Administering Operations Manager

This chapter includes the following topics:

Performing Operations Manager Administration Tasks

From the IP Communications Operations Manager (Operations Manager) Administration tab, you can perform the tasks listed in Table 19-1.

Table 19-1 Operations Manager Administration Tasks

Tasks	Description
Polling and Thresholds See Configuring Polling and Thresholds, page 17-1.	From Polling and Thresholds, you can: • Change polling intervals, timeouts, and retries by device group • Enable and disable polling settings • Change thresholds, resetting the limits against which polled data will be compared • Customize threshold settings • Reprioritize groups for polling and thresholds • Apply polling and threshold changes to the system—After you apply changes, Operations Manager configures data collectors to: – Start using updated polling parameters and threshold values – Resume polling for devices or device elements that were previously suspended
SRST Poll Settings See Configuring SRST Poll Settings, page 18-1.	From the SRST Poll Settings page, you can configure SRST monitoring.
Service Quality Settings See Configuring Service Quality Settings, page 19-7.	From the Service Quality Settings page, you can: • Add or delete a remote IP Communications Service Monitor (Service Monitor) to Operations Manager. • Set a MOS threshold. **Note** For Operations Manager to process traps from a Service Monitor, you must add the Service Monitor to Operations Manager *and* you must use Service Monitor to configure Operations Manager as a trap receiver.
System Status See Generating and Understanding the System Status Report, page 19-10.	From the System Status page, you can generate a System Status report.
Logging See Using Logging to Enable and Disable Debugging, page 19-14.	From the Logging page, you can change the type—and quantity—of messages written to log files, enabling and disabling debugging, for example.

Table 19-1 Operations Manager Administration Tasks (continued)

Tasks	Description
System Preferences See Setting System-Wide Parameters Using System Preferences, page 19-12.	From the System Preferences page, you can configure the following: • SNMP trap receiving—Change the port on which Operations Manager listens for SNMP traps • SNMP trap forwarding—(Optional) Set a host and port number as a recipient for pass-through traps • Default SMTP server—Change or enter a default server to use for e-mail notifications. • Purging schedule—Select the time when database purging occurs daily. • Common Services Servers—Enter remote servers running other CiscoWorks products, such as: – Resource Manager Essentials (RME) – Campus Manager – CiscoView
Add Users See Configuring Users (ACS and Non-ACS), page 19-19.	Launches a Common Services window that opens to the Local User Setup page.

For more information, see the following additional topics:

- Configuring SNMP Trap Receiving and Forwarding, page 19-4
- Viewing Purge Scheduler Status, page 19-13

Scheduling Operations Manager Tasks

When Operations Manager is first installed, most tasks listed in Table 19-2 are scheduled by default to ensure that they do not run concurrently. You can configure the schedules for these tasks to meet the requirements of your site. However, you should still avoid running them concurrently.

Table 19-2 Scheduling Considerations

Scheduling Task	Default Schedule	Comments and Notes
Database purging	Run daily at midnight.	The amount of time it takes to purge the database depends on the size of the database.
Phone discovery	Run daily at midnight, 04:00, 08:00, 12:00, 16:00, and 20:00.	You should determine how long the last phone discovery took to complete by comparing at the start and end times for the last collection on the IP Phone Discovery Schedule page. See Working with IP Phone Discovery, page 15-22. Knowing how long phone discovery normally takes to complete will help you to schedule.
Inventory collection	Run weekly on Monday at 2:00 a.m.	By default, inventory collection starts 2 hours after database purging.

In addition to configuring schedules with Operations Manager, a system administrator can schedule database backups. You should be careful to coordinate the database backup schedule to avoid running concurrently with the tasks listed in Table 19-2.

For more information about schedules, see the following topics:

- Viewing Purge Scheduler Status, page 19-13
- Backing Up and Restoring Operations Manager Data, page 19-24

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 you must do one of the following:

- Configure SNMP to send traps directly to Operations Manager
- Integrate SNMP trap receiving with an NMS or a trap daemon

To send traps directly to Operations Manager, perform the tasks in the Enabling Devices to Send Traps to Operations Manager, page 19-4. To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 19-5.

Enabling Devices to Send Traps to Operations Manager

Note If your devices send SNMP traps to a Network Management System (NMS) or a trap daemon, see Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 19-5.

Because Operations Manager uses SNMP MIB variables and traps to determine device health, you must configure your 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 appropriate for your device:

- Enabling Cisco IOS-Based Devices to Send Traps to Operations Manager, page 19-4
- Enabling Catalyst Devices to Send SNMP Traps to Operations Manager, page 19-5

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

For devices running Cisco IOS software, provide 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, refer to the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Step 2 Select **Products & Services > Cisco IOS Software**.

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

Step 4 Select **Technical Documentation** and select the appropriate command reference guide.

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, refer to the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Step 2 Select **Products & Services > Cisco Switches**.

Step 3 Select the appropriate Cisco Catalyst series switch.

Step 4 Select **Technical Documentation** and select the appropriate command reference guide.

Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs

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 (NMSs):

- 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 19-4. Specify port 162 as the destination trap port.

