CHAPTER 3

Getting Started

This section instructs you to set up Cisco Unified Operations Manager (Operations Manager) and view diagnostic results. It includes:

Timesaver

To view the online video tutorials for Operations Manager, click on the E-Learning icon in the Online help.

Configuring Operations Manager to Monitor Devices

Operations Manager obtains devices to monitor from the CiscoWorks Device and Credentials Repository (DCR). The DCR is a common repository of devices and their credentials for use by individual applications.

This section contains:

- Verifying Devices Added to Operations Manager
- Scheduling Inventory Collection
- Troubleshooting Device Import and Inventory Collection
- Editing Device Configuration and Credentials
- Modifying SNMP Timeout and Retries
- Performing Manual Inventory Collection on Devices

For Operations Manager to monitor a device, it must first be added to the DCR. After a device is added to the DCR, you can then add it to the Operations Manager inventory, which is separate from the DCR.

Note When Operations Manager is installed, it will automatically synchronize with the DCR and add inventory. This is the default setting.

You can add devices automatically from the DCR to Operations Manager by activating automatic synchronization (the default), or you can add them manually through the Device Selection page. For more information on how Operations Manager is affected by the DCR, see Understanding the DCR, page 3-3.

You should exclude the *NMSROOT* directory from virus scanning. Problems can arise if files are locked because of virus scanning.

NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it is C:\PROGRA~1\CSCOpx.

Table 3-1 lists some possible deployment scenarios for Operations Manager, and what you will need to do to add devices to Operations Manager inventory.

Table 3-1 Adding Devices to Inventory Scenarios

Deployment Scenario	What to Do
• Deploying Operations Manager as an independent server. • Automatically synchronizing your inventory with the DCR.	Add devices from the DCR using automatic synchronization. Automatic synchronization is the default setting.[1] If you have changed the synchronization setting from automatic, you will need to change it back. See Configuring Automatic Device Selection in Operations Manager, page 3-10.
• Deploying Operations Manager as an independent server. • Manually controlling the devices that are added to inventory.	Manually add devices from the DCR. See Adding Devices Manually from the DCR to Operations Manager, page 3-10.
• Deploying Operations Manager as an independent server. • You want to use automatic discovery, but not all the devices discovered through automatic discovery need to be managed in Operations Manager.	• Add devices from the DCR using automatic synchronization.[1] • Configure automatic synchronization to select devices based on parameters that you set. See Configuring Automatic Device Selection in Operations Manager, page 3-10.

Table 3-1 Adding Devices to Inventory Scenarios (continued)

Deployment Scenario	What to Do
• Deploying Operations Manager with CiscoWorks LAN Management Solution (LMS). • Using the Operations Manager DCR as the master DCR. • Automatically synchronizing your inventory with the DCR.	• Set up the Operations Manager DCR as a master and the LMS DCRs as slaves. Configuring the DCR in Master and Slave Mode, page 3-4. • Run physical discovery. See Adding Devices to the DCR, page 3-5 • Verify that automatic synchronization is configured in Operations Manager. See Configuring Automatic Device Selection in Operations Manager, page 3-10.
• Deploying Operations Manager with LMS. • Synchronizing the Operations Manager DCR with an existing master DCR. • Automatically synchronizing your inventory with the DCR.	• Set up the Operations Manager server DCR as a slave and one of the LMS DCRs as a master. Configuring the DCR in Master and Slave Mode, page 3-4. • Configure Operations Manager to add devices to a master DCR. See Adding Devices to the DCR, page 3-5. • Run physical discovery. See Adding Devices to the DCR, page 3-5 • Verify that automatic synchronization is configured in Operations Manager. See Configuring Automatic Device Selection in Operations Manager, page 3-10.
• Deploying Operations Manager with LMS. • Synchronizing the Operations Manager with an existing master DCR. • Manually controlling the devices managed by Operations Manager.	• Set up the Operations Manager server DCR and the LMS server DCRs as slave and master. Configuring the DCR in Master and Slave Mode, page 3-4. • Configure Operations Manager to add devices to a master DCR. See Adding Devices to the DCR, page 3-5. • Run physical discovery. See Adding Devices to the DCR, page 3-5 • Verify that manual synchronization is configured in Operations Manager. See Configuring Automatic Device Selection in Operations Manager, page 3-10.

1. Ensure you have set up device credentials for your network devices.

Understanding the DCR

The Device and Credentials Repository (DCR) is a centralized device repository for sharing device information across applications. It provides a single place for managing device credentials and attributes. This ensures 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 applications that support the DCR, such as Operations Manager and LMS applications. (Service Monitor and Service Statistics Manager neither use nor support the DCR.)

Note A device must be added to the DCR before it can be added to the Operations Manager inventory (see Adding Devices to the DCR, page 3-5).

After 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 the IP address. When the device is added to Operations Manager, Operations Manager maps the DCR ID to the device name during inventory collection.

Operations Manager also uses the DCR ID to verify whether 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 name as the device name—is provided in *Cisco Unified Operations Manager User Guide 8.5* or the Online help.

You can add devices automatically from the DCR to Operations Manager by activating automatic synchronization (which is the default), or you can add them selectively by deactivating using the Device Selection page.

When a device is deleted it may or may not be deleted from the DCR. Deletion is determined by how Operations Manager is configured with the DCR (for details on deleting devices, see *Cisco Unified Operations Manager User Guide 8.5* or the Online help).

The synchronization between the DCR and the Operations Manager inventory is controlled from the Device Selection page.

- For automatic synchronization (this is the default), see Configuring Automatic Device Selection in Operations Manager, page 3-10.
- For manual synchronization (in which you selectively add devices from the DCR to the Operations Manager inventory), see Adding Devices Manually from the DCR to Operations Manager, page 3-10.

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.

Configuring the DCR in Master and Slave Mode

By default, the DCR on the Operations Manager server is configured as a standalone or independent repository. If you decide to configure the DCR for Operations Manager as a master or a slave, the procedures for doing so are given in the CiscoWorks Online help.

To access the CiscoWorks Online help, from the Operations Manager home page, select **Administration** and select any link under a (CiscoWorks/Common Services) heading. A new window opens; click the Help link.

Ensure that the versions of Operations Manager and CiscoWorks are compatible before configuring the master and slave mode. See the *Supported and Interoperable Devices and Software Table for Cisco Unified Operations Manager 8.0* for compatibility information.

You must perform prerequisite tasks and you must configure the master and the slave in the proper order. The following procedure can help you get started and locate the information you need in the Online help.

