In the device selector, locate the device you added.
- Step 3** Click on the device. The device information appears in the right pane. Verify that Device Status is Monitored. A Monitored state on the device indicates that it was imported successfully.



**Note** For a complete explanation of the device states, see [Understanding the Device Summary and Device States, page 15-7](#).

- Step 4** If the device is not in the Monitored state, refer to [Troubleshooting Device Import and Inventory Collection, page 15-14](#).
- 



**Tip**

If your device appears in the device selector under the All Monitored Devices group, it was fully imported into Operations Manager. Only the devices in the All Partially Monitored Devices group and the All Unreachable Devices group were not imported fully into Operations Manager.

---

## Troubleshooting Device Import and Inventory Collection



**Note**

If device inventory collection or discovery is being performed over a slow network connection, or if the devices are unusually slow in responding to SNMP or HTTP requests, you can change the `ivr.properties` file to avoid Operations Manager from timing out during discovery or inventory collection. The file is located in the `NMSROOT/conf/ivr` folder.

To increase the time allocated for discovery or inventory collection, change the property `messageFactor:6` to `messageFactor:10`. The higher the number, the longer Operations Manager waits before timing out.

---



**Note**

`NMSROOT` is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it is `C:\Program Files\CSCOPx`.

---

- Step 1** Select **Devices > Device Management > View/Rediscover/Delete**. The View/Rediscover/Delete Devices page opens. [Figure 15-3](#) shows an example of the View/Rediscover/Delete Devices page.
- Step 2** Expand the folder that contains your device (according to its inventory collection status; refer to [Verifying Device Import, page 15-14](#)).
- Step 3** Click the device name or IP address. The device information is populated.

- Step 4** Look under Data Collection Status Information for error information.
- Step 5** Perform the required actions to clear the error.
- 

## Editing Device Configuration and Credentials

After you add devices, you can change their configuration setup using CiscoWorks Common Services. From Operations Manager, select **Devices > Device Credentials**. The Common Services Device Summary page appears.

**Note**

Operations Manager provides you with a link to the CiscoWorks home page in the top right corner of your browser. From the CiscoWorks home page, select **Device and Credentials > Device Management**. For more details on using CiscoWorks Common Services Device Management, see the CiscoWorks Common Services online help.

---

From the Common Services Device Management page you can access the Device Properties page. From this page, you can edit the following:

- Basic information, IP address, and domain names.
- Device type (MDF group).
- Credentials information such as usernames, passwords, and community strings.
- User-defined fields that store additional user-defined data for a device.

**Note**

If you are changing credentials for a device that also has a duplicate, be sure to change the credentials on both devices in case the primary device is deleted.

---

Click the Help button to view more information on the device credentials you can change using Common Services.

## Using Default Device Credentials

The Default Credentials page enables you to specify credentials that will be tried by auto-discovery in order to physically discover the devices in the network. Once auto-discovery determines the correct credentials for a device, it will enter those credentials in the DCR for that device. The credentials specified in the Default Credentials page are not used for any other purpose in Operations Manager.

