CHAPTER 2

Getting Started

These topics provide an task-based look at how to get started using Cisco Prime Unified Operations Manager (Cisco Prime UOM):

Timesaver To view the online video tutorials for Cisco Prime UOM, click on the E-Learning icon in the Online help.

Completing Cisco Prime UOM Setup Tasks

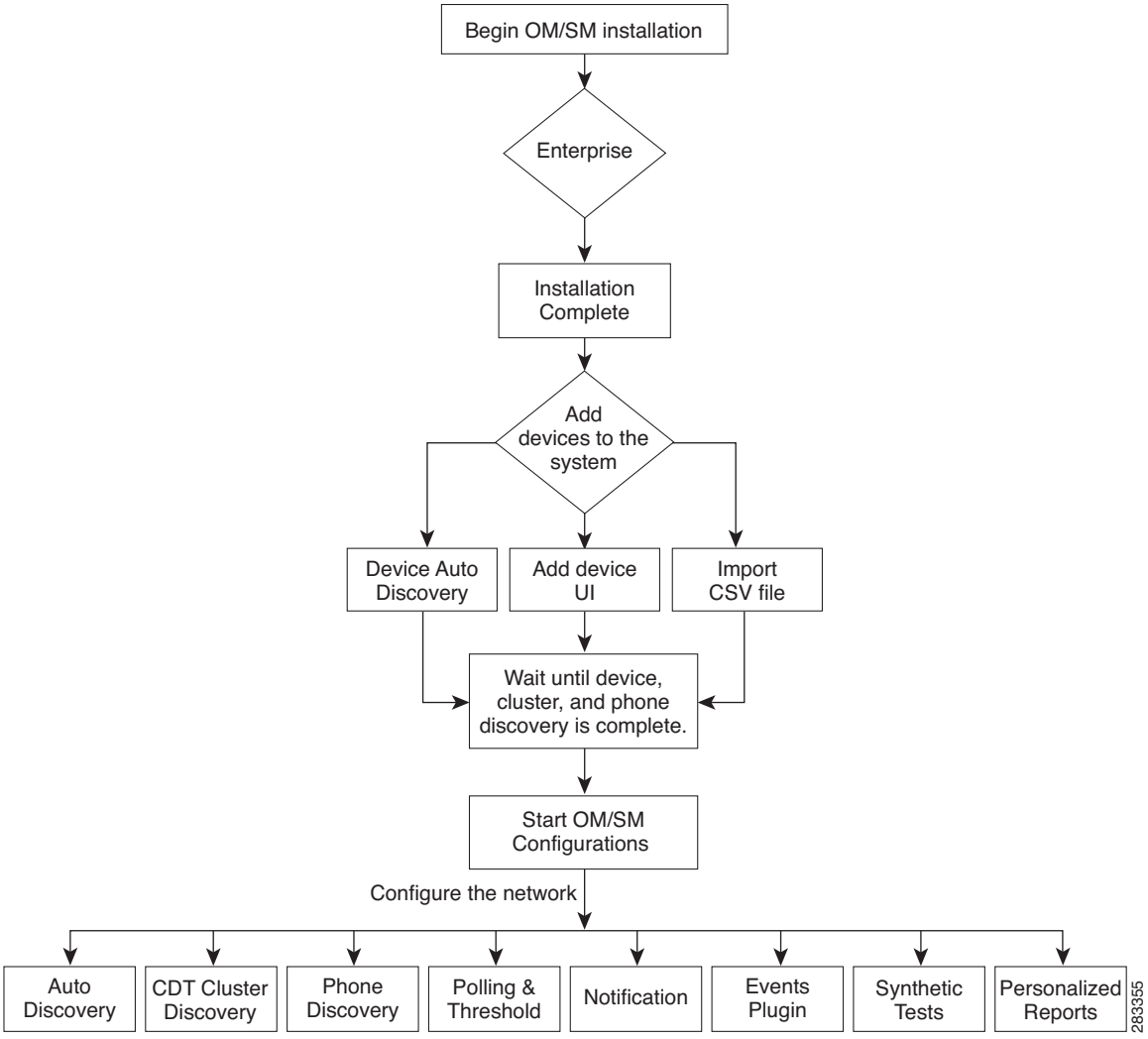
There are many set up tasks that Cisco Prime UOM requires to monitor the Unified Communications devices in your network. Depending on your deployment, you can use the following flowcharts that show you what you need to do before you can use Cisco Prime UOM to monitor your Unified Communications network. After setup you can collect data, run reports and monitor critical device events that may impact your network.

Use the setup tasks flowcharts that fit your deployment:

Enterprise Deployment Setup Tasks

This topic contains information on the tasks that you need to complete before you can start using enterprise version of Cisco Prime UOM to monitor your Unified Communications network.