Note To start Operations Manager, see Starting Operations Manager, page 3-20.

To configure the DCR in Master and Slave modes:

Step 1 Choose **Administration > Device and Credentials (Common Services > Administration**.

A Common Services window opens.

Step 2 Click the **Mode Settings** link in the left pane.

The Mode Settings window appears.

Step 3 Click the Help link in the top right corner of the page. Find the instructions for completing the master-slave configuration prerequisites. These include:

- Adding a peer server user on the system with the master DCR.
- Creating a System Identity User on the system with the slave DCR.
- Copying security certificates.

Step 4 Follow the instructions in the Online help to complete the prerequisites and to configure a master and a slave in the correct order.

Adding Devices to the DCR

Devices are added to the DCR through the Operations Manager Add Devices page (**Administration > Device Management > Device Configuration > Add Devices**).

This section contains:

- Configuring Operations Manager Physical Discovery
- Configuring Credentials
- Filtering Operations Manager Physical Discovery

Note To add devices to the DCR using bulk import (importing from an NMS or from a file), see Importing Devices Into the DCR, page 3-9.

Step 1 Choose **Administration > Device Management > Device Configuration > Add Devices**.

The Add Devices page appears.

Step 2 Enter the following:

- IP address or hostname. Multiple devices can be entered at the same time, using a comma-separated list. Ensure the device hostname is DNS resolvable. While adding multiple devices together, all devices must be of the same type and use the same credentials.
- Enter SNMPv2c/SNMPv1 credentials.
- Enter SNMPv3 credentials.
- Enter HTTP credentials (required only for Cisco Unified Communications Manager).
- Windows credentials (required only for Windows-based MCS application servers).

Step 3 Click **OK**.

Configuring Operations Manager Physical Discovery

To configure Operations Manager physical discovery:

Step 1 Choose **Devices > Device Management > Auto-Discovery Configuration**.

The Auto-Discovery Configuration page appears.

You can also access the Discovery Configuration page from the Device Management: Summary page, by clicking the Configure button.

Discovery requires SNMP and/or SNMPv3 credentials.

If the credentials are not configured, when you click **Discovery Configuration**, a blank Discovery Configuration page appears and you have the option of configuring credentials.

a. Select the **Credentials** radio button.

b. Click **Add.**

The Configure Credentials page appears (see Configuring Credentials, page 3-7).

If the Discovery radio button is not selected, select it.

Step 2 Do one of the following:

- Select the **Use Communications Manager or Cisco Discovery Protocol (CDP)** check box, and do one of the following:
  - Enter seed devices using a comma-separated list of IP addresses.

    When using a Cisco Unified Communications Manager as the seed device, the following types of devices are discovered:

    - Other Cisco Unified Communications Managers in the network
    - Cisco Unity
    - MGCP Voice Gateways
    - H.323 Voice Gateways
    - Gatekeepers

    In addition to the Cisco Unified Communications Manager-based discovery, the following types of discoveries occur, resulting in additional devices being added to the inventory:

    - CDP-based discovery
    - ARP-based discovery
    - Route table-based discovery
  - Select the **Use devices currently in the system** check box.
  - Select a hop count.

  Discovery may skip more than the number of hops selected. Discovery uses multiple technologies to discover devices, which may result in devices violating L2 or L3 hops.

  If you are using Hop count to limit discovery, an alternate way of achieving the same objective is to use the Include and Exclude filters from the Discovery Configuration page (see Filtering Operations Manager Physical Discovery, page 3-8).

or

- Select the **Use ping sweep check box**. The seed devices and the ping sweep options can be used in an either/or mode.

  When you select the Use Ping Sweep check box, 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.

Step 3 In the Run pane, configure when physical discovery should run.

- If you want physical discovery to run immediately, select the **now** radio button.
- If you want to schedule physical discovery to run at certain intervals, do either of the following:
  - Select **daily**. Enter the time and select the days on which physical discovery should run.
  - Select the **every** radio button. Choose how often you want physical discovery to run, enter the times between which you want it to run, and select the day on which it should run.

Step 4 Click **OK**.

Configuring Credentials

Discovery requires SNMP and/or SNMPv3 credentials. If the credentials are not configured when you try to configure discovery, you will only be able to access the Configure Credentials page. You must enter SNMP and/or SNMPv3 credentials before running discovery.

Step 1 Choose Devices **> Device Management > Auto-Discovery Configuration > Credentials**.

The Configure Credentials page appears.

Step 2 Click **Add**.

If you are changing the existing credentials for a device, select the target device and then click **Edit**. This Edit option allows you to change only the credentials. If you want to change the target device, you must delete the entire row and then re-add all the details.

Step 3 Enter the following:

- IP address or hostname. Multiple devices can be entered at the same time, using a comma-separated list.

  When you add multiple devices at the same time, all the devices must be the same type of device and use the same credentials. If you are using wildcard entries, only the following formats are supported: *.*.*.* or 10.76.93.[39-43].
- (Optional) Change the SNMP timeout and retries.
- SNMPv2c/SNMPv1 credentials.
- SNMPv3 credentials.
- HTTP credentials (only required for Cisco Unified Communications Manager).
- Windows credentials (only required for Windows-based MCS application servers).

Step 4 Click **OK**.

Filtering Operations Manager Physical Discovery

You can configure Operations Manager physical discovery to filter out devices. This is optional; it is not required to run physical discovery.

Step 1 Choose Devices **> Device Management > Auto-Discovery Configuration > Filters and Schedule**.

The Filters and Schedule page appears.

Step 2 Select the **Filters** radio button. Table 3-2 describes the optional filters that are available to you when running physical discovery.

Table 3-2 Physical Discovery Filters

Filter	Description
IP Address	(Optional) Enter comma-separated IP addresses or IP address ranges for devices that you want to: • Include—In the auto-discovery process. • Exclude—From the auto-discovery process. You can use wildcards when specifying the IP address range. An asterisk (*) denotes the octet range of 1-255. Also, the octet range can be constrained using the [xxx-yyy] notation. For example: • To include all devices in the 172.20.57/24 subnet in the auto-discovery process, enter an Include filter of 172.20.57.*. • 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]. 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. After 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.