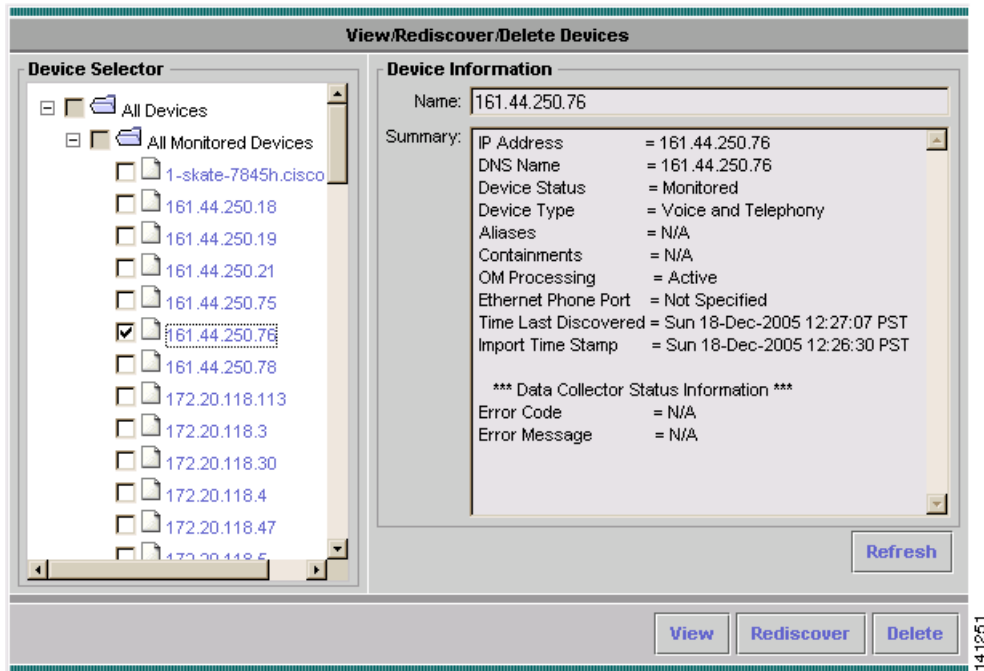
---

- Step 1** Select **Devices > Device Management > Discovery Credentials**. The Default Credentials page opens.
- Step 2** Enter the credentials that you want Operations Manager to use.
- Step 3** Click **Save**.
-

# Performing Inventory Collection, Viewing Details, and Deleting Devices

Performing inventory collection, viewing details, and deleting specific devices is controlled by the View/Rediscover/Delete Devices page. [Figure 15-3](#) shows the View/Rediscover/Delete Devices page.

**Figure 15-3** View/Rediscover/Delete Devices Page

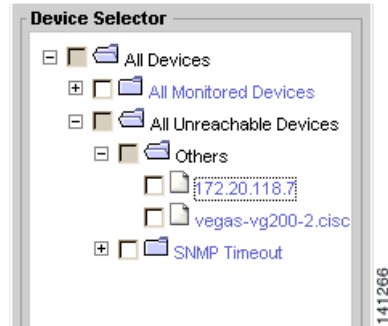


## Note

If at any time while using the View/Rediscover/Delete Devices page, you want to refresh the view, click the **Refresh** button.

The View/Rediscover/Delete Devices page contains two panes. The left pane displays a device selector, from which you select the device or group that you want to update or delete. The right pane displays the information for the selected object.

The devices that appear in the device selector are organized in folders, based on whether they are monitored by Operations Manager. The folders appear only if there is a device to go in the folder. [Figure 15-4](#) shows an example of the device selector.

**Figure 15-4** View/Rediscover/Delete Devices Selector

Under the All Devices folder, devices are placed in three possible subfolders:

- All Monitored Devices—Contains devices that are fully monitored in the Operations Manager inventory.
- All Partially Monitored Devices—Contains devices that have been successfully imported by some of the data collectors in Operations Manager.
- All Unreachable Devices—Contains devices that were not successfully imported into Operations Manager. Descriptions of the errors are displayed in the right pane, next to Error Message.

Details about, and procedures for, performing inventory collection, viewing details, or deleting devices using this page are provided in these topics:

- [Performing Inventory Collection on Devices, page 15-17](#)
- [Viewing Device Details, page 15-18](#)
- [Understanding a Device Report, page 15-19](#)
- [Deleting Devices, page 15-21](#)
- [Scheduling Inventory Collection, page 15-22](#)

## Performing Inventory Collection on Devices

Through the View/Rediscover/Delete Devices page, you can manually collect inventory on devices or device groups. When inventory collection takes place, if there are any changes to a device or group configuration, the new settings will overwrite any previous settings.



### Note

Configuration changes on a device are discovered by Operations Manager only during discovery (inventory collection) of the device. Therefore any changes to a device's configuration will not be shown by Operations Manager until the next inventory collection after the configuration change.

Inventory collection occurs only for active devices. Suspended devices do not go through inventory collection. If some of the devices you are selecting for inventory collection are suspended devices, Operations Manager displays messages indicating that only the active devices will go through inventory collection.