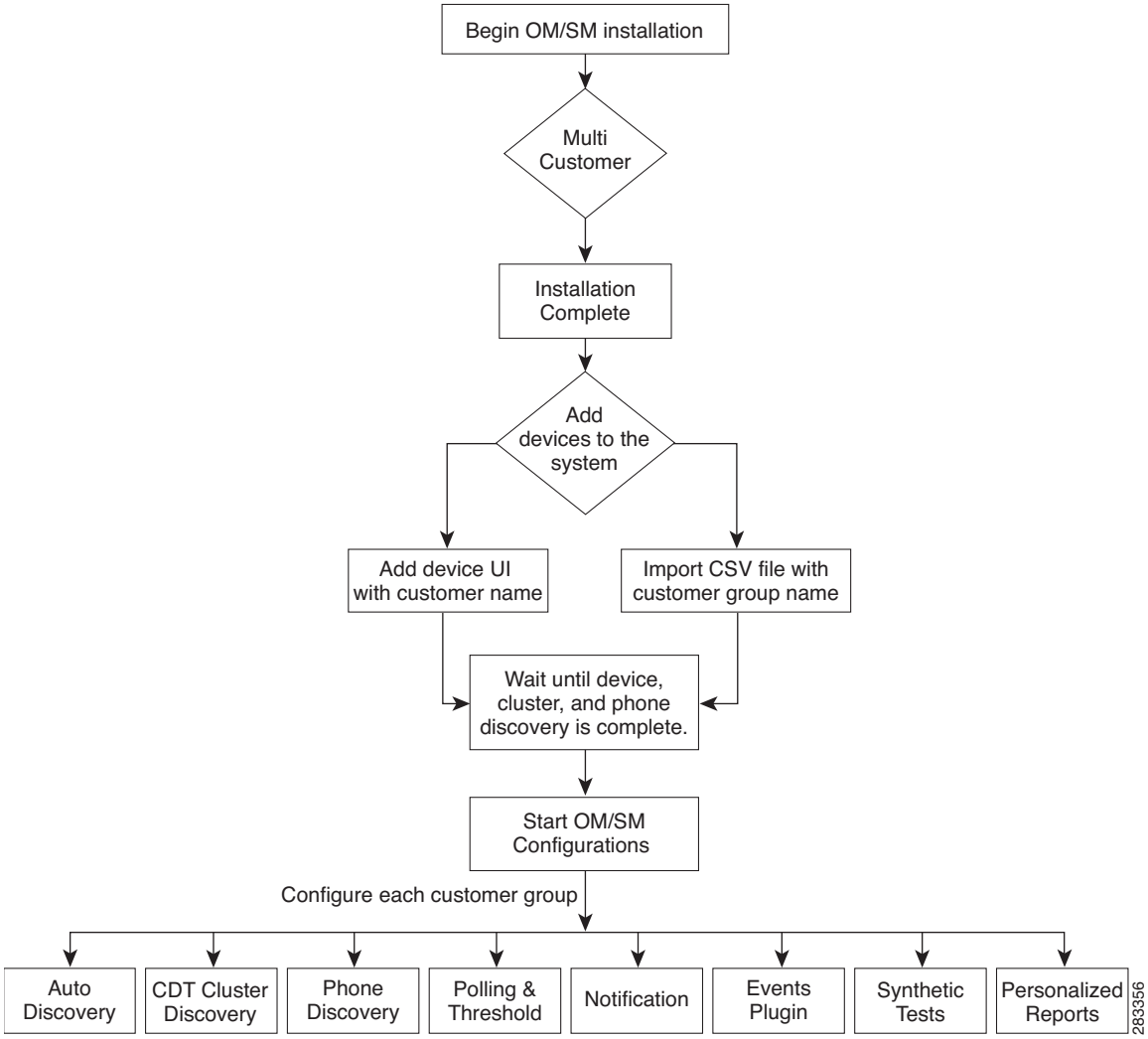
Figure 2-1 Set Up Tasks for an Enterprise Deployment



Multiple End-Customer Setup Tasks

This topic contains information on the tasks that you need to complete before you can start using multiple end-customer version of Cisco Prime UOM to monitor your Unified Communications network.

Figure 2-2 Set Up Tasks for a Multiple End-Customer Deployment



Configuring Cisco Prime UOM

This section includes tasks that are required to successfully use Cisco Prime UOM:

- Configuring Operations Manager to Monitor Devices, page 2-4
- Adding Cisco Unified Communications Management Server Links from Cisco Prime UOM, page 2-20
- Understanding and Configuring Security, page 2-21

Configuring Operations Manager to Monitor Devices

Cisco Prime UOM obtains devices to monitor from the Common Services Device and Credentials Repository (DCR). The DCR is a common repository of devices and their credentials for use by individual applications.

This section contains:

For Cisco Prime UOM 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 Cisco Prime UOM inventory, which is separate from the DCR.

Note When Cisco Prime UOM enterprise is installed, it will automatically synchronize with the DCR and add inventory. This is the default setting. For multiple end-customer installations, devices must be added manually.

For Enterprise users, you can add devices automatically from the DCR to Cisco Prime UOM by activating automatic synchronization (the default),. You can also add them manually through the Device Selection page.

For multiple end-customers, you can add them manually using Device Add page or Device Import. For more information on how Cisco Prime UOM is affected by the DCR, see Understanding the Device and Credentials Repository.

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 Cisco Prime UOM is installed on your system. If you selected the default directory during installation, it is C:\PROGRA~1\CSCOpx.

Table 2-1 lists some possible deployment scenarios for Cisco Prime UOM, and what you will need to do to add devices to Cisco Prime UOM inventory.