Table 3-2 Physical Discovery Filters (continued)

Filter	Description
Domain	(Optional) Enter comma-separated domain names for devices that you want to: • Include—In auto-discovery processing. • Exclude—From auto-discovery processing. The 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. For example: • **.cisco.com* matches any name ending with *.cisco.com.* • **.?abc.com* matches any name ending with *.aabc.com*, *.babc.com*, and so on.
SysLocation	(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: • Include—In auto-discovery processing. • Exclude—From auto-discovery processing. 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 *San* * will match all SysLocation strings starting with *San Francisco*, *San Jose*, etc.

Step 3 Click **Apply**.

Importing Devices Into the DCR

For bulk import (from an NMS or from a file) Operations Manager provides you a direct link to the DCR (**Device Management > Device Configuration > > Import Devices**).

Step 1 Choose **Administration > Device Management > Device Configuration > Import Devices**.

The Common Services Import Devices page appears.

Step 2 Enter the import information.

If you need help importing, click the Help button on the page, and the CiscoWorks Online help opens.

Configuring Automatic Device Selection in Operations Manager

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

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

Note Devices must exist in the DCR before you can add them to Operations Manager.

To configure automatic device selection:

Step 1 Choose **Administration > Device Management > Device Configuration > DCR Device Selection**.

The Device Selection page appears.

Step 2 Activate the Automatic radio button.

Step 3 Click **Apply**.

Operations Manager is synchronized with the DCR. Any DCR devices currently not in Operations Manager are added. Operations Manager performs inventory collection for the new devices that are being added.

Step 4 Verify whether any duplicate devices exist, by selecting **Administration > Device Management > Device Configuration > IP Address Report**.

If you do not require the duplicate device for your deployment, remove it (for information on deleting devices, see *Cisco Unified Operations Manager User Guide* 8.5 or the Online help).

Adding Devices Manually from the DCR to Operations Manager

If Operations Manager is configured for automatic device selection, you do not need to perform this procedure. With manual device selection, you need to manually select devices to monitor. You need to do this periodically after devices have been added to the DCR.

For example, if you run Operations Manager physical discovery on a weekly basis, you should consider checking for new devices that you want to monitor after discovery completes.

Note Devices must exist in the DCR before you can add them to Operations Manager.

To add devices manually:

Step 1 Choose **Administration > Device Management > Device Configuration > DCR Device Selection**.

The Device Selection page appears.

Step 2 Select the Manual radio button.

All devices that are not in Operations Manager inventory are available through the device selector.

Step 3 Select devices the following ways:

- Entering device names or IP addresses in the Device Display Name, and clicking **Filter**.
- Using the group selector.

If you want to see the devices you have selected, click the **Selection** tab, and a list of devices appears.

Step 4 Click **Select**.

Operations Manager performs inventory collection on the devices that are being added.

Step 5 Verify whether any duplicate devices exist, by choosing **Administration > Device Management > Device Configuration > IP Address Report**.

If you do not require the duplicate device for your deployment, remove it (for information on deleting devices, see *Cisco Unified Operations Manager User Guide* 8.5 or the Online help).

For more information, see *Cisco Unified Operations Manager User Guide* 8.5.

Understanding 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 choose **Devices > Device Management**.

Table 3-3 Device States

State	Description
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[1] in Operations Manager, but not all. If a device is in this state, you should 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 Troubleshooting Device Import and Inventory Collection, page 3-13.
Unsupported	The device is not supported by Operations Manager.

1.Table 3-4 displays the states that devices go through while they are being added to Operations Manager inventory, and explains what causes a device to go into a particular device state.

Table 3-4 Transition States of Devices when Being Added to Inventory

Start Inventory Collection	Result of Inventory Collection	Resulting Device State
Inventory collection in progress.	Successfully discovered.	Monitored.
Inventory collection in progress.	Not all credentials were supplied or some services were down.	Partially Monitored.
Inventory collection in progress.	• SNMP information is not configured. • Device is not responding. • Device is not reachable. • Device credentials are not correct.	Unreachable.
Inventory collection in progress.	• The device model is not recognized. • The software version is not supported.	Unsupported

Verifying Devices Added to Operations Manager

You can verify that your devices have been added to Operations Manager inventory by checking whether they are in the Monitored state on the Device Summary. To verify devices:

Step 1 Choose **Administration > Device Management >Device Summary**.

Step 2 Locate your devices and check whether they are in the Monitored state.

If you find that problems have occurred during inventory collection, see Troubleshooting Device Import and Inventory Collection, page 3-13. For more information, see *Cisco Unified Operations Manager User Guide* 8.5 or the Operations Manager Online help.

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.

On the Inventory Collection Schedule page (**Administration > Device Management > > Inventory Collection > Device**), you can edit, suspend, or resume the device inventory collection schedule. (See Editing the Device Inventory Collection Schedule, page 3-13.)

On the IP Phone Discovery Schedule page (**Devices > Device Management > Inventory Collection > IP Phone**), you can add, edit, or delete the IP Phone discovery schedules. (See Adding a Phone Discovery Schedule, page 3-13.)

Editing the Device Inventory Collection Schedule

To edit the Device Inventory Collection Schedule:

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

The Device Inventory Collection page appears.

Step 2 Click **Edit**.

The Inventory Collection Schedule: Edit page appears.

Step 3 Change the desired scheduling information.

Step 4 Click **OK**.

Step 5 Click **Yes**.

Adding a Phone Discovery Schedule

To add a Phone Discovery schedule

Step 1 Choose **Devices > Device Management > Inventory Collection > IP Phone Details**.

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**.

Troubleshooting Device Import and Inventory Collection

Problems might occur during physical discovery (Operations Manager adds devices to the DCR) and can also occur during inventory collection (Operations Manager adds devices to its inventory for monitoring).

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 prevent 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.

This section contains:

- Understanding Inventory Collection Messages
- Devices in a Partially Monitored State
- Devices in Unreachable States

To troubleshoot device inventory collection, try the following:

- If a device is not responding, confirm all device credentials and re-add the device. See Editing Device Configuration and Credentials, page 3-18.
- If device inventory collection times out for several devices, increase SNMP timeout settings. See Modifying SNMP Timeout and Retries, page 3-18.
- View device error information on the Modify/Delete Device page. See Performing Manual Inventory Collection on Devices, page 3-19.
- Verify that the device is operational during the import and that it supports MIB II.
- Verify that the device is resolvable in DNS. See Verifying Cisco Unified Communications Manager DNS Settings, page 3-32.
- Check the reason for devices being in the Unreachable state. See Starting Operations Manager, page 3-20.
- After troubleshooting the problem, check the device status. See Verifying Devices Added to Operations Manager, page 3-12.