The following events will also trigger inventory collection:

- The entire Operations Manager inventory is polled. This is controlled by the inventory collection schedule. (See [Scheduling Inventory Collection, page 15-22](#).)
- Operations Manager is using automatic synchronization with the DCR, and a device is added, or a change is made to a device in the DCR. Such DCR changes include a device being deleted or having its credentials (IP address, SNMP credentials, MDF type) changed in the DCR.
- Operations Manager is using manual synchronization with the DCR, and a device is added to Operations Manager using the Device Management: Summary page.



**Note**

Do not confuse the Operations Manager physical discovery process (which adds devices to the DCR) or the Operations Manager inventory collection process (which probes devices and updates components in Operations Manager inventory) with the DCR synchronization process. Operations Manager inventory collection is a process that affects only the Operations Manager inventory.

- 
- Step 1** Select **Devices > Device Management > View/Rediscover/Delete**. The View/Rediscover/Delete Devices page appears.
- Step 2** Select the device or group for which you want to perform inventory collection.
- Step 3** Click **Rediscover**. Inventory collection is started.
- 

## Viewing Device Details

You can select devices and view information about them in a report. There are two ways you can generate this report:

- Through the View/Rediscover/Delete Devices page, where you can view details about particular devices that you choose. See [Using the View/Rediscover/Delete Devices Page to Generate a Device Report, page 15-19](#).
- Through the Device Management: Summary page, where you can view details about all the devices in a particular device state. See [Using the Device Management: Summary Page to Generate a Device Report, page 15-19](#).

The device report provides basic information about the device such as name, IP address, when it was added, and so on. (For a description of a device detail display, see [Understanding a Device Report, page 15-19](#).)



**Note**

If you require more detailed information about a device, use the Detailed Device View. It provides information about device components, including hardware and software information, environment, connectivity, interface components, and so on. (For a description of the Detailed Device View, see [Viewing Device Elements in Detail, page 3-77](#).)

[Figure 15-4](#) shows an example of the View/Rediscover/Delete Devices page. Devices are organized in folders according to their device state. (See [Understanding the Device Summary and Device States, page 15-7](#).)

---

### Using the View/Rediscover/Delete Devices Page to Generate a Device Report

---

- Step 1** Select **Devices > Device Management > View/Rediscover/Delete**. The View/Rediscover/Delete Devices page appears.
- Step 2** For each device for which you want to view details, in the device selector, expand the folders where the device is located.
- Step 3** Select a device by clicking the box next to it. Do this for each device for which you want to view details. If you want to view details for all of the devices in a group, click the box next to the group.
- Step 4** Click **View**.  
A report appears, listing the device information.
- 

---

### Using the Device Management: Summary Page to Generate a Device Report

---

- Step 1** Select **Devices > Device Management**. The Device Management: Summary page appears.
- Step 2** Locate the device state for which you want to view the devices.
- Step 3** In the number column that corresponds to the device state, click the number.  
A report appears, listing the device information.



---

**Note** If the number in the column is zero, you will not be able to generate a report.

---

## Understanding a Device Report

A device report displays details for the devices that you select. See [Viewing Device Details, page 15-18](#) for information on selecting devices.

[Figure 15-5](#) shows an example of a device report.