Table 2-1 Adding Devices to Inventory Scenarios

Deployment Scenario	What to Do
• Deploying Cisco Prime UOM 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 2-11.
• Deploying Cisco Prime UOM 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 2-12.
• Deploying Cisco Prime UOM as an independent server. • Using automatic discovery, but not all the devices discovered through automatic discovery need to be managed in Cisco Prime UOM.	• 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 2-11.
• Deploying Cisco Prime UOM with CiscoWorks LAN Management Solution (LMS). • Using the Cisco Prime UOM DCR as the master DCR. • Automatically synchronizing your inventory with the DCR.	• Set up the Cisco Prime UOM DCR as a master and the LMS DCRs as slaves. Configuring the DCR in Master and Slave Mode, page 2-6. • Run physical discovery. See Adding Devices to the DCR, page 2-7 • Verify that automatic synchronization is configured in Cisco Prime UOM. See Configuring Automatic Device Selection in Operations Manager, page 2-11.

Table 2-1 Adding Devices to Inventory Scenarios (continued)

Deployment Scenario	What to Do
• Deploying Cisco Prime UOM with LMS. • Synchronizing the Cisco Prime UOM DCR with an existing master DCR. • Automatically synchronizing your inventory with the DCR.	• Set up the Cisco Prime UOM server DCR as a slave and one of the LMS DCRs as a master. Configuring the DCR in Master and Slave Mode, page 2-6. • Configure Cisco Prime UOM to add devices to a master DCR. See Adding Devices to the DCR, page 2-7. • Run physical discovery. See Adding Devices to the DCR, page 2-7 • Verify that automatic synchronization is configured in Cisco Prime UOM. See Configuring Automatic Device Selection in Operations Manager, page 2-11.
• Deploying Cisco Prime UOM with LMS. • Synchronizing the Cisco Prime UOM with an existing master DCR. • Manually controlling the devices managed by Cisco Prime UOM.	• Set up the Cisco Prime UOM server DCR and the LMS server DCRs as slave and master. Configuring the DCR in Master and Slave Mode, page 2-6. • Configure Cisco Prime UOM to add devices to a master DCR. See Adding Devices to the DCR, page 2-7. • Run physical discovery. See Adding Devices to the DCR, page 2-7 • Verify that manual synchronization is configured in Cisco Prime UOM. See Configuring Automatic Device Selection in Operations Manager, page 2-11.

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

Configuring the DCR in Master and Slave Mode

By default, the DCR on the Cisco Prime UOM server is configured as a standalone or an independent repository. If you decide to configure the DCR for Cisco Prime UOM 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 Cisco Prime UOM 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 Cisco Prime UOM, page 1-26.

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.

Follow the instructions in the Common Services 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 Cisco Prime UOM 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 2-11.

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 2-9).

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. This results 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 2-10).

  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 the **daily** radio button. 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 of the same type and use the same credentials. If you use 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 Cisco Prime UOM 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 2-2 describes the optional filters that are available to you when running physical discovery.

Table 2-2 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 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 2-2 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) Cisco Prime UOM 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

Cisco Prime UOM 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 Cisco Prime UOM to collect inventory for all devices, depending on how many devices are being added to Cisco Prime UOM.

Note Devices must exist in the DCR before you can add them to Cisco Prime UOM.

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**.

Cisco Prime UOM is synchronized with the DCR. Any DCR devices currently not in Cisco Prime UOM are added. Cisco Prime UOM 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 Deleting Devices, page 8-57.

Adding Devices Manually from the DCR to Operations Manager

If Cisco Prime UOM 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 Cisco Prime UOM.

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 Cisco Prime UOM 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 Deleting Devices, page 8-57.

Understanding Device States

The Device Management: Summary page lists the device states for all devices in the Cisco Prime UOM inventory. Select **Administration > Device Management > Device Configuration > Device Summary** to view the page.

To view the status on phone discovery collection, see Viewing and Scheduling Phone XML Discovery Status, page 8-63.

Table 8-3 describes the information displayed on the Device Management Summary page.

Table 2-3 describes the device transition states when you add devices to the inventory.

Table 2-3 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 Cisco Prime UOM

You can verify that your devices have been added to Cisco Prime UOM 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 2-15.

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 2-14.)

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 2-14.)

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

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 2-16.
- If device inventory collection times out for several devices, increase SNMP timeout settings. See Modifying SNMP Timeout and Retries, page 2-16.
- View device error information on the Modify/Delete Device page. See Performing Manual Inventory Collection on Devices, page 2-17.
- 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 Device DNS Settings, page 2-35.
- Check the reason for devices being in the Unreachable state. See To use Cisco Prime UOM more fully, there may be configuration steps specific to devices, reports, or other features. For more details, see Configuring Devices Before Device Collection, page 2-18.Before You Start Cisco Prime UOM, page 2-19.
- After troubleshooting the problem, check the device status. See Verifying Devices Added to Cisco Prime UOM, page 2-13.

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 Cisco Prime UOM, page 2-13).

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 To use Cisco Prime UOM more fully, there may be configuration steps specific to devices, reports, or other features. For more details, see Configuring Devices Before Device Collection, page 2-18.Before You Start Cisco Prime UOM, page 2-19).

Step 5 Perform the required actions to clear the error.