  If another NMS is already listening for traps on the standard UDP trap port (162), you must configure Operations Manager to use another port, such as port 9000. See Setting System-Wide Parameters Using System Preferences, page 19-12.

- If your network devices are already sending traps to another management application, configure that application to forward traps to Operations Manager.

Table 19-3 describes scenarios for SNMP trap receiving and lists the advantages of each.

Table 19-3 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. • 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.

Ports and Protocols that Operations Manager Uses

Operations Manager uses the following protocols:

- SNMP
- ICMP
- TCP/IP
- SMTP
- RMI
- HTTP

Operations Manager uses the TCP and UDP ports described in Table 19-4.

Table 19-4 Operations Manager Incoming Ports

Port Number	Usage
162	Default port number used by Operations Manager for receiving traps
40000–41000	Used by Common Transport Mechanism for internal application messaging
42344	Used by Synthetic Testing web service
42350–42353	Used by messaging software
43441–43459	Used as database ports: • Operations Manager uses the following ports: – 43445—Used by Alert History database engine – 43446—Used by inventory service database engine – 43447—Used by event processing database engine – 43449—Used by IP Phone Information Facility database engine – 43459—Used by Service Monitor database engine
9002	Used by the Broker to listen to both the IP telephony server and the device fault server
9009	Default port number used by the IP telephony server for receiving traps from the device fault server

Configuring Service Quality Settings

Service Quality Settings enable you to integrate Service Monitors with Operations Manager.

Note

- IP Communications Service Monitor (Service Monitor) is a separately licensed product that is installed when you install Operations Manager; see your Cisco representative to obtain a license.
- You can license Service Monitor on the same server as Operations Manager. You can also obtain standalone versions of Service Monitor to install and license on other servers.

For Operations Manager to process traps from Service Monitor, you must do both of the following:

- Configure Service Monitor to send traps to Operations Manager. (See *User Guide for IP Communication Service Monitor*.)
- Configure Operations Manager to process traps from particular Service Monitors. See Adding and Deleting Service Monitors, page 19-7. Operations Manager discards any traps received from a Service Monitor that has not been added to Operations Manager.

Service Monitor sends MOS violation traps to Operations Manager when MOS falls below a threshold configured on Service Monitor. In response to these traps, Operations Manager generates a warning alert. To enable Operations Manager to generate a critical alert when MOS falls to a more critical level than that defined by Service Monitor, configure a lower MOS threshold on Operations Manager. See Configuring Service Quality Event Settings, page 19-9.

Adding and Deleting Service Monitors

Use this procedure to specify the Service Monitors for which Operations Manager processes traps. This procedure enables you to add the locally installed Service Monitor and remotely installed Service Monitors.

Step 1 Select **Administration > Service Quality Settings > Service Monitors**. The Service Monitors page appears, displaying the information in the following table.

GUI Element	Action/Description
Check box column	Select to delete a Service Monitor and click the Delete button. **Note** After you delete a Service Monitor, Operations Manager discards any traps received from it.
IP Address column	Server where Service Monitor is installed. **Note** Operations Manager processes traps from *only* those Service Monitors listed here.
Description column	User-entered description.
Add button	Click to add a Service Monitor. See Adding a Service Monitor to Operations Manager, page 19-8.
Configure button	Click to open the Service Monitor home page and configure a Service Monitor. See Configuring a Service Monitor, page 19-9
Delete button	Click to delete Service Monitors that you have selected. See Deleting a Service Monitor from Operations Manager, page 19-8.

Adding a Service Monitor to Operations Manager

Use this procedure to add a locally installed or remotely installed Service Monitor to Operations Manager.

Step 1 Select **Administration > Service Quality Settings > Service Monitors**. 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.
- Remarks—Optional.

Step 4 Click **Add**. The Service Monitor page appears, displaying information for the newly added Service Monitor.

Deleting a Service Monitor from Operations Manager

Use this procedure to delete a locally installed or remotely installed Service Monitor from Operations Manager.

Note After you delete a Service Monitor from Operations Manager, Operations Manager discards any traps received from it.

Step 1 Select **Administration > Service Quality Settings > Service Monitors**. The Service Monitor page appears.

Step 2 Select check boxes for Service Monitors that you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **OK**.

Configuring a Service Monitor

Use this procedure to launch the Service Monitor home page for the selected Service Monitor.

Step 1 Select **Administration > Service Quality Settings > Service Monitors**. The Service Monitor page appears.

Step 2 Select a Service Monitor and click **Configure**. The Service Monitor home page opens.

Note You might be asked to log in.

Step 3 Click **Help** on the Service Monitor home page for more information on using Service Monitor.

Configuring Service Quality Event Settings

Note Service Quality events are displayed on the Service Quality Alert display. See Monitoring Service Quality Alerts, page 4-1.

Use this procedure to configure:

- The MOS level that triggers a CriticalServiceQualityIssue event.

  Service Monitor sends a trap when MOS falls below the threshold configured on Service Monitor. You can configure an event setting on Operations Manager that specifies a lower MOS threshold than the one configured on Service Monitor. When Operations Manager receives a trap with MOS less than or equal to the event setting, Operations Manager generates a CriticalServiceQualityIssue event. When Operations Manager receives a trap with MOS greater than the event setting, Operations Manager generates a ServiceQualityIssue event.
- How often to clear events so that they are no longer displayed on the Service Quality Alert Detail display.
- The number of traps and the number of minutes after which to trigger a MultipleServiceQualityIssue event.