Figure 15-5 Device Report

**CISCO SYSTEMS** IP Communications Operations Manager  
User Selected Devices as of 21-Sep-2005




Showing 1 - 5 of 5 records

Device Type	Device Name	IP Address	Device Capabilities	Status	Monitored Since	Last Inventory Collection
1. Host	161.44.250.19	161.44.250.19	IPCC; IPCC Router; IPCC Logger; IPCC Peripheral Gateway; IPCC-PIM; IPCC CTI Gateway; IPCC CTI Object Server; Host; Voice and Telephony	Monitored	19-Sep-2005 16:52:16	19-Sep-2005 16:54:45
2. Host	161.44.250.78	161.44.250.78	IPCC; IPCC Peripheral Gateway; IPCC-PIM; Host; Voice and Telephony	Monitored	19-Sep-2005 16:52:17	19-Sep-2005 16:54:42
3. Router	172.20.119.107	172.20.119.107	Voice Gateway; CallManager Express; VoiceServices; IPSLA; Router; Routers	Monitored	19-Sep-2005 16:52:18	19-Sep-2005 16:57:14
4. Host	172.20.119.108	172.20.119.108	Unity Express; VoiceServices; Host; Interfaces and Modules	Monitored	19-Sep-2005 16:52:18	19-Sep-2005 16:54:13
5. Router	172.20.118.6	172.20.118.6	Voice Gateway; IPSLA; MGCP; H323; Router; Routers	Monitored	19-Sep-2005 16:52:20	19-Sep-2005 16:57:16

Rows per page: 20 Go to page: 1 of 1 Pages

Table 15-5 describes the information displayed in a device report.

Table 15-5 Device Report

Heading/Button	Description
Device Type	Device type.
Device Name	Device name. Link to the Detailed Device View for the device. Clicking the link opens a Detailed Device View for the device. See <a href="#">Understanding the Layout of the Detailed Device View, page 3-74</a> .
IP Address	Device IP address.
Device Capabilities	Functions that a device can perform; for example, switch, voice gateway, Cisco CallManager, Host, and so on.
Status	Current state the device is in.
Monitored by IPCOM Since	The time and date that inventory collection was first completed for the device.
Last Inventory Collection	The time and date that inventory collection was last completed for the device.
	Downloads the Device Details display to a file on your computer.
	Displays the report in a printer-friendly format.
	Opens the Operations Manager online help.

## Deleting Devices

The View/Rediscover/Delete Devices page allows you to delete devices from the Operations Manager inventory (local deletion). It does not affect the DCR (all DCR device management is performed from the Common Services home page).

When a device is deleted from the DCR (which can only be done from the Common Services home page), it is automatically deleted from Operations Manager, regardless of the synchronization setting. If you want to delete a duplicate device, use **Devices > Device Credentials**. This takes you directly to CiscoWorks Common Services Device Management.

When you delete a device from the Operations Manager inventory and Operations Manager is configured to use manual synchronization, the deleted device will appear on the Device Selection page, in the device selector, when the Manual radio button is selected. A deleted device will not be readded when Operations Manager inventory collection is performed. A deleted device can only be added back into Operations Manager inventory through manual import. The device can not be added using automatic import.

While a device is being deleted, Operations Manager will not allow any inventory collection, suspend operations, or resume operations to be performed on the device. When you delete a containing device, all of the contained devices are deleted.

**Note**

If you only want to suspend the managed state of a device, you do not need to delete the device from Operations Manager. You can suspend and resume the managed state of a device through the Detailed Device View page. For more details on suspending and resuming the managed state of a device, see the following:

- [Suspending/Resuming Devices, page 3-80](#)
- [Suspending/Resuming a Device Component, page 3-81](#)

**Note**

Depending upon the load that exists on the system, Operations Manager takes approximately 15 to 40 seconds to delete a device.

**Note**

Your login determines whether you can perform this operation.

- Step 1** Select **Devices > Device Management > View/Rediscover/Delete**. The View/Rediscover/Delete Devices page appears.
- Step 2** Select the device or group that you want to delete.
- Step 3** Click **Delete**.
- Step 4** In the confirmation box, click **Yes**.

## Scheduling Inventory Collection

There are separate inventory collection schedules for devices and phones. There is only one inventory collection schedule for devices. You cannot create additional schedules; you can only edit the existing schedule. For IP phones, you can create multiple inventory collection schedules.

In the Inventory Collection Schedule page (**Devices > Device Management > Device**), you can edit, suspend, or resume the device inventory collection schedule. (See [Working with the Device Inventory Collection Schedule, page 15-22](#).)

In the IP Phone Discovery Schedule page (**Devices > Device Management > IP Phone**), you can add, edit, or delete the IP phone discovery schedules. (See [Working with IP Phone Discovery, page 15-22](#).)