Also see Table 8-9 which explains the possible reasons for the error codes that you see in the Modify/Delete Devices page, that occur for partially monitored devices.

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, Cisco Prime UOM times out. Cisco Prime UOM 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 retry value is 3 seconds, Cisco Prime UOM 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 Cisco Prime UOM only during discovery (inventory collection) of the device. Therefore any changes to a device's configuration are not shown by Cisco Prime UOM 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, Cisco Prime UOM displays messages that only active devices will go through inventory collection.

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

The following events also trigger inventory collection:

- The entire Cisco Prime UOM inventory is polled. This is controlled by the inventory collection schedule. (See Scheduling Inventory Collection, page 2-14.)
- Cisco Prime UOM 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.
- Cisco Prime UOM uses manual synchronization with the DCR, and a device is added to Cisco Prime UOM 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 Cisco Prime UOM.

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.

Configuring Devices Before Device Collection

This section provides an overview of the following topics:

- Working with Voice Application Systems and Software, page 2-25
- Configuring Syslog Receivers to Send Events to Cisco Prime UOM, page 2-28

Adding Devices to Cisco Prime UOM

This section provides an overview to the steps for device discovery and inventory collection.

There are many options to add devices to Cisco Prime UOM. Depending on the deployment you are using, you can add devices using the options in Table 2-4:

Table 2-4 Adding Devices into the Cisco Prime UOM Inventory

Deployment Type	Inventory Collection Options	Description
Enterprise users only	1. Discover devices automatically.[1]	• Use default settings (no action required for Enterprise customers). For more details, see Discovering Devices Automatically for Enterprise Deployments, page 8-3.
		• Configure discovery settings for automatic discovery. See Adding Specific Devices from the DCR, page 8-7. • For a video tutorial on automatic device discovery, click on the E-Learning icon in the online help.
Enterprise or multiple end-customers	2. Manually add devices. (Enterprise or multiple-end customers users only)	Adding Devices to the DCR, page 8-8
Enterprise or multiple end-customers	3. Import devices. (Enterprise or multiple-end customers users only)	Importing Devices Into the DCR, page 2-11

1. Device credentials are required to collect inventory information. Auto-discovery is the default for Enterprise customers. For details on how to handle discovery for multiple end-customer deployments, see Adding Devices to the DCR, page 8-8 or Importing Devices Into the DCR, page 2-11.

Customizing Cisco Prime UOM

This section include tasks that are not required, but can expand Cisco Prime UOM's capabilities:

- Supported NMS Integration, page 2-21
- Viewing Events, page 2-35

After you add devices to Cisco Prime UOM is monitoring your network, Table 2-5 summarizes tasks that you might want to perform to customize Cisco Prime UOM for your specific deployment.

Note All these tasks are optional; they are not required for Cisco Prime UOM to monitor your network.

Table 2-5 Setting Up Cisco Prime UOM

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 Cisco Prime UOM-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.
Configure polling parameters and thresholds	Cisco Prime UOM 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 Cisco Prime UOM server is low. By default, Cisco Prime UOM does not set the voice utilization polling settings. If you want to use Cisco Prime UOM's performance monitoring capabilities, you must first enable voice utilization polling.
Configure purging	By default, Cisco Prime UOM purges the database daily at midnight. You can modify the schedule.
Configure inventory collection	For enterprise users only, Cisco Prime UOM 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, Gateway, and Cluster views.
Activating certain device events	Most device events will display in the user interface after the device has been added to the Cisco Prime UOM database. However, several events will not be displayed in Cisco Prime UOM out of the box. You must activate the following events in order for Cisco Prime UOM 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 Cisco Prime UOM more fully, there may be configuration steps specific to devices, reports, or other features. For more details, see Configuring Devices Before Device Collection, page 2-18.Before You Start Cisco Prime UOM

You can access Cisco Prime UOM from either the Cisco Prime UOM 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 Cisco Prime UOM server must also meet all the system requirements for a client system (for client system requirements, see the *Installation Guide for Cisco Prime Unified Operations Manager*.
- Disable any popup blocker utility that is installed on your client system before launching Cisco Prime UOM.
- By default, SSL is not enabled in Common Services. If you upgraded to Cisco Prime UOM 8.7 and SSL was enabled before the upgrade, it remains enabled after the upgrade.

Starting Cisco Prime UOM on a Client System

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

Starting Cisco Prime UOM on the Cisco Prime UOM 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 Cisco Prime UOM home page to the Internet Explorer Trusted Sites Zone. You will not be able to access the Cisco Prime UOM 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 Cisco Prime UOM home page.

To add the Operations Manager home page:

Step 1 Open Cisco Prime UOM 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 Cisco Prime UOM

To add a link to a locally installed or remotely installed Service Monitor, Service Statistics Manager, or Provisioning Manager server from Cisco Prime UOM, use the UC Management Suite tab.

For step-by-step instructions, see Setting Up Cisco Unified Communications Management Application Links, page 21-1.