The Modify/Delete Devices page displays device information and data collection information. You can use Modify/Delete Devices to determine the current state of a device and view data collection errors.

Step 1 Choose **Administration > Device Management > Device Configuration > Modify/Delete Devices**.

The Modify/Delete Devices page opens.

Step 2 Expand the folder that contains your device (according to its inventory collection status See Verifying Devices Added to Operations Manager, page 3-12).

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 (see Starting Operations Manager, page 3-20).

Step 5 Perform the required actions to clear the error.

Understanding Inventory Collection Messages

Table 3-5 lists messages that might be shown for devices that are in the Unreachable state.

Table 3-5 Inventory Collection Error Messages

Message	Meaning	Action
SNMP Timeout	The device is in the Unreachable state because the SNMP read-only community string for the device is incorrect.	See Editing Device Configuration and Credentials, page 3-18 to enter the correct read community string for the device.
Others: Missing IP Address or Data Collector Timeout	The device is in the Unreachable state because of some other reason. The resolution for the device may have failed or the data collector timed out.	Click the device on the Modify/Delete Devices page. The error message displays the exact problem. • If the IP address is missing: – Readd the device with the correct IP address. or – Make sure that Operations Manager can resolve the device name: try adding the domain name as part of the device name. • If the data collector times out, restart the daemon manager to get all data collectors synchronized.

Devices in a Partially Monitored State

Table 3-6 explains the possible reasons for the error codes that you see in the Modify/Delete Devices page, that occur for partially monitored devices.

Why Cisco Unified Communications Manager May Go into the Partially Monitored State

- If the incorrect HTTP credentials were entered for a Cisco Unified Communications Manager, it may go into the Partially Monitored state. When this occurs none of the Perfmon Counters are polled. To change device credentials, see Editing Device Configuration and Credentials, page 3-18.
- If ports 135, 145, and 1025-65000 are not open in a firewall setup, Cisco Unified Communications Manager goes into the Partially Monitored state. Verify that these ports are open. If you need to open the ports, after doing so, rediscover the device.

Why Certain Voice Applications May Go into the Partially Monitored State

The following devices may go into the Partially Monitored state:

- Cisco IP Contact Center
- Cisco Unity Connection
- Cisco Unity
- Cisco Personal Assistant

If insufficient credentials are provided during the addition of these devices, they become partially monitored, and some of their WMI attributes are not polled. To change device credentials, see Editing Device Configuration and Credentials, page 3-18.

Table 3-6 Error Shown on the Modify/Delete Devices Page

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = CCM Authentication Failure Error Message = Success:WrongCredentials	Either Unified Communications Manager http credentials are not entered or the credentials provided are incorrect.	Verify that you provided the correct http credentials in the DCR by using the credentials to log in to the Unified Communications Manager Admin page, and rediscover the device.
Error Code= CCM Authentication Failure Error Message= Success:UnknownCredential Error	SNMP management MIBs are not responding. The MIBs and their associated errors could be one of the following: • MIB-2—The ipAddressTable is not responding. • CISCO-CCM-MIB—The ccmTable is not responding. Specifically the ccmClusterId attribute is not responding. • Inventory collection could not find the ccmVersion detail. This may be because the ccmVersion attribute in the CISCO-CCM-MIB is not responding.	Restart the SNMP Agent on the system and rediscover the device.

Table 3-6 Error Shown on the Modify/Delete Devices Page (continued)

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = CCM Authentication Failure Error Message = Success:WebServiceDown	HTTP service is not running or responding to requests from Operations Manager.	Verify that the web server is running by launching the Unified Communications Manager Admin page. Check the firewall to see if it is blocking the HTTP/HTTPS connection between Unified Communications Manager and Operations Manager.

Error Code = CCM Authentication Failure
Error Message = Success: HTTPSCertificateNotImported
	Unified Communications Manager certificate has failed.	Do the following:
		1. Check the file IPToHostName.txt in the CSCOpx\lib\jre\lib\security folder. It should contain an entry like the following:
		`deviceip>=<hostname> record for each of the ccm For e.g. 10.76.91.115=blrsd1`
		2. Go to the keytool utility location *NMSROOT*\CSCOpx\lib\jre\bin.
		3. Run the following command:
		`keytool -list -keystore <NMSROOT>\CSCOpx\lib\jre\lib\security\cacerts`
		The downloaded certificates are displayed.
		4. Verify that there is an entry similar to the following for the Cisco Unified Communications Manager:
		`Certificate fingerprint (MD5): AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4 cn=ct-sd, ou=nmtg, o=cisco systems, l=bangalore, st=Karnataka, c=in, Oct 26, 200 5, trustedCertEntry`
		5. Rediscover the device.

Devices in Unreachable States

Devices may go into the Unreachable state due to the following reasons:

- SNMP timeout
- Data collector timeout

If an SNMP timeout occurs, verify the SNMP access credentials provided during discovery.

If a data collector timeout occurs, verify that the SNMP management interface is not a serial or a generic interface (such as Frame Relay with the subnet mask 255.255.255.252). You should always access SNMP details using an Ethernet interface.

Editing Device Configuration and Credentials

After you add devices, you can change their configuration as follows. To edit device configuration and credentials:

Step 1 Choose **Administration > Device Management > Device Configuration > Device Credentials**.

The Common Services Device Summary page opens.

Step 2 Expand the folder that contains your devices.

Step 3 Select the device or device group that you want to update.

Step 4 Click **Edit Credentials**.

The Edit Device Configuration: Change Credentials page appears.

- If you select a single device, all the existing credentials for that device are populated in the Edit Device Configuration: Change Credentials page (asterisks populate the field).
- If you select multiple devices, only a comma-separated list of IP addresses is displayed.

  The auto-populated credentials (asterisks) do not reflect the actual credentials; they only indicate that credentials are available.

Step 5 You can update the following credentials:

- SNMPv2c/SNMPv1
- SNMPv3
- HTTP
- WMI

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.

Step 6 Click **OK**.

Modifying SNMP Timeout and Retries

If an SNMP query does not respond in time, Operations Manager times out. Operations Manager retries contacting the device for as many times as you indicate. The timeout period is doubled for every subsequent retry.

For example, if the timeout value is 4 seconds and the retries value is 3 seconds, Operations Manager waits 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry.

The SNMP timeout and retry values are global settings. Change these values as follows:

Step 1 Choose **Devices > Device Management > Inventory Collection > SNMP Configuration**.