## Working with the Device Inventory Collection Schedule

You can perform the following tasks with the device inventory collection schedule:

- [Editing the Device Inventory Collection Schedule, page 15-22](#)
- [Suspending and Resuming the Inventory Collection Schedule, page 15-22](#)

### Editing the Device Inventory Collection Schedule

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Select <b>Devices &gt; Device Management &gt; Device</b> . The Device Inventory Collection page appears. |
| <b>Step 2</b> | Click <b>Edit</b> . The Inventory Collection Schedule: Edit page appears.                                |
| <b>Step 3</b> | Change the desired scheduling information.   |
| <b>Step 4</b> | Click <b>OK</b> .  |
| <b>Step 5</b> | Click <b>Yes</b> .   |
- 

### Suspending and Resuming the Inventory Collection Schedule

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Select <b>Devices &gt; Device Management &gt; Device</b> . The Device Inventory Collection page appears.                                 |
| <b>Step 2</b> | If the schedule is active and you want to stop it from performing inventory collection, click <b>Suspend</b> .                           |
| <b>Step 3</b> | If the schedule is not active and you want Operations Manager to perform inventory collection at a scheduled time, click <b>Resume</b> . |
- 

## Working with IP Phone Discovery

When you select **Devices > Device Management > IP Phone**, you can perform the following tasks:

- [Viewing IP Phone Collection Status](#)
- [Adding an IP Phone Discovery Schedule](#)
- [Editing an IP Phone Discovery Schedule](#)
- [Deleting an IP Phone Discovery Schedule](#)

## Viewing IP Phone Collection Status

- 
- Step 1** Select **Devices > Device Management > IP Phone**. The IP Phone Discovery Schedule page appears. The IP Phone Collection Status pane displays the following:
- Collection Status—Displays the status of the discovery process. The status could be any one of the following:
    - In progress—When you start PIFServer for the first time or restart it, discovery takes place automatically and the status appears as *In Progress*.
    - Complete—The discovery process is complete.
    - Not available. Try after some time—Appears when you start PIFServer for the first time, or restart it, and the discovery process has not yet begun.
  - Last Collection Start Time—Displays the start time of the last discovery.
  - Last Collection End Time—Displays the end time of the last discovery.
- 

## Adding an IP Phone Discovery Schedule

- 
- Step 1** Select **Devices > Device Management > IP Phone**. The IP Phone Discovery Schedule page appears.
- Step 2** Click **Add**. The Add Schedule dialog box appears.
- Step 3** Enter the following:
- A name for the discovery schedule
  - The day of the week when you want discovery to occur
  - The time of the day when you want discovery to occur
- Step 4** Click **OK**.
- 

## Editing an IP Phone Discovery Schedule

- 
- Step 1** Select **Devices > Device Management > IP Phone**. The IP Phone Discovery Schedule page appears.
- Step 2** Select the phone discovery schedule that you want to edit.
- Step 3** Click **Edit**. The Edit Discovery Schedule dialog box appears.
- Step 4** You can change the following:
- The name of the discovery schedule
  - The day of the week when you want discovery to occur
  - The time of the day when you want discovery to occur
- Step 5** Click **OK**.
- Step 6** After all your changes are done, click **Apply**.
-

## Deleting an IP Phone Discovery Schedule

- 
- Step 1** Select **Devices > Device Management > IP Phone**. The IP Phone Discovery Schedule page appears.
- Step 2** Click **Delete**.
- Step 3** In the confirmation box, click **Yes**.
- 

## Determining the Media Server Account to Use for Cisco CallManager Access

To enable Operations Manager to access a Cisco CallManager, you must supply the username and password for an account on the media server. The account to use depends upon the Cisco CallManager version and might also depend on whether multilevel administration access (MLA) is enabled for the Cisco CallManager. [Table 15-6](#) lists the options.

**Table 15-6 Username and Password for Accessing the Cisco CallManager**

Cisco CallManager Version on Media Server	MLA Enabled or Disabled for Cisco CallManager	Required Account
Earlier than 4.0	Enabled or disabled	Valid Windows 2000 administrator account on the media server.
4.0 or later	Enabled	A multilevel administration access account with either full access or read-only access to the Standard Serviceability Functional Group.
	Disabled	Valid Windows 2000 administrator account on the media server.