For important details about Service Monitor event and trap processing, see Processed SNMP Traps, page C-1. For open issues, see the *Release Notes for Cisco Prime Unified Operations Manager.*

Understanding and Configuring Security

Cisco Prime UOM supports the following security-related mechanisms:

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

  Cisco Prime UOM supports integration with Cisco Secure ACS. For more information, see Security Configuration with Cisco Secure ACS, page C-1 in the *Installation Guide for Cisco Prime Unified Operations Manager.*
- 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. Cisco Prime UOM 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

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

- Cisco Prime UOM listens for traps from managed devices on port 162 (the default). If your network devices already send traps to another management application, configure that application to forward traps to Cisco Prime UOM.
- Cisco Prime UOM forwards traps to destinations that you specify, as follows:
  - To forward pass-through traps, see Configuring SNMP Trap Receiving and Forwarding, page 2-21.
  - To forward processed traps, see Configuring Notifications, page 15-8.

  For more information on pass-through and processed traps, see Processed SNMP Traps, page C-1.

Configuring SNMP Trap Receiving and Forwarding

Cisco Prime UOM can receive traps on any available port and forward them to a list of devices and ports. This capability enables Cisco Prime UOM 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 Cisco Prime UOM or to one of the following:

- An NMS

- A trap daemon

This section contains:

- Updating the SNMP Trap Receiving Port, page 2-22
- Configuring Devices to Send Traps to Cisco Prime UOM, page 2-22
- Integrating Cisco Prime UOM Trap Receiving with NMS or Trap Daemons
- Configuring SNMP Trap Forwarding, page 2-23
- Forwarding Windows Events as SNMP Traps, page 20-7

To send traps directly to Cisco Prime UOM, perform the tasks in Enabling Devices to Send Traps to Operations Manager, page 20-6.

To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in Integrating Cisco Prime UOM Trap Receiving with NMS or Trap Daemons, page 2-22.

Updating the SNMP Trap Receiving Port

By default, Cisco Prime UOM 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 Cisco Prime UOM uses, see Ports and Interfaces that Cisco Prime UOM Monitors, page 8-6.

Configuring Devices to Send Traps to Cisco Prime UOM

Because Cisco Prime UOM 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 Cisco Prime UOM to monitor, SNMP must be enabled and the device must be configured to send SNMP traps to the Cisco Prime UOM server.

Make sure your devices are enabled to send traps to Cisco Prime UOM by using the command line or GUI interface that is appropriate for your device. See Enabling Devices to Send Traps to Operations Manager, page 20-6.

Integrating Cisco Prime UOM 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 Cisco Prime UOM is running to the list of trap destinations in your network devices. See Configuring Devices to Send Traps to Cisco Prime UOM, page 2-22. 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 Cisco Prime UOM.

Table 2-6 describes scenarios for SNMP trap receiving and lists the advantages of each.

Table 2-6 Configuration Scenarios for Trap Receiving

Scenario	Advantages
Network devices send traps to port 162 of the host where Cisco Prime UOM is running. Cisco Prime UOM receives the traps and forwards them to the NMS.	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • Cisco Prime UOM 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 Cisco Prime UOM is running.	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • Cisco Prime UOM does not receive traps dropped by the NMS.

Configuring SNMP Trap Forwarding

By default, Cisco Prime UOM 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.

  For a list of ports that other Cisco Unified Communications Manager applications uses, see Ports and Protocols that Operations Manager and other CUCM Applications Use, page 20-9.

Step 3 Click the **Apply** button.

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 Configuring Notifications, page 15-8.

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 Cisco Prime UOM home page.

To add the Operations Manager home page:

Step 1 Open Cisco Prime UOM 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**.

Configuring DSCP Traffic Prioritization on Cisco Prime UOM Server

In order to enable the Cisco Prime UOM server to mark packets marked with a configurable DSCP priority, perform the following procedure on Windows 2008 server only:

1. Go to Windows Start > Run.
2. Enter gpedit.msc and click **Enter** to open the Local Group Policy Editor.
3. Select **Local Computer Policy > Computer Configuration > Windows Settings > Policy-based QoS** and create a policy. For example, one named dscp_settings.

4. In the Policy Profile tab, specify a DSCP value for this policy. For example, 55.
5. In the Application Name tab, select All Applications.
6. In the IP Addresses tab, select This QoS policy applies to Any source IP address and any destination IP address.
7. In the Protocol and Ports tab, select this QosS policy applies to TCP and UDP. Also select the source and destination port as any.
8. Click OK.
9. To apply these policy changes you must run the following command: gpupdate /force

Working with Voice Application Systems and Software

The following topics describe hardware-specific and version-specific tasks and behavior:

Note See Cisco Unified Communications Manager Compatibility Matrix on Cisco.com for complete up-to-date information about Cisco Unified Communications Manager versions and support.

Configuring Voice Application Systems and Software for Use with Cisco Prime UOM

Table 2-7 lists tasks that you must perform before Cisco Prime Unified Operations Manager (Cisco Prime UOM) can successfully monitor Cisco voice application software.