Step 1 Select **Administration > Service Quality Settings > Event Settings**. The Service Quality Event Settings page appears.

Step 2 Enter values in the following fields:

- **Mark the Service Quality Issue event critical when MOS drops below**—Enter the MOS score that should trigger a Service Quality Issue event to critical. The default is 3.5. (The range of MOS values is .1 to 4.9.)

  Note Ensure that you set this MOS score lower than the MOS threshold that is set in Service Monitor.

- **Generate a Multiple Service Quality Issues event when more than `[a]` Service Quality Issue events occur in `[b]` minutes**. Enter the number of:
  - [a]—Service Quality Issue events.
  - [b]—Minutes in which the specified number of Service Quality Issue events must occur for Operations Manager to generate a Multiple Service Quality Issues event.
- **Clear events after**—Select the number of hours after which Operations Manager should clear service quality events so that they do not appear on the Service Quality Alerts dashboard.

  Note After events are cleared, you can continue to view them in service quality event history for the next 31 days. See Getting Started with Service Quality Event History Reports, page 11-14.

Step 3 Click **Save**.

Generating and Understanding the System Status Report

To access a System Status report, select **Administration > System Status**. The System Status Report opens.

To navigate through the System Status Report, use the following:

- Go to field—Select a section of the report from the list. At the end of any section, you can click a Back to Top link.
- Summary—Select a section of the report by clicking any of the following links:
  - Failed Processes
  - Inventory
  - Data Purging
  - Diagnostics: Synthetic Tests
  - Diagnostics: Phone Status Tests
  - Diagnostics: Node-to-Node Tests
  - Notifications
  - System Limits

Note You can also select a section of the report by clicking a View Details link in the summary.

The System Status Report contains the following sections:

- **Failed Processes**—Names of processes that failed.
- **Inventory**—Displays the name, last execution time, status, and next scheduled time for the following types of data collection:
  - Discovery—Identifies new devices and adds them to the DCR. (Optional. Can be scheduled or run as needed.)
  - DCR Domain Status—Adds devices to the DCR from other CiscoWorks servers if Operations Manager is configured to synchronize devices and credentials (rather than working in Isolated mode).
  - Device Selection—Adds devices to those that Operations Manager monitors either automatically—as they are added to the DCR— or when a user manually selects them from the DCR.
  - Device Inventory Collection—Probes devices that Operations Manager monitors to update device components and their status; does not discover devices.
  - Phone Inventory Collection—Discovers and collects information about all IP phones in the network by checking all switches and Cisco CallManagers monitored by Operations Manager; does not discover devices.
- **Data Purging**—Start time, end time, and status for most recent database purging task.
- **Diagnostics: Synthetic Tests**—Tests that failed: Test Name, Test Type, Source (IP address or DNS name), Target (IP address or DNS name), Failure Time, Reason.
- **Diagnostics: Phone Status Tests**—Tests that failed: Test Name, Source Router, Extension, MAC Address, IP Address Failure Time, Reason.
- **Diagnostics: Node-to-Node Tests**—Tests that failed: Test Name, Test Type, Endpoints, Failure Time, Reason.
- **Notifications**—Device Event Description, Event ID, Destination(s), Failure Time, Reason.
- **System Limits**—Current value, Limit value, and Limited By for the following parameters:
  - Devices—Current: Number of devices in Operations Manager monitored inventory. Limit: Number of devices allowed by license.
  - Phones—Current: Number of phones in Operations Manager monitored inventory. Limit: Number of phones allowed by license.
  - IP Communications Service Monitor— Licensed or not licensed.
  - Synthetic Tests.
  - Phone Reachability Tests.
  - Node-to-Node Tests.
  - Devices monitored for performance and capacity.
  - Devices monitored for SRST.

Setting System-Wide Parameters Using System Preferences

From the System Preferences page, you can configure all of the following:

Step 1 Select **Administration > Preferences**. The System Preferences page appears.

Step 2 Enter data described in the following table.

GUI Element	Description/Action
Trap Forwarding Parameters table	(Optional) Enter up to three recipients for pass-through traps: • Trap Server *n* (where *n* is a number from 1 to 3)—Enter an IP address or DNS name. • Port—Enter a port number on which the host can receive traps. **Note** By default, Operations Manager does not forward pass-through traps. For more information see: • Processed and Pass-Through Traps, and Unidentified Traps and Events, page B-1. • Configuring SNMP Trap Receiving and Forwarding, page 19-4.
CiscoWorks Servers table	(Optional) For each CiscoWorks server (RME, Campus, and CiscoView), do the following: • Protocol—Select http (or https if SSL is enabled on the server). • Server—Enter the IP address or DNS name. • Port—Enter the port number used to start CiscoWorks on the server; the port number is usually 1741 when the protocol is https and 443 when the port number is https. **Note** Operations Manager can use this information to launch these CiscoWorks products.
SNMP Trap Community field	Enter a read community string.
Trap Receiving Port field	Enter a port to change the port on which Operations Manager listens for SNMP traps. The default is 162. For more information, see Configuring SNMP Trap Receiving and Forwarding, page 19-4. **Note** For a list of ports that are already in use, see Ports and Protocols that Operations Manager Uses, page 19-6.