## Viewing Discovery Status

In Operations Manager, you can use the Device Management: Summary page to determine the discovery status of the devices that are being added. For details on accessing and understanding the Device Management: Summary page, see [Understanding the Device Summary and Device States, page 15-7](#).

## Editing SNMP Timeout and Retries

If an SNMP query does not respond in time, Operations Manager will time out. It will then retry contacting the device for as many times as listed under the `snmpretries` attribute in the configuration file. The timeout period is doubled for every subsequent retry. For example, if the timeout value is 4 seconds and the retries value is 3, Operations Manager waits for 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry.

The SNMP timeout and retries are global settings.

The default values are:

- Timeout—4 seconds
- Retries—3

- 
- Step 1** Select **Devices > Device Management > SNMP Configuration**. The SNMP Configuration page appears.
- Step 2** Select a new SNMP timeout setting.
- Step 3** Select a new Number of Retries setting.
- Step 4** Click **Apply**.
- Step 5** In the confirmation box, click **Yes**.
- 

## Configuring LDAP

- [Adding an LDAP Server, page 15-25](#)
- [Modifying LDAP Server Configuration, page 15-26](#)
- [Deleting an LDAP Server, page 15-26](#)

## Adding an LDAP Server

Operations Manager can be configured to connect to a Lightweight Directory Access Protocol (LDAP) server, so that Operations Manager can access user information stored in the LDAP server.

**Note**

---

LDAP servers that use SSL authentication are not supported by Operations Manager.

---

- 
- Step 1** Select **Devices > Device Management > LDAP Configuration**. The LDAP Server Configuration page appears.
- Step 2** Click **Add**. The Add LDAP Server page opens.
- Step 3** In the Connection Details area, do the following:
- Enter the LDAP server name or IP address.
  - Enter the port number—Port used for LDAP requests on the LDAP server.
  - If you want to use anonymous login for authentication, select the Use Anonymous Login check box.
  - Enter an admin DN—If your LDAP server requires authentication for lookups, set this to the name of a user who has permission to search the subtree specified in the search base.
  - Enter the password for the LDAP server and reconfirm the password.
  - Enter a search base—Set this parameter to the search base for LDAP lookups. This search base should include all users who must be returned from the lookup.
- Step 4** In LDAP Search Parameters, do the following:
- Enter a name for the search.

- Enter a telephone number—Enter the number as it is stored in the LDAP server.
- Enter a telephone filter—Enter the exact telephone number prefix. This enables Operations Manager to get only extension number details for each person from the LDAP server. This will be correlated with the extension number obtained from Cisco CallManager, to display the username.

**Step 5** Click **Add**.

---

## Modifying LDAP Server Configuration

**Step 1** Select **Devices > Device Management > LDAP Configuration**. The LDAP Server Configuration page appears.

**Step 2** Select the LDAP server that you want to change.

**Step 3** Click **Modify**. The Edit LDAP Server Configuration page appears.

**Step 4** In the LDAP Server Connection Details area, you can change the following:

- The LDAP server name or IP address.
- The port number—Port used for LDAP requests on the LDAP server.
- Whether to use anonymous login for authentication—Select or deselect the Use Anonymous Login check box.
- An admin DN—If your LDAP server requires authentication for lookups, set this to the name of a user who has permission to search the subtree specified in the search base.
- The password for the LDAP server—Be sure to reconfirm the password.
- A search base—Set this parameter to the search base for LDAP lookups. This search base should include all users who must be returned from the lookup.

**Step 5** In the LDAP Search Parameters area, you can change the following:

- Common name.
- Telephone number—Enter the number as it is stored in the LDAP server.
- Telephone filter—Enter the exact telephone number prefix. This enables Operations Manager to get only extension number details for each person from the LDAP server. This will be correlated with the extension number obtained from Cisco CallManager, to display the username.