Table 2-7 Configuration Tasks by Application Software Version and System

If you have the following voice application software…	On the following voice application systems…	You must perform the following tasks
Any voice application software that Cisco Prime UOM supports	Media Server	Setting a Media Server's SNMP Services Community String Rights, page 2-28
Cisco Unified Communications Manager 3.3 and later	Media Server	Changing the Cisco Unified CM Cluster Name, page 2-26
Cisco Unified Communications Manager 6.x and later	Media Server	Configuring Syslog Receiver on Cisco Unified CM, page 2-28
	Media Server	Configuring CDR Forwarding on Cisco Unified CMs, page 2-27
Cisco Unified Communications Manager Express	Router	Set **CCMEEnabled** on the router to true. Set **snmp get** for 1.3.6.1.4.1.9.9.439.1.1.1.0 to return 1.
SRST Router	Router	Enable the SRST service on this router. Set **snmp get** for 1.3.6.1.4.1.9.9.441.1.2.1.0 to return 1.
Cisco Unity Connection	Not applicable	Configuring Syslog Receiver on Cisco Unity Connection, page 2-31
Cisco Unified Communications Manager 5.1.3 or later in Syslog/RTMT	Voice Gateways Media Server	Activating Events in Operations Manager, page E-82
Cisco Unified Presence	Not applicable	Configuring Syslog Receiver on Cisco Unified Presence, page 2-32

Changing the Cisco Unified CM Cluster Name

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

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

For detailed instructions on configuring Cisco Unified CM, see the Cisco Unified CM documentation

To change the Cisco Unified CM cluster name:

Step 1 To change the Cisco Unified CM cluster name: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 CDR Forwarding on Cisco Unified CMs

You can monitor Call Detail Record (CDR) trunk utilization on your Unified CMs using Cisco Prime UOM.

You must add Service Monitor as a UC management application monitored by Cisco Prime UOM. For details, see Accessing a Service Monitor Server, page 21-2.

You must also enable polling in Cisco Prime UOM. For details, see Editing Polling Parameters, page 19-15.

To monitor CDR-based trunk data using Cisco Prime UOM and Service Monitor:

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

Step 2 Go to the Service Parameters Configuration page by selecting **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 Cisco Prime UOM as a Billing Server in the Cisco Unified CM:

a. Select **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 Cisco Prime UOM 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**.

Setting a Media Server's SNMP Services Community String Rights

Note Use this procedure on media servers running voice application software. Cisco Prime UOM installation ensures that the SNMP service is installed and enabled on that server.

Cisco Prime UOM cannot monitor supported voice applications running on a media server if community string rights for SNMP services are set to *none*. The SNMP queries will not succeed unless the rights for the community string are changed to *read-only*, *read-write*, or *read-create*.

Step 1 On the media server system, select **Start > Settings > Control Panel > Administrative Tools > Services**.

The Services window opens.

Step 2 Double-click **SNMP Service**.

The SNMP Services Properties window opens.

Step 3 Select the **Security** tab.

Step 4 Select **Community String** and click **Edit**.

Step 5 Change the rights from NONE to READ ONLY.

Cisco Prime UOM requires read-only rights. You are not required to set the rights to read-write or read-create.

Configuring Syslog Receivers to Send Events to Cisco Prime UOM

To successfully receive Cisco Unified Communications Manager, Unity Connection, or Unified Presence syslog messages on Cisco Prime UOM, you must add the syslog receiver from the device's administration and/or serviceability web page. Use the following procedures to perform the necessary steps.

Service Down events are now included as syslog events that are supported in Cisco Prime UOM.

- Configuring Syslog Receiver on Cisco Unified CM, page 2-28
- Configuring Syslog Receiver on Cisco Unity Connection, page 2-31
- Configuring Syslog Receiver on Cisco Unified Presence, page 2-32

Configuring Syslog Receiver on Cisco Unified CM

To successfully receive Cisco Unified Communications Manager 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 Cisco Prime UOM.

For additional details on what syslog events map to Unified Communications Manager releases, see the events listed in Fault Monitor or browse Table E-2.

To configure syslog receiver on Cisco Unified Communications Manager:

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

Step 2 Select **System > Enterprise Parameters**.

Step 3 Go to Cisco Syslog Agent section and update the following required fields:

- **Remote Syslog Server Name** with the IP address of Cisco Prime UOM
- Select *Informational* from the drop-down menu for **Syslog Severity For Remote Syslog Messages**

Step 4 Select **Cisco Unified Serviceability** from the Navigation drop-down in the top-right corner of the device's home screen.

Step 5 Select **Alarm > Alarm Configuration**.

Caution Do not use the CCM enterprise service parameter to configure the syslog receiver for Cisco Prime UOM syslog integration. When the enterprise parameter is enabled, all syslog messages (with matching severity levels) are sent regardless of whether or not they are intended to be processed by Cisco Prime UOM.

Step 6 Select the correct alarm configuration elements (Server, Service Group, and Service) for your particular machine and then click **Go**. For example:

- Enter Cisco Prime UOM server name/address in Server text box.
- Select Service Group and Service options based on the following table:

For This Unified Communications Manager Version...	Select These Alarm Configuration Elements...
4.x	Cisco CallManager

For This Unified Communications Manager Version...	Select These Alarm Configuration Elements...
5.1	• Server > Service > Cisco AMC Service • Server > Service > Cisco CDR Agent • Server > Service > Cisco CDR Repository Manager • Server > Service > Cisco CallManager • 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 • Service Group > Remote Syslogs

Step 7 Click on the **Enable Alarm** check box, select proper Alarm Event Level.