GUI Element	Description/Action
Default SMTP Server	Enter a fully qualified SMTP server name for Operations Manager to use when sending e-mail notifications. For more information, see Using Notifications, page 14-1. **Note** See Ensuring that E-Mail Notifications Are Not Blocked, page 19-13.
Daily Purging Schedule	Select the time of day to start purging the Alert History database: • Hour—From 0 to 23 • Minute—From 0 to 50 in 10-minute intervals The default is 00:00. Purging maintains 31 days of data in the database. **Note** Review the information in the Scheduling Operations Manager Tasks, page 19-3 to ensure that daily purging does not conflict with the other scheduled jobs listed there.

Step 3 Click **Apply**.

Ensuring that E-Mail Notifications Are Not Blocked

If you have an antivirus application on the default SMTP server, verify that a port-blocking rule does not stop notification e-mail from being sent. Some antivirus applications use port-blocking to block mass-mailing worms. Delete the port-blocking rule if necessary.

For more information about notification e-mail, see Configuring Subscriptions, page 14-12.

Viewing Purge Scheduler Status

You can check the status of the Operations Manager data purge job from the Job Browser each day after the job runs.

Note You can also check the status of daily purging on the System Status report; see Generating and Understanding the System Status Report, page 19-10.

Step 1 Launch the CiscoWorks home page by clicking the **CiscoWorks** link in the upper right-hand corner of the Operations Manager home page.

Step 2 From the CiscoWorks home page, select **Common Services > Server > Admin > Job Browser**. The Job Browser page appears, displaying a table of scheduled jobs.

Step 3 Look for the Operations Manager:DataPurge job in the Type column and check for information in the Status column.

Note If you delete the Operations Manager:DataPurge job using the Job Browser, purging will not resume until you restart the daemon manager, reboot the server, or reconfigure the daily purging schedule.

Using Logging to Enable and Disable Debugging

Operations Manager writes application log files for all major functional modules. By default, Operations Manager writes only error and fatal messages to these log files. You cannot disable logging. However, you can:

- Collect more data when needed by increasing the logging level
- Return to the default logging level as the norm

Step 1 Select **Administration > Logging**. The Logging Configuration page is displayed.

Note You cannot disable logging. Operations Manager will always write error and fatal messages to application log files.

Step 2 For each Operations Manager functional module, the Error check box is always selected; you cannot deselect it.

To set all modules to Error, the default logging level:

a. Click the **Default** button. A confirmation page is displayed.

b. Click **OK**.

To change the logging level for individual modules:

a. For each module that you want to change, select one (or deselect all) of the following logging levels:

- Warning—Log error messages and warning messages
- Info—Log error, warning, and informational messages
- Debug—Log error, warning, informational, and debug message

Note Deselecting all check boxes for a module returns it to Error, the default logging level.

b. Review your changes. To cancel your changes, click the **Cancel** button. Otherwise, click the **Apply** button. Clicking the **Apply** button starts immediately resetting the changed logging levels for the Operations Manager functional modules.

For information about changing the logging level for the system application MIB, see Viewing the System Application MIB Log File, page 19-30.

Accessing and Deleting Log Files

Each Operations Manager module writes log files to its own folder within the <*NMSROOT*>\log\itemLogs folder. Table 19-5 lists each Operations Manager module, the name of the folder where the log files are stored, and the related log files.

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

When a log file reaches a preset maximum size, the module backs up the file and starts writing to a new log file. The maximum size for a log file varies by module. The maximum number of backed up log files that a module keeps also varies.

Note Operations Manager does not automatically reset the DFMServer log file (DFM.log). To maintain good system performance, back up this file when it grows larger than 30 MB. See Maintaining the DFM Log File, page 19-27.

By default, Operations Manager writes error messages only to log files. You can change the logging level and thereby affect the amount of information stored in log files. To do so, see Using Logging to Enable and Disable Debugging, page 19-14.

Table 19-5 Operations Manager Log Files by Module

Function/Module	Folder in <*NMSROOT*>	Log Files
Alert and Event History	\log\itemLogs\FH	FHUI.log FHCollector.log
Alerts and Events Display	\log\itemLogs\AAD	AAD.log
Application and Connectivity Poller	\log\itemLogs\VHM	VHMPoller.log TISPollerLogger.log
Detailed Device View	\log\itemLogs\DDV	DDV.log
Device Management	\log\itemLogs\tis	DCRAdapter.log DeviceManagement.log TISServer.log
Event Processing Adapters	\log\itemLogs\epa	adapterServer.log dfmEvents.log vhmEvents.log
Event Promulgation Module	\log\itemLogs\EPM	EPM.log
Graphics Utility	\log\itemLogs\TGU	TGU.log TGU_DataProcessor.log
IP Phone Information Facility	\log\ipiu	ipiuapp.log
IP Phone Information Facility Server	\log	pif.log
IP Phone Status	\log\itemLogs\PR	PhoneReachability.log
IP Phone Status Display	\log\itemLogs\PAD	PAD.log
IP SLA Library	\log\itemLogs\IPSLA	STL.log
IPC Discovery	\log\itemLogs\discovery	discovery.log
IPT Health Report	log\itemLogs\ipthr	ipthr.log
Inventory Collection Schedule	\log\itemLogs\Rediscovery	Rediscovery.log