The SNMP Configuration page appears.

Step 2 Select a new SNMP timeout setting. The default is 4 seconds.

Step 3 Select a new Number of Retries setting. The default is 3 retries.

Step 4 Click **Apply**.

Step 5 Click **Yes** to confirm.

Performing Manual Inventory Collection on Devices

Through the Modify/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 are not 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 select for inventory collection are suspended devices, Operations Manager displays messages that only active devices will go through inventory collection.

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.

The following events also trigger inventory collection:

- The entire Operations Manager inventory is polled. This is controlled by the inventory collection schedule. (See Scheduling Inventory Collection, page 3-12.)
- Operations Manager uses 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.
- Operations Manager uses manual synchronization with the DCR, and a device is added to Operations Manager using the Device Selection page.

If you are using the ACS login module, the System Identity user that is configured in ACS should have permission to run all job management-related tasks in Common Services and the rediscovery task in Operations Manager. You must know the ACS administrator HTTP credentials to register the Operations Manager server with the ACS server.

When rediscovery occurs, all devices in the system are discovered. Therefore, this task should be made available only to the person who has access to all devices in the network.

Step 1 Choose **Administration > Device Management > Device Configuration > Modify/Delete Devices**.

The Modify/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.

Starting Operations Manager

You can access Operations Manager from either the Operations Manager server or a client system.

- If a client system is available, we recommend that you perform all configuration and day-to-day activities from the client system. If a client system is not available, the Operations Manager server must also meet all the system requirements for a client system (for client system requirements, see Table 1-5).
- Disable any popup blocker utility that is installed on your client system before launching Operations Manager.
- By default, SSL is not enabled in Common Services. If you upgraded to Operations Manager 8.5 and SSL was enabled before the upgrade, it remains enabled after the upgrade.

Starting Operations Manager on a Client System

In Internet Explorer, enter the Operations Manager server's IP Address or name followed by the port number 1741. For example, http://*om_server name*:1741.

Starting Operations Manager on the Operations Manager Server

From the Windows desktop, choose **Start > All Programs > Cisco Unified Operations Manager > Cisco Unified Operations Manager**.

Note If Enhanced Security is enabled on the Windows 2003 or Windows 2008 system, you must add the Operations Manager home page to the Internet Explorer Trusted Sites Zone. You will not be able to access the Cisco Unified Operations Manager home page until it is added to the trusted sites.

Adding the Operations Manager Home Page to the Internet Explorer Trusted Site Zone

If Enhanced Security is enabled on the Windows 2003 or Windows 2008 system, you must perform the following procedure before you can access the Operations Manager home page.

To add the Operations Manager home page:

Step 1 Open Operations Manager and choose **Start > All Programs > Cisco Unified Operations Manager > Cisco Unified Operations Manager**.

Step 2 From the File menu, select **Add this site to**.

Step 3 Click **Trusted Sites Zone**.

Step 4 In the **Trusted Sites** dialog box, click **Add** to move the site to the list.

Step 5 Click **Close**.

Step 6 Refresh the page to view the site from its new zone.

Step 7 Check the Status bar of the browser to confirm that the site is in the **Trusted Sites Zone**.

Adding Cisco Unified Communications Management Server Links from Operations Manager

Use this procedure to add a link to a locally installed or remotely installed Service Monitor server from Operations Manager. For important details about Service Monitor event and trap processing, as well as licensing, see the Online help or the *Cisco Unified Operations Manager User Guide* 8.5.

You can also link to Provisioning Manager and Service Statistics Manager servers. See the Operations Manager Online help or the *Cisco Unified Operations Manager User Guide* 8.5 for instructions.

To add a link to a Service Monitor server:

Step 1 Choose **Administration > UC Management Suite > Service Monitor**.

The Service Monitor page appears.

Step 2 Click **Add**.

The Add Service Monitor page appears.

Step 3 Enter data in the following fields:

- IP Address—IP address of a remote server where Service Monitor is installed.
- Protocol—HTTP or HTTPS.
- Port—Port by which Service Monitor is accessed. Cannot be left blank.
- Status—Selection for whether to use this Service Monitor as a cross-launch server.
- Remarks—Optional.

Step 4 Click **Add**.

The Service Monitor page appears, displaying information for the newly added Service Monitor.

Understanding and Configuring Security

Operations Manager supports the following security-related mechanisms:

- SNMPv3 protocol (Authentication/No-Privacy option)—Operations Manager supports the Authentication/No-Privacy option between the server and the device.
- Local security or Cisco Secure ACS—Access to tasks within Operations Manager is either controlled by local security (Common Services Local Login Module) or Cisco Secure ACS. Local security is enabled on the server by default.

  Operations Manager supports integration with Cisco Secure ACS. For more information, see Security Configuration with Cisco Secure ACS, page C-1.
- SSL—Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys. (SSL is not enabled in Common Services by default.)

  You can enable or disable SSL depending on the need to use secure access. Operations Manager supports SSL between clients and the server.

To get started with configuring security, see the Setting Up Security topic in the Common Services help.

Supported NMS Integration

Operations Manager supports integration with network management systems (NMS) that reside on your network. Operations Manager does not support an NMS residing on the same system as Operations Manager.

- Operations Manager listens for traps from managed devices on port 162 (the default). If your network devices are already sending traps to another management application, configure that application to forward traps to Operations Manager.
- Operations Manager forwards traps to destinations that you specify, as follows:
  - To forward pass-through traps, see Configuring SNMP Trap Receiving and Forwarding, page 3-22.
  - To forward processed traps, see "Managing SNMP Trap Notifications" in the "Using Notification Services" chapter of *Cisco Unified Operations Manager User Guide* 8.5.

  For more information on pass-through and processed traps, see the appendix "Processed and Pass-through Traps, and Other Unidentified Traps and Events" in *Cisco Unified Operations Manager User Guide* 8.5.

Configuring SNMP Trap Receiving and Forwarding

Operations Manager can receive traps on any available port and forward them to a list of devices and ports. This capability enables Operations Manager to easily work with other trap processing applications.

However, you must enable SNMP on your devices and configure SNMP to send traps either directly to Operations Manager or to one of the following:

- An NMS
- A trap daemon

This section contains:

To send traps directly to Operations Manager, perform the tasks in Enabling Devices to Send Traps to Operations Manager, page 3-23.

To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in Integrating Operations Manager Trap Receiving with NMS or Trap Daemons, page 3-24.