**Step 6** Click **Edit**.

---

## Deleting an LDAP Server

**Step 1** Select **Devices > Device Management > LDAP Configuration**. The LDAP Server Configuration page appears.

**Step 2** Select the LDAP server that you want to delete.

**Step 3** Click **Delete**.

---

# Understanding Cisco CallManager Security Certificates

Cisco CallManager 4.1 or later supports enabling Secure Socket Layers (SSLs) on virtual directories. For secure communication between Operations Manager and Cisco CallManager:

1. On Cisco CallManager 4.1 or later, enable SSL on these virtual directories:
  - CCMApi—Operations Manager uses services in this virtual directory to perform AXL/SOAP database queries.
  - Soap—Operations Manager uses services in this virtual directory to perform AXL/SOAP device queries.



---

**Note** By default, SSL is not enabled on the CCMApi and Soap virtual directories.

---

For information on enabling SSL (using Windows Internet Information Services (IIS)), see *Cisco CallManager Security Guide* for the appropriate release of Cisco CallManager.

2. On the server where Operations Manager is installed, view and install any required Cisco CallManager security certificates. See [Viewing and Importing a Cisco CallManager Security Certificate](#), page 15-29.



---

**Note** If you do not install required security certificates, Operations Manager cannot monitor connectivity between devices and the Cisco CallManager; the Cisco CallManager remains in the Partially Monitored state.

---

3. To ensure that you maintain up-to-date security certificates on the Operations Manager server, periodically validate Cisco CallManager security certificates. Validation does the following:
  - Checks expiry dates.
  - Verifies that the security certificates stored on the server with Operations Manager are the same as those on the Cisco CallManager.

See [Validating Cisco CallManager Security Certificates](#), page 15-30.

## Managing Cisco CallManager Security Certificates

The information in this topic is applicable only for media servers running Cisco CallManager 4.1 or later. You should perform this procedure after any of the following:

- You import a media server that is running Cisco CallManager 4.1 or later.
- You enable SSL on the CCMApi or Soap virtual directory on a media server (running Cisco CallManager 4.1 or later).
- A media server running Cisco CallManager 4.1 or later goes into the Partially Monitored state.

**Step 1** Select **Devices > Device Management > Manage CCM Security Certificates**.



**Note** Operations Manager checks each Cisco CallManager media server to determine whether it requires a security certificate and checks the Operations Manager server to determine whether a certificate has been imported.

The Manage CCM Security Certificates page appears, displaying the following information.

Column	Description	Usage Notes
Cisco CallManager Media Server	Media server DNS name or IP address	—
IP Address	Media server IP address	—
Certificate Status	Not Imported—A valid certificate exists on the Cisco CallManager media server. Operations Manager requires the certificate.	You must import the certificate.
	Imported—The certificate has been imported into Operations Manager; whether the certificate is valid is not yet known.	To validate the certificate, you can: <ul style="list-style-type: none"> <li>View the certificate; when you do so, Operations Manager updates the certificate status.</li> <li>Validate all certificates.</li> </ul>
	Not Required—The Cisco CallManager is not using HTTPS.	—
	Validated—The certificate has been imported into Operations Manager and matches the valid certificate on the Cisco CallManager media server. <b>Note</b> This status is displayed only immediately after you view, import, or validate certificates.	You can: <ul style="list-style-type: none"> <li>Validate the certificate again.</li> <li>View the certificate (however, you cannot import it again).</li> </ul>

Column	Description	Usage Notes
Certificate Status (continued)	No Longer Valid—The certificate on the Operations Manager server does not match the current, valid certificate in Cisco CallManager.  <b>Note</b> This status is displayed only immediately after you view or validate certificates.	You must import the certificate.
	Not Validated—An error occurred; for example, the Cisco CallManager is not responding or the certificate in the Cisco CallManager has expired.	See the error messages that are displayed and take steps to correct the problem.

From this page, you can view, import, and validate security certificates.

## Viewing and Importing a Cisco CallManager Security Certificate



### Note

The following information is applicable for media servers running Cisco CallManager 4.1 or later.