Table 19-5 Operations Manager Log Files by Module (continued)

Function/Module	Folder in <*NMSROOT*>	Log Files
Inventory Collector	\log\itemLogs\vhm	connectivityProgress.log DFMCollector.log InventoryCollector.log Poller.log TISPollerLogger.log VHMGSUPoller.log VHMIntegrator.log
Inventory Interactor	\log\itemLogs\vhm	CiscoCallManagerOrClusterGrouping.log Interactor.log
Inventory Service	\log\itemLogs\tis	DCRAdapter.log TISServer.log
Node-to-Node Tests Common Utilities	\log\itemLogs\IPSLA	DAL.log plib.log
Node-to-Node Tests Data Poller	\log\itemLogs\IPSLA	WPUSS.log WPU_DataPoller.log
Node-to-Node Tests Device Management	\log\itemLogs\IPSLA	DMAudit.log WPUDM.log
Node-to-Node Tests Management	\log\itemLogs\IPSLA	SM.log SMAudit.log
Notification Services	\log\itemLogs\nots	nots.log notifications_audit.log notifications_failures.log notifications_success.log
PTM Adapter for Data Settings	\log\itemLogs\cfi	PollingThresholdAdapter.log
PTM Adapter for Voice Settings	\log\itemLogs\vhm	VHMPollingThresholdAdapter.log
Polling and Threshold Manager	\log\itemLogs\PTM	PTMClient.log PTMDB.log PTMOGS.log PTMPTA.log PTMServer.log
Purging Scheduler	\log\itemLogs\DPS	DPS.log

Table 19-5 Operations Manager Log Files by Module (continued)

Function/Module	Folder in <*NMSROOT*>	Log Files
SRST Monitoring	\log\itemLogs\srst	srst_audit.log srst_import_errors.log srst_test_creation_results.log srst_import.log srst_ui.log srst_server.log
Self Diagnostic Report	\log\itemLogs\sdr	sdr.log
Service Impact Reports Server	\log\itemLogs\sir	sir.log
Service Level View Server	\log\itemLogs\topo	Topology_Client.log Topology_Server.log
Service Quality Alerts Display	\log\itemLogs\QOVAD	QOVAD.log
Service Quality Manager	\log\itemLogs\QoVM	QoVMServer.log
Synthetic Testing Server	\log	STServer.log
Synthetic Testing UI	\log	ct-ui.log
View Manager	\log\itemLogs\VGM	vgm.log
View Severity Manager	\log\itemLogs\vsm	AlertInfo.log GroupHandler.log UserInfo.log vsmServer.log

Note The Operations Manager application logging service also maintains log files under the following folder: <*NMSROOT*>\log\itemLogs.

Security Considerations

These topics address some important Operations Manager security issues:

- File Ownership and Protection, page 19-17
- SSL, page 19-18
- SNMPv3, page 19-18
- Changing the Password for Operations Manager Databases, page 19-18

File Ownership and Protection

Security for Operations Manager files is based on the same standards used for CiscoWorks.

Caution Do not change the protection of any file or directory to be less restrictive. You may, if you wish, make the protections more restrictive.

All Operations Manager files are installed with owner CASUSER. Only CASUSER can create, delete, or edit the files installed in *NMSROOT*. *NMSROOT* is the directory where CiscoWorks is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

Note File protections are not enforced on FAT partitions.

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. You can enable or disable SSL depending on the need to use secure access.

Operations Manager supports SSL between clients and the server. By default, Operations Manager is not SSL-enabled. For information on enabling SSL, refer to the Common Services online help.

SNMPv3

Like CiscoWorks Common Services, Operations Manager supports SNMPv3 (authentication and access control but no data encryption) between server and devices to eliminate leakage of confidential info. This provides packet-level security, integrity protection, and replay protection, but does not encrypt the packets.

Changing the Password for Operations Manager Databases

Before You Begin

The procedure in this topic enables you to change the password for the following Operations Manager databases:

- itemEPM—Event promulgation
- itemFH—Alert History
- itemInv—Inventory
- itemIpiu—IP phone information
- qovr—IP Communications Service Monitor

Step 1 At the command prompt on the Operations Manager server, stop the daemon manager by entering the following command:

```
net stop crmdmgmt
```

Step 2 Change directory to *NMSROOT*\conf\itemDb\bin. For example:

```
cd Program Files\CSCOpx\conf\itemDb\bin
```

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

Step 3 Enter ChangeItemDbPasswd.pl, providing a new password as input. For example:

```
ChangeItemDbPasswd.pl newpassword
```

Step 4 Restart the daemon manager by entering the following command:

```
net start crmdmgmt
```

Device Support

When support for new devices becomes available for Operations Manager, Incremental Device Updates (IDUs) will be announced on the planner page for Operations Manager on Cisco.com. Visit the planner page for announcements, downloads, and installation instructions for IDUs as they become available.