Updating the SNMP Trap Receiving Port

By default, Operations Manager receives SNMP traps on port 162. If you need to change the port, you can do so.

To update the SNMP trap receiving port:

Step 1 Choose **Administration > System Settings > Miscellaneous >Preferences**.

The System Preferences page appears.

Step 2 In the Trap Receiving Port field, enter the port number.

Step 3 Click **Apply**.

For a list of ports that Operations Manager uses, see Verifying TCP and UDP Ports that Operations Manager Uses, page 2-8.

Enabling Devices to Send Traps to Operations Manager

Because Operations Manager uses SNMP MIB variables and traps to determine device health, you must configure devices to provide this information. For any Cisco devices that you want Operations Manager to monitor, SNMP must be enabled and the device must be configured to send SNMP traps to the Operations Manager server.

Make sure your devices are enabled to send traps to Operations Manager by using the command line or GUI interface that is appropriate for your device:

- Enabling Cisco IOS-Based Devices to Send Traps to Operations Manager, page 3-23
- Enabling Catalyst Devices to Send SNMP Traps to Operations Manager, page 3-24

Enabling Cisco IOS-Based Devices to Send Traps to Operations Manager

For devices running Cisco IOS software, enter the following commands:

```
(config)# snmp-server [community string] ro
(config)# snmp-server enable traps
(config)# snmp-server host [a.b.c.d] traps [community string]
```

where [*community string*] indicates an SNMP read-only community string and [*a.b.c.d*] indicates the SNMP trap receiving host (the Operations Manager server). For more information, see the appropriate command reference guide.

To send traps:

Step 1 Log into Cisco.com.

Step 2 Choose **Support > Cisco IOS and NX-OS Software**.

Step 3 Select the Cisco IOS Software release version used by your Cisco IOS-based devices.

Step 4 Under Reference Guides, select the appropriate command reference guide.

Periodically, information on Cisco.com is reorganized and, as a result, navigation paths change. If this happens, use Search to look for Cisco IOS Command References.

Enabling Catalyst Devices to Send SNMP Traps to Operations Manager

For devices running Catalyst software, provide the following commands:

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [a.b.c.d] [community string]
```

Where [*community string*] indicates an SNMP read-only community string and [*a.b.c.d*] indicates the SNMP trap receiving host (the Operations Manager server).

For more information, see the appropriate command reference guide.

To send SNMP traps:

Step 1 Log into Cisco.com.

Step 2 Select **Products & Services**.

Step 3 Under Network Systems, select **Switches**.

Step 4 Select the appropriate Cisco Catalyst series switch.

Step 5 In the Support box, select **References** and select the appropriate command reference guide.

When you select **References**, you may be prompted to log into Cisco.com.

Periodically, information on Cisco.com is reorganized and, as a result, navigation paths change. If this happens, try using Search to look for Catalyst Command References.

Integrating Operations Manager Trap Receiving with NMS or Trap Daemons

You might need to complete one or more of the following steps to integrate SNMP trap receiving with other trap daemons and other Network Management Systems (NMS):

- Add the host where Operations Manager is running to the list of trap destinations in your network devices. See Enabling Devices to Send Traps to Operations Manager, page 3-23. Specify port 162 as the destination trap port.
- If your network devices are already sending traps to another management application, configure that application to forward traps to Operations Manager.

Table 3-7 describes scenarios for SNMP trap receiving and lists the advantages of each.

Table 3-7 Configuration Scenarios for Trap Receiving

Scenario	Advantages
Network devices send traps to port 162 of the host where Operations Manager is running. Operations Manager receives the traps and forwards them to the NMS.	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • Operations Manager provides a reliable trap reception, storage, and forwarding mechanism. • NMS continues to receive traps on port 162 on the host where the NMS is running. • Network devices continue to send traps to port 162.
The NMS receives traps on default port 162 and forwards them to port 162 on the host where Operations Manager is running.	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • Operations Manager does not receive traps dropped by the NMS.

Configuring SNMP Trap Forwarding

By default, Operations Manager does not forward unprocessed SNMP traps. However, you can configure it to do so.

To configure trap forwarding:

Step 1 Choose **Administration > System Settings > Miscellaneous > Preferences**.

The System Preferences page appears.

Step 2 Under Trap Forwarding Parameters enter:

- An IP address or name for the server.
- A port number on which the server can receive traps.

Step 3 Click the **Apply** button.

Forwarding Windows Events as SNMP Traps

In order for Operations Manager to view forwarded Windows events from Windows-based devices as SNMP traps, you must configure the event to trap forwarder utility (**evntwin.exe**). Evntwin configures the translation of events to traps based on information in the Evntwin configuration file.

It is installed when the Windows SNMP service is installed. You need to select the event numbers that you want to forward as SNMP traps.

To select the events you want forwarded and update the evntwin configuration file:

Step 1 Go to **Start > Run** and enter **evntwin.exe**.

The Event to Trap Translator window opens.

Step 2 Select the Custom radio button, then click **Edit**.

Step 3 Select the event source in the Event sources pane.

Step 4 Select the event in the Events pane, click **Add**, and when the pop-up opens, click **OK**.

The selected event is now in the upper pane, Events to be translated to traps.

Step 5 Repeat step 4 until all events to be converted are selected.

Step 6 Click **Apply**.

Step 7 Click **Export** and save the file as **events.cnf** on your disk.

Step 8 Enter the following command:

*NMSROOT***evntcmd events.cnf**

where *NMSROOT* is the path where you saved the events.cnf on your machine.

Configuring Health Monitor

The Health Monitor utility monitors Operations Manager processes, notes when a process stops and restarts, and can send e-mail updates.

To get e-mail updates:

Step 1 Edit the *NMSROOT*/HealthMonitor/conf/HealthMonitor.cfg file.

Step 2 Enter a value for each of these parameters:

- SMTP_Server—SMTP mail server address.
- Receiver_Email_ID—E-mail ID for the administrator to be notified
- Sender_Email_ID—E-mail ID that identifies the sender

Step 3 After you update the file, put the updates into effect by restarting the HealthMonitor service. From the command line, enter these commands:

```
net stop HealthMonitor
net start HealthMonitor
```

For more information, see *Cisco Unified Operations Manager User Guide 8.5*.

Configuring Cisco Unified Communications Manager for Use with Operations Manager

For Operations Manager to discover and manage Cisco Unified Communications Manager (Unified CM), you must either perform the configurations described in this section or verify that the existing Unified CM settings are correct. Incorrect settings cause incomplete monitoring of Unified CM. This results in inconsistent behavior in some Operations Manager features.

This topic contains the following tasks:

For additional details on other voice application configurations, (such as Unity Connection and activating events and configuring Event Monitoring Service) see the Online help or user guide topic, *Working with Voice Application Systems and Software*.

Changing the Cisco Unified Communications Manager Cluster Name

Note You must use this procedure only if you are running a media server with Cisco Unified Communications Manager 3.3 or later.

Operations Manager cannot manage two clusters with the same name. If you are managing multiple Cisco Unified Communications Manager clusters, you must change the default cluster name. Cisco Unified Communications Manager starting with 3.3 use the default cluster name *StandAloneCluster*.

For detailed instructions on configuring Cisco Unified Communications Manager, see the Cisco Unified Communications Manager documentation.

To change the Cisco Unified Communications Manager cluster name:

Step 1 Open the Cisco Unified Communications Manager Administration page.

Step 2 From the menu bar, select **System**, and choose **Enterprise Parameters**.

The Enterprise Configuration page appears.

Step 3 In the Cluster ID field, enter a new cluster name.

Step 4 Click **Update**.

Configuring the Syslog Receiver on Cisco Unified Communications Manager

To successfully receive Cisco Unified Communications Manager (Unified CM) syslog messages, you must add the syslog receiver from the device's serviceability web page.

Syslog processing detects the following registered entities on the Unified CM cluster:

- Any registration changes on phones, voice mail endpoints, gateways, and so on.
- Any new phones provisioned in the cluster.

New phones provisioned are discovered if they are provisioned to an existing device pool. If the phone is part of a new device pool added to the cluster after the last cluster device discovery, you must use **Run Now** to view these phones in Operations Manager.

For additional details on which syslog events map to Unified CM releases, see the Event appendix in the *Cisco Unified Operations Manager User Guide 8.5*.

To add Operations Manager as a syslog receiver:

Step 1 On your Cisco Unified CM, select **Cisco Unified Serviceability** from the Navigation pull-down in the top-right corner of the device's home screen.

Step 2 Choose **Alarm > Configuration**.

Step 3 Select one of the Operations Manager servers and click **Go**.

Step 4 Select the correct alarm configuration elements for your particular machine as shown in the following table and click **Go**.

For This Unified Communications Manager Version...	Select These Alarm Configuration Elements...
4.x	Cisco CallManager
5.x	• Server > Service > Cisco AMC Service • Server > Service > Cisco CDR Agent • Server > Service > Cisco CDR Repository Manager • Server > Service > Cisco Call Manager • Server > Service > Cisco Database Layer Monitoring • Server > Service > Cisco DRF Client • Server > Service > Cisco DRF Master
6.x and later	• Service Group > CM Services > Service > Cisco CallManager • Service Group > CDR Service > Cisco CDR Agent and Cisco CDR Repository Manager • Service Group > Database and Admin Services > Cisco Database Layer Monitoring • Service Group > Performance and Monitoring Services > Cisco AMC Service • Service Group > Backup and Restore > Cisco DRF Client and Cisco DRF Master

Step 5 Check **Apply to all nodes**. See Figure 3-1 for an example of the serviceability page for a version 6.x device.

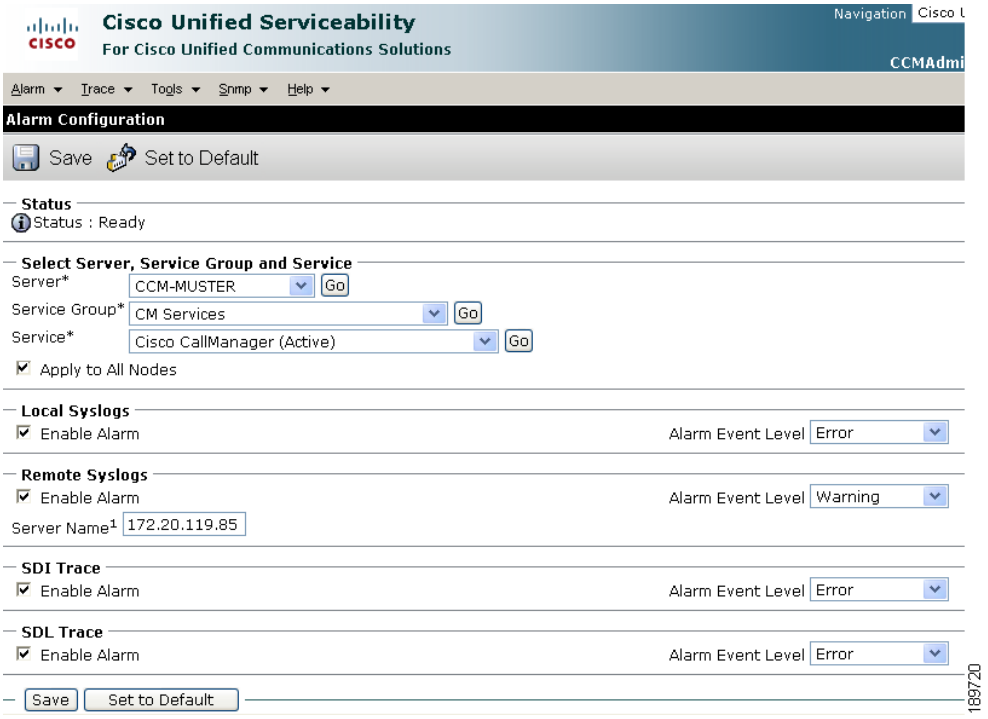
The serviceability page may display differently depending on the device version you are configuring.

Step 6 In Remote Syslogs, click the **Enable Alarm** check box, select the proper Alarm Event Level (see the Alarm Configuration Settings in *Cisco Unified Serviceability Administration Guide for Cisco Unified Communications Manager* on Cisco.com),

Step 7 Enter the Operations Manager server name or IP address in remote Server Name text box.

Step 8 Set the alarm event level to **Informational**. Provide any necessary information based on your Cisco Unified CM.

Figure 3-1 Unified Serviceability Web Page for a Unified Communications Manager Version 6.x Device



Step 9 Click **Save**.

Syslog messages have a limitation of 1,024 characters (including the heading). Some syslog-based event details may not contain the full information because of this syslog limitation. If the syslog message exceeds this limit, it is truncated to 1,024 characters by the syslog sender.

Activating Events in Operations Manager

Most device events appear in one of several event displays after the device has been added to the Operations Manager database. However, several events are not displayed in Operations Manager by default. You must activate the following events to enable Operations Manager to display them:

- Number Of Registered Gateways Increased

- Number Of Registered Gateways Decreased
- Number Of Registered MediaDevices Increased
- Number Of Registered MediaDevices Decreased

These events are raised at the cluster level; therefore, individual device information might not be available in the event description.

To access individual device information, use the RTMT tool. Choose **Filter > Devices > MediaDevices or Gateway**, then select the check box for all states and generate the report. This report displays all registered and unregistered media devices or gateways.

To activate these event pairs:

Step 1 Open the *NMSROOT*\conf\seg\sysLogConfig.xml file.

Step 2 Remove the comment for Syslog by removing the lines marked.

Step 3 Restart the SEGServer process.

Configuring CDR Forwarding on Cisco Unified Communications Managers

You can monitor Call Detail Record (CDR) trunk utilization on your Unified CMs using Operations Manager.

You must add Service Monitor as a UC management application monitored by Operations Manager. For details, see the Online help for **Administration > UC Management Suite > Service Monitor**.