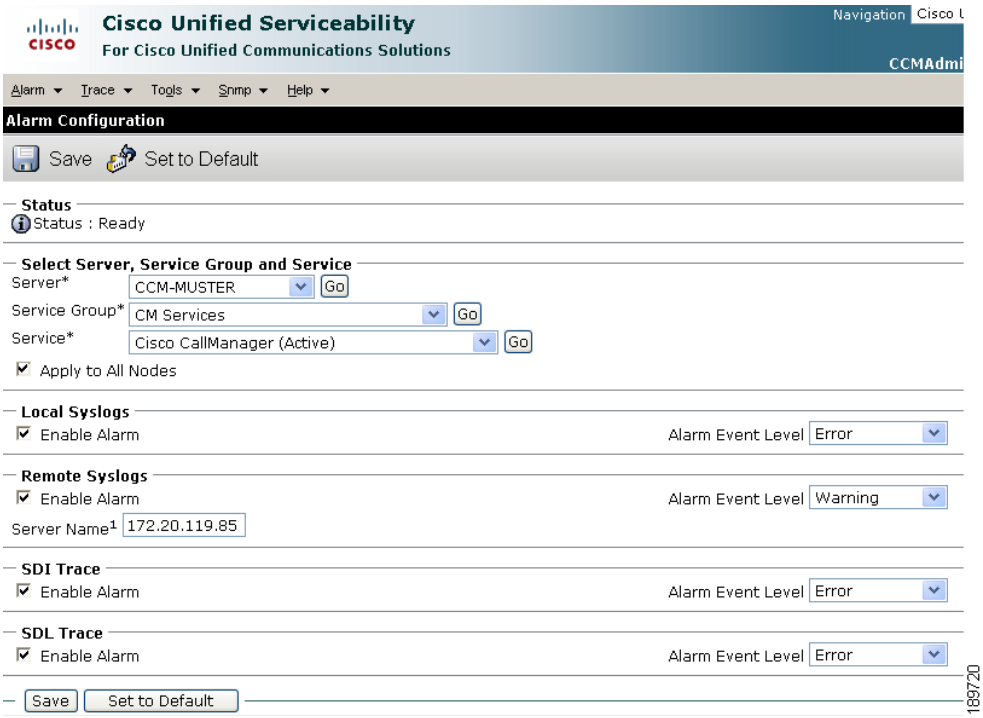
See the Alarm Configuration Settings in *Cisco Unified Serviceability Administration Guide for Cisco Unified Communications Manager* on Cisco.com.

For example, for Local Syslogs, set the alarm event level to **Error**.

Step 8 Enter any necessary information based on your Unified Communications Manager. For device cluster discovery or remote syslog notification, set the alarm event level to **Informational**.

Step 9 Check **Apply to all nodes**. (See Figure 2-3 on page 2-31 for an example of a serviceability page. The serviceability web page may differ depending on the device version you are configuring.

Figure 2-3 Cisco Unified Serviceability Page for Version 6.0



Step 10 Click **Save**.

Syslog messages have a limitation of 1,024 characters (including the heading). Any 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.

Configuring Syslog Receiver on Cisco Unity Connection

To successfully receive Cisco Unity Connection syslog messages, you must add the syslog receiver from the device's serviceability web page.

For additional details on what syslog events map to Unity Connection releases, see the events listed in Fault Monitor or browse Table E-2.

To configure syslog receiver on Cisco Unity Connection:

Step 1 On your Cisco Unity Connection, select **Cisco Unity Connection Administration** from the Navigation drop-down in the top-right corner of the device's home screen.

Step 2 Select **System > Enterprise Parameters**.

Step 3 Go to Cisco Syslog Agent section and update the following required fields:

- **Remote Syslog Server Name** with the IP address of Cisco Prime UOM
- Select *Informational* from the drop-down menu for **Syslog Severity For Remote Syslog Messages**

Step 4 Select **Cisco Unity Connection Serviceability** from the Navigation drop-down in the top-right corner of the device's home screen.

Step 5 Select **Alarm > Configurations**.

Select the correct alarm configuration elements for your particular machine:

- For Unity Connection 8.x:
  - Enable Informational Alarms for Local syslogs
  - Enable Informational Alarms Remote Syslogs and enter the Server name as Cisco Prime UOM Server IP address

Step 6 Click **Save** to save the configuration to complete syslog configuration.

Configuring Syslog Receiver on Cisco Unified Presence

To successfully receive Cisco Unified Presence syslog messages, you must add the syslog receiver from the device's serviceability web page.

For additional details on what syslog events map to Unified Presence releases, see the events listed in Fault Monitor or other interfaces, see Table E-2.

To configure syslog receiver on Cisco Unified Presence:

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

Step 2 Select **Alarm > Configurations**.

Step 3 Select the correct alarm configuration elements (Server, Service Group, and Service) for your particular machine and then click **Go**. For example:

- Enter the Cisco Prime UOM server name/address in Server text box.
- Select **CUP Services** in the Service Group.
- For Remote Syslogs, select **Enable Alarms** and set the Alarm Event Level to **Informational**.

Step 4 Click **Save** to save the configuration to complete syslog configuration.

Configuring the Unity Event Monitoring Service

The Event Monitoring Service (EMS) should already be installed along with the Remote Serviceability Kit.