When a new IDU becomes available, you can download it from Cisco.com.

Performing System Administration Tasks

You can use CiscoWorks to perform many system administration tasks, including the following:

- Launching the CiscoWorks Home Page, page 19-19
- Configuring Users (ACS and Non-ACS), page 19-19
- Creating Self-Signed Security Certificates Yearly, page 19-23
- Backing Up and Restoring Operations Manager Data, page 19-24
- Changing the Password for Operations Manager Databases, page 19-18
- Starting and Stopping Operations Manager Processes, page 19-25

Launching the CiscoWorks Home Page

Step 1 Click the CiscoWorks link in the upper right-hand corner of the Operations Manager home page. The CiscoWorks home page opens.

Configuring Users (ACS and Non-ACS)

The CiscoWorks server provides the mechanism for authenticating and authorizing users for CiscoWorks applications. What users can see and do is determined by their user role. System Administrators can configure user roles from the CiscoWorks home page by selecting **Server > Security > Single-Server Management > Local User Setup**. From here you can add, edit, or delete users.

The CiscoWorks server provides two different mechanisms or *modes* for authenticating users for CiscoWorks applications:

- CiscoWorks Local Mode—By default, the CiscoWorks server uses CiscoWorks Local mode, or *non-ACS mode*. In CiscoWorks Local mode, CiscoWorks assigns roles, along with privileges associated with those roles, as described in the Common Services Permission Report. (You can generate a Permission Report from the Common Services home page by selecting **Server > Reports > Permission Report** and clicking **Help**.) For more information, refer to Configuring Users Using CiscoWorks Local Mode, page 19-20.
- CiscoSecure Access Control Server (ACS) Mode—ACS specifies the privileges associated with roles; however, ACS also allows you to perform device-based filtering, so that users only see devices they are authorized to see. Using ACS, which is called *ACS mode*, is supported when ACS is installed on your network and Operations Manager is registered with ACS. For more information, refer to Configuring Users Using ACS Mode, page 19-20.

If Common Services is using ACS mode, Operations Manager must also use ACS mode; otherwise, Operations Manager users will not have any permissions. However, if another instance of Operations Manager is already integrated with ACS, the new Operations Manager will also be integrated with ACS.

Configuring Users Using CiscoWorks Local Mode

Use this procedure to add a user and specify a user role using CiscoWorks Local Mode.

Step 1 Select **Administration > Add Users**. The Common Services Local User Setup window opens.

Step 2 Click the Help button on the Local User Setup window for information on the configuration steps.

Use the CiscoWorks Permission Report to understand how each user role relates to tasks in Operations Manager. From the Common Services home page, select **Server > Reports > Permission Report > Generate Report** and scroll down until you find IP Communications Operations Manager.

Configuring Users Using ACS Mode

To use this mode for Operations Manager, Cisco Secure ACS must be installed on your network, and Operations Manager must be registered with ACS.

Step 1 Verify which mode the CiscoWorks server is using. From the Common Services home page, select **Server > Security > AAA Mode Setup** and check which Type radio button is selected: ACS or Non-ACS.

Step 2 Verify whether Operations Manager is registered with ACS (if ACS is selected) by checking the ACS server.

Step 3 To edit ACS roles:

- Refer to the ACS online help (on the ACS server) for information on editing roles.
- Refer to the Common Services online help for information on the implications of ACS on the DCR (specifically, role dependencies).

Note If you edit Operations Manager roles using ACS, your changes will be propagated to all other instances of Operations Manager that are using Common Services servers that are registered with the same ACS server.

Using Operations Manager in ACS Mode

Before performing any tasks that are mentioned here, you must ensure that you have successfully completed configuring Cisco Secure ACS with the CiscoWorks server. If you have installed Operations Manager after configuring the CiscoWorks Login Module to ACS mode, then Operations Manager users are not granted any permissions. However, the Operations Manager application is registered to Cisco Secure ACS.

Note The System Identity Setup user that is defined in the CiscoWorks server must be added to the Cisco Secure ACS, and this user must have Network Administrator privileges.

CiscoWorks login modules allow you to add new users using a source of authentication other than the native CiscoWorks server mechanism (that is, the CiscoWorks Local login module). You can use the Cisco Secure ACS services for this purpose.

By default, the CiscoWorks server authentication scheme has five roles in ACS mode. They are listed here from least privileged to most privileged:

Help Desk	User with this role has the privilege to access network status information from the persisted data. User does not have the privilege to contact any device or schedule a job that will reach the network. Example: Launch Service Level View.
Approver	User with this role has the privilege to approve all Operations Manager tasks. User can also perform all the Help Desk tasks. Example: Launch Alerts and Events.
Network Operator	User with this role has the privilege to perform all tasks that involve collecting data from the network. User does not have write access on the network. User can also perform all the Approver tasks. Example: Add a synthetic test.
Network Administrator	User with this role has the privilege to change the network. User can also perform Network Operator tasks. Example: Set the default view for Service Level View.
System Administrator	User with this role has the privilege to perform all CiscoWorks system administration tasks. See the Permission Report from CiscoWorks home page (**Common Services > Server > Reports > Permission Report**). Example: Configure LDAP.