Use this procedure to update and view the security certificate status for a Cisco CallManager media server and to import the certificate. (To update the security certificate status for all Cisco CallManager media servers, see [Validating Cisco CallManager Security Certificates, page 15-30](#).)

**Step 1** Select **Devices > Device Management > Manage CCM Security Certificates**. The Manage CCM Security Certificates page appears.

**Step 2** Select a media server and click **View Certificate**.



### Note

If the certificate status is Not Required, the radio button for the media server is grayed out. For a description of each certificate status, see [Managing Cisco CallManager Security Certificates, page 15-27](#).

Operations Manager validates the security certificate. One of the following appears:

- An error dialog box—Displays validation errors.
- The View Security Certificate on Cisco CallManager Media Server page—Displays updated certificate details obtained from the Cisco CallManager media server.

**Step 3** If an error dialog box is displayed, click **OK** and take steps to resolve the problem; see [Responding to Errors While Viewing or Validating Certificates, page 15-31](#).

**Step 4** If the View Security Certificate on Cisco CallManager Media Server page is displayed:

- If the certificate status is Not Validated, the certificate on the Cisco CallManager has expired. See user documentation for the Cisco CallManager for information on how to manage security certificates.

- If you want to view the public key and signature, click the View link for:
  - Public Key—Opens the Public Key for Security Certificate: *media server name* window. Click **Close** to close this window.
  - Signature—Opens the Signature for Security Certificate: *media server name* window. Click **Close** to close this window.
- If you can install the certificate, click **Import Certificate**.



**Note** The Import Certificate button is grayed out if the certificate cannot be imported. This is the case when the certificate status is Validated or Not Validated.

The Manage CCM Security Certificates page appears, displaying updated information.



**Note** Installing a security certificate from a Cisco CallManager on the server where Operations Manager resides enables communication between Operations Manager on the same server and all virtual directories in the Cisco CallManager.

## Validating Cisco CallManager Security Certificates



**Note** The following information is applicable for media servers running Cisco CallManager 4.1 or later.

Use this procedure to update the certificate status for all media servers displayed on the Manage CCM Security Certificates page.

- Step 1** Select **Devices > Device Management > Manage CCM Security Certificates**. The Manage CCM Security Certificates page appears.
- Step 2** Click **Validate Certificates**.



**Note** Validation is performed for all Cisco CallManager media servers. You do not need to select any Cisco CallManager media servers.

One of the following appears:

- Information dialog box—Displays a message that indicates certificate validation was successful for all Cisco CallManager media servers.
- Error dialog box—Lists Cisco CallManager media servers and errors that occurred while validating certificates.

- Step 3** Click **OK**. The Manage CCM Security Certificates page appears with updated certificate status.
- Step 4** If errors occurred, see [Responding to Errors While Viewing or Validating Certificates, page 15-31](#).

## Responding to Errors While Viewing or Validating Certificates


**Note**

The following information is applicable for media servers running Cisco CallManager 4.1 or later.

[Table 15-7](#) lists errors that might occur while managing Cisco CallManager security certificates and suggests how to respond to them.

**Table 15-7** *Cisco CallManager Security Certificate Errors*

Errors	What to do
Cisco CallManager not responding—Cisco CallManager or HTTP server might be down or unreachable.	<ol style="list-style-type: none"> <li>1. Verify network reachability.</li> <li>2. Make sure that Cisco CallManager and the HTTP server process are running.</li> <li>3. Try to view, import, or validate the certificate again.</li> </ol>
<ul style="list-style-type: none"> <li>• Certificate required, but missing in Cisco CallManager.</li> <li>• Security certificate on the Cisco CallManager media server has expired.</li> </ul>	See user documentation for the Cisco CallManager for information on how to manage security certificates on the Cisco CallManager.
Certificate not required—HTTPS has been disabled in Cisco CallManager.	Refresh the page by clicking Manage CCM Security Certificates; the certificate status should be Not Required.
A general error occurred while reading the certificate from Cisco CallManager.	See the DeviceManagement.log file on the Operations Manager server for more details.