You must also enable polling in Operations Manager. For details, see the Online help for **Administration > Polling and Thresholds > Polling Settings**.

To monitor CDR-based trunk data using Operations Manager and Service Monitor:

Step 1 On the Unified Communications Manager, select **Administration**.

Step 2 Go to the Service Parameters Configuration page by choosing **System > Service Parameters**.

Step 3 Set parameters for:

- **CDR Enabled Flag** by scrolling down to **System** and selecting **True**.
- **Call Diagnostics Enabled** by scrolling down to **Cluster wide Parameters** (Device - General) and selecting **Set to Enable Only When CDR Enabled Flag is True**.

Step 4 To add Operations Manager as a Billing Server in the Cisco Unified CM:

a. Choose **Tools > CDR Management**.

b. Scroll down to Billing Applications Server Parameters and click **Add New**.

c. Enter the following
   - Host Name/IP Address—IP address of the system where Operations Manager is installed.
   - User Name—Enter *smuser'*
   - Password—Default password is *smuser*

d. Select the SFTP Protocol.

e. Directory path—Enter */home/smuser*

f. Select the **Resend on failure** check box.

Step 5 Click **Add**.

(Optional) Configuring RTMT on Cisco Unified Communications Managers

Operations Manager uses the same polling rate and threshold settings as the Real-Time Monitoring Tool (RTMT). In normal operation, you do not need to do anything. The default will work properly.

Note Configuring RTMT impacts Unified Communications Manager and Operations Manager performance.

If you want to have a lower polling rate, increase the polling rate to monitor in real time, then update the parameter settings on Cisco Unified Communications Manager. To do so:

Step 1 Go to the Unified Communications Manager Administration page.

To change polling rates for Unified CM 6.x and later:

a. Choose **System > Service Parameter > publisher > Cisco AMC Service.**

b. Change the Data Collection Polling rate value.

To change threshold parameters:

a. Install and launch RTMT.

b. Select **AlarmCentral**.

c. Select a specific alert and right-click to launch Alert Property.

Step 2 Click **Save**.

Setting HTTP Credentials on Cisco Unified Communications Manager

Operations Manager uses the Administrative XML Layer (AXL) API in addition to SNMP to manage Cisco Unified Communications Manager. This means that Operations Manager makes SOAP calls over HTTP via the AXL interface to collect fault and performance information from Cisco Unified Communications Manager.

Operations Manager requires the HTTP username and password in order to execute these queries. The username and password do not need to have administrator privileges. You only need credentials with read-level access to access http://<*server-name*>/ccmadmin.

Verifying Cisco Unified Communications Manager DNS Settings

Operations Manager is unable to collect the correct monitoring information if it cannot resolve the Unified CM name using DNS. You must verify that the Unified CM is resolvable in DNS (both forward and backward).

Note the following about DNS:

- If the Unified CM is configured with the IP address only, the DNS setting is not a problem.
- If the Unified CM is configured with a DNS name, then it can be resolved from the Unified CM Server.
- The Unified CM should also be configured to send syslogs to Operations Manager server. For detailed steps, see Configuring the Syslog Receiver on Cisco Unified Communications Manager, page 3-28.

Viewing Events

You can view events using the Unified Dashboard displays. Select the **Diagnostics** tab from the Unified Dashboard and choose from any of the view displays to access event information.

Other event displays are available from:

- Fault Monitor
- Reports
- Service Level View

For more details, see the Online help or the *Cisco Unified Operations Manager User Guide* 8.5.

Customizing Operations Manager

After discovery completes Operations Manager is monitoring your network, Table 3-8 summarizes tasks that you might want to perform to customize Operations Manager for your specific deployment.

Note All these tasks are optional; they are not required for Operations Manager to monitor your network.

Table 3-8 Setting Up Operations Manager

Task	Description
Configure notifications	In addition to learning about events by monitoring the Unified Dashboard displays, you can subscribe users to receive e-mail and hosts to receive Operations Manager-generated SNMP traps in response to events.
Configuring device groups	Create device groups to use with, for example, views in the Fault Monitor displays, or with notification groups in Notification Services.

Table 3-8 Setting Up Operations Manager (continued)

Task	Description
Configure polling parameters and thresholds	Operations Manager provides default values for polling parameters and threshold values. However, you can update the values as needed for your network. You should plan to apply the changes when activity on the Operations Manager server is low. By default, Operations Manager does not set the voice utilization polling settings. If you want to use Operations Manager's performance monitoring capabilities, you must first enable voice utilization polling.
Configure purging	By default, Operations Manager purges the database daily at midnight. You can modify the schedule.
Configure inventory collection	Operations Manager provides a single default schedule for inventory collection. You can use that schedule, or you can suspend it.
Customize your Diagnostics view	You can change which view portlets you want to display in your Diagnostic Summary, Server, Phone, and Cluster views.
Activating certain device events	Most device events will display in the user interface after the device has been added to the Operations Manager database. However, several events will not be displayed in Operations Manager out of the box. You must activate the following events in order for Operations Manager to display them: • HardwareFailure • Number Of Registered Gateways Increased • Number Of Registered Gateways Decreased • Number Of Registered MediaDevices Increased • Number Of Registered MediaDevices Decreased

To use Operations Manager more fully, you might want to perform additional configuration tasks. See the Online help or *Cisco Unified Operations Manager User Guide 8.5* for information on using and configuring Operations Manager.