Cisco Secure ACS allows you to edit the privileges for these roles. You can also create custom roles and privileges that help you customize Common Services client applications to best suit your business workflow and needs.

To edit the default CiscoWorks privileges, see Cisco Secure ACS online help. (On Cisco Secure ACS, click **Online Documentation > Shared Profile Components > Command Authorization Sets**.)

Editing CiscoWorks Roles and Privileges in Cisco Secure ACS

If another instance of Operations Manager is registered with the same Cisco Secure ACS, your instance of Operations Manager will inherit those role settings. Furthermore, any changes you make to Operations Manager roles will be propagated to other instances of Operations Manager through Cisco Secure ACS. If you reinstall Operations Manager, your Cisco Secure ACS settings will automatically be applied upon Operations Manager restart.

Step 1 Select **Shared Profile Components >** Operations Manager and click on the Operations Manager roles that you want to edit.

Step 2 Select or deselect any of the Operations Manager tasks that suit your business workflow and needs.

Step 3 Click **Submit**.

Device-Based Filtering

You can configure ACS to restrict access to all Operations Manager displays. You can also configure ACS to restrict access to devices and applications. Device-based and application-based filtering affects:

- Devices—To be able to view information for a device, configure the device, and configure diagnostic tests that involve the device, you must have access to it.
- Phones—To be able to view information for a phone, you must have access to either the switch connected to the phone or to the Cisco CallManager to which the phone is registered.

Note ACS does not perform any filtering on VLANs.

Note Device-based filtering is not performed at the Cisco CallManager cluster level. All users can see cluster-level alerts and Alert History.

Device-based filtering can only be performed on the following Operations Manager displays:

- **Monitoring Dashboards**—All displays.
- **Diagnostics**—All displays.
- **Device Management**—All displays.

Note If any user starts the inventory collection process, all devices managed by Operations Manager are probed (not just those for which the user has access).

- **Notifications > Notification Criteria**.

Note If you update device access in ACS, Operations Manager does not update running notifications.

- **Reports**:
  - **Alert and Event History**—All displays.
  - **Service Quality History**—All displays.
- **Administration > Polling and Thresholds**

Note Only the Polling Parameters Summary and the Thresholds Parameters Summary pages are filtered.

Most Operations Manager tasks are device-centric. The devices listed for you while performing the Operations Manager tasks are based on your role and associated privileges, defined in Cisco Secure ACS.

Note Refer to the Common Services online help for important information on how ACS custom roles affect the DCR and device-based filtering.

Creating Self-Signed Security Certificates Yearly

When you install Operations Manager, Operations Manager creates a self-signed security certificate on the server. Users on some client systems must install the certificate; see Responding to Security Alerts, page 1-21. Self-signed security certificates expire one year from the date of creation.

Create a new self-signed security certificate yearly before the certificate expires. You can also do so after the certificate expires; however, users might not be able to access Operations Manager until you complete this task.

Step 1 Select **Common Services > Server > Admin > Security Management > Create Self Signed Certificates**. The Create Certificates page appears.

Step 2 Enter the values for the fields described in the following table.

Field	Description	Usage Notes
Country Name	Name of your country	Use two-character country code.
State or Province	Name of your state or province	Use two-character state or province code or complete name of state or province.
Locality	Name of your city or town	Use two-character city or town code or complete name of city or town.
Organization Name	Name of your organization	Use complete name or abbreviation for your organization.
Organization Unit Name	Name of department in your organization	Use complete name or abbreviation for your department.
Host Name	Name of server on which Operations Manager is installed	Use the DNS name of the server. **Note** Use the proper domain name, which should already be displayed in the Host Name field.
Email Address	Your e-mail address	—

Step 3 Click **Submit**. (Alternatively, click **Restore to Default** to clear all fields and re-enter information.)

Backing Up and Restoring Operations Manager Data

This topic explains how to access the backup applications, such as Back Up Data Now and Schedule Backup. This topic also explains how to locate the online help procedures for restoring data.

Step 1 From the CiscoWorks home page, select **Common Services > Server > Admin > Backup**. The Backup Job page appears.

Step 2 Click the Help button and follow the instructions for backing up and restoring data.

Database files are stored using the backup directory structure described in Table 19-6.

- Format—*/generation_number/suite/directory/filename*
- Example—/1/itemFh/database/itemFh.db

Table 19-6 Operations Manager Backup Directory Structure

Option	Description	Usage Notes
generationNumber	Backup number	For example, 1, 2, and 3, with 3 being the latest database backup.
suite	Application, function, or module	When you perform a backup, data for all suites is backed up. The CiscoWorks server suite is cmf. The Operations Manager application suites are: • dfm—Data collection and analysis for devices in IP infrastructure • itemEpm—Event promulgation • itemFh—Alert history • itemInv—Device inventory • itemIPIU—Phone information • qovr—Service quality • vhm—Data collection and analysis for voice-enabled devices • wpu—Node-to-Node tests.
directory	What is being stored	Each application or suite listed. Directories include database and any suite applications.
filename	File that has been backed up	Files include database (.db), log (.log), version (DbVersion.txt), manifest (.txt), tar (.tar), and data files (datafiles.txt).