Configure the Event Monitoring Service to support these Unity events in Cisco Prime UOM:

- OutOfDiskSpace—Event Source: ESE, Event ID: 482.
- HardDiskError—Event Source: Cissesrv, Event ID: 24600.
- ExchangeLoginFailed—Event Source: CiscoUnity_Doh, Event ID: 32013.

For details on these events, see Supported Events, page E-3.

To configure the Event Monitoring Service:

Step 1 Open the Tools Depot on the Desktop and navigate to **Diagnostic Tools > Event Monitoring Service**.

Step 2 Double-click to run.

Step 3 Create a recipient to receive notifications by selecting **File > New > Recipient** or, select the Recipients node in the navigation tree and click **Create New Recipient**.

Step 4 Enter a Recipient Name to identify a single recipient (or a group as there can be multiple email addresses under SMTP).

Step 5 Select the desired notification method tabs.

- The SNMP trap tabs works with the Remote Serviceability Kit to send traps to a destination (defined under windows SNMP service properties).
- The Syslog tab allows entry of a Syslog server address for the event.
- The failover tab is not a notification, but can force a failover upon receipt of a specified event.

The Test button at the top of the page sends a test event to the defined recipients. These can be:

- Event Source: EMSTest
- Event ID:10001
- Description: Event Monitoring Service Test Message

Step 6 Create a monitored event by selecting **File > New> Event**, or, select the Monitored Events node in the navigation tree and click **Create New Event**.

If the event exists currently in the Windows Event Viewer, to populate the event information in the Add New Event dialog:

- Select the event in Windows Event Viewer.
- Select **Copy Event to Clipboard**.
- Use Import Event From Clipboard in the Add New Event dialog.

To manually add the event:

Step 1 Select **Event Source** from the pull-down menu

Step 2 Select a specific Event ID and enter the desired ID. All Event IDs could also be used to obtain all events from a specified event source.

Step 3 Select **Type** to filter what level notifications should be sent for.

Step 4 Select **Errors**, **Warnings**, and **Informational** for all level events or if the Type is **unknown**.

Step 5 Enter Notes that will be included with the notification, such as troubleshooting steps.

The content section allows you to record a custom WAV for the event used along with the Recipient Voicemail option.

The Email Subject and Body can be used to customize the formatting of the messages sent to Recipient Email and SMTP notification methods. If no customization is desired, leave default fields as is.

Step 6 Select **OK** after adding the new event.

To activate the new event, one or more Recipients need to be added to it.

Step 1 Select the newly added event and click on the **Add Recipients** icon. The Recipients and notification methods can be further defined with check boxes here.

Step 2 Check the **Active** check box and **Apply** to activate the event.

You may also perform this step from the Monitored Events node in the navigation tree.

You can also exclude or ignore events that pass the other criteria by selecting **File > New > Exclusion**, or, select the Exclusions node in the navigation tree and click **Create New Exclusion**.

If the event exists currently in the Windows Event Viewer, you can populate the event information in the Add Exclusion dialog by selecting the event in Windows Event Viewer and clicking **Copy Event to Clipboard**. Then use Import Event From Clipboard in the Add Exclusion dialog.

To manually exclude the event:

Step 1 Select the event Source from the pull-down.

Step 2 Select **Specific Event ID** and enter the desired ID. All Event Ids could also be used to obtain all events from a specified event Source.

Step 3 Select **OK** when finished adding the new exclusion.

Configuring RTMT on Cisco Unified CM

Cisco Prime UOM uses the same polling rate and threshold settings as RTMT. In normal operation, you do not need to do anything. The defaults will work properly.

Note This impacts Unified Communications Manager (Unified CM) performance and Cisco Prime UOM.

If you want to have a lower polling rate, increase the polling rate to monitor in real-time, and then update the parameter settings on Unified CM, do the following:

- To update the polling and threshold parameter settings, go to the Unified Communications Manager Administration page.
- To change polling rates for CallManager 6.x and later, select **System > Service Parameter > publisher > Cisco AMC Service**, then change the Data Collection Polling rate value.
- To change threshold parameters, install and launch RTMT, select **AlarmCentral**, then select a specific alert and right-click to launch Alert Property.

Setting HTTP Credentials on Cisco Unified CM

Cisco Prime UOM uses the AVVID XML Layer (AXL) API in addition to SNMP to manage Cisco Communications Manager. This means that Cisco Prime UOM makes SOAP calls over HTTP via the AXL interface to collect fault and performance information from Cisco Unified Communications Manager. Cisco Prime UOM 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 *http://server-name/ccmadmin*.

Verifying Cisco Unified Communications Device DNS Settings

Cisco Prime UOM is unable to collect the correct monitoring information if it cannot use domain name service (DNS) to resolve the Unified CM names.

Verify the devices can be resolved (both forward and backward).

Note the following about DNS:

- If the device is configured with the IP address only, the DNS setting is not a problem.
- If the device is configured with a DNS name, then it can be resolved from the server.
- The device should also be configured to send syslogs to the Cisco Prime UOM server. For detailed steps, see Configuring Syslog Receiver on Cisco Unified CM, page 2-28.
- For additional information n DNS resolution, see Adding Devices to the DCR, page 8-8 and the Deployment Guide on Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html.

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