Starting and Stopping Operations Manager Processes

Note You cannot stop or unregister a process if any process that depends on it is running. You must first stop or unregister all dependent processes, and then stop or unregister the process.

Step 1 Log in to Operations Manager as a system administrator and launch the CiscoWorks home page.

Step 2 Select **Common Services > Server > Admin > Processes**. The Process Management page appears.

Note If a process is not listed, it has not yet been started.

Step 3 Do one of the following:

- Select check boxes next to processes that are running and click **Stop**.
- Select check boxes next to processes that are stopped and click **Start**.

Table 19-7 provides a complete list of Operations Manager-related CiscoWorks processes.

Table 19-7 Operations Manager-Related CiscoWorks Processes

Name	Description	Dependency
AdapterServer	Event adapter takes events from backend servers.	None
DataPurge	Database and data file purging.	jrm
DfmBroker	DFM Broker maintains a registry about VHM and DFM domain managers. A domain manager registers the following information with the broker when its initialization is complete: • Application name of the domain manager • Hostname where the domain manager is running • TCP port at which the HTTP server is listening When a client needs to connect to the domain manager, it first connects to the broker to determine the hostname and TCP port where that server's HTTP service is listening. It then disconnects from the broker and establishes a connection to the domain manager.	None
DfmServer	Infrastructure device domain manager, a program that provides backend services for Operations Manager. Services include SNMP data retrieval and event analysis. The DfmServer log is *NMSROOT*/objects/smarts/logs/DFM.log. For more information, see Maintaining the DFM Log File, page 19-27.	DfmBroker
EPMDbEngine	Event Promulgation Module (EPM) database engine—Repository for the EPM module.	None
EPMDbMonitor	EPM database monitor.	EPMDbEngine
EPMServer	Sends events to notification services.	EPMDbEngine
FHDbEngine	Alert History database engine—Repository for alerts and events.	None
FHDbMonitor	Alert History database monitor.	FHDbEngine
FHPurgeTask	Alert History purge task.	None
FHServer	Alert History server.	FHDbMonitor, FHDbEngine, EPMDbEngine, EPMServer
GPF	Performance and capacity monitoring data collection.	ITMOGSServer, INVDbEngine
GpfPurgeTask	Purges performance polling records.	None
INVDbEngine	Device inventory database engine.	None
INVDbMonitor	Device inventory database monitor.	INVDbEngine
InventoryCollector	Phone inventory collector.	EssMonitor
IPCDiscovery	Physical device discovery.	None.
IPIUDataServer	Provides information about IP phones.	ESS
IPIUDbEngine	Phone inventory database engine.	None
IPIUDbMonitor	Phone inventory database monitor.	IPIUDbEngine
IPSLAPurgeTask	Purges node-to-node test records.	None

Table 19-7 Operations Manager-Related CiscoWorks Processes (continued)

Name	Description	Dependency
IPSLAServer	Node-to-node test server.	INVDbMonitor, InventoryCollector
ITMCTMStartup	Internal communication process.	None
ITMDiagServer	Diagnostics server.	INVDbEngine, ESS
ITMOGSServer	Operations Manager Object Grouping Service server evaluates group membership.	CmfDbEngine, ESS, DCRServer
IVR	Internal process.	None
NOTSServer	Notification server monitors alerts and sends notifications based on subscriptions.	EPMDbEngine, EPMServer, INVDbEngine, ITMOGSServer
PIFServer	Performs phone discovery, CDP neighbor discovery, monitoring, and phone reachability.	PIFDbEngine, ESS
PTMServer	Polling and thresholds server.	ITMOGSServer
QoVMServer	Service Monitor server.	ESS
QOVR	Service Quality alerts process.	QOVRDbMonitor
QOVRDbEngine	Service Monitor database engine.	None
QOVRDbMonitor	Service Monitor database monitor.	QOVRDbEngine
QOVRMultiProcLogger	Service Monitor logging.	None
SDRPurgeTask	Purges Self-Diagnostic Reports.	None
SIRServer	Voice model and rule-based engine for generating Service Impact Reports.	EPMDbEngine, ESS.
SRSTServer	Configures and runs SRST tests.	PIFServer, PMServer, ESS, TISServer
STServer	Periodically runs synthetic tests against Cisco CallManagers and provides real-time status updates to Operations Manager.	INVDbEngine, ESS
TISServer	Inventory server.	INVDbEngine, EssMonitor
TopoServer	Service level view server.	SIRServer, ITMOGSServer
VHMIntegrator	Integrates voice and infrastructure data.	ESS
VHMServer	Maintains voice data.	DfmBroker
VsmServer	Maintains and evaluates views.	ITMOGSServer

Maintaining the DFM Log File

If the DFM.log file grows larger than 30 MB, there is a risk of Operations Manager performance problems. To prevent such problems, you should back up the log file and start a new one.

Step 1 Stop the CiscoWorks daemon manager by entering the following command:

```
net stop crmdmgtd
```

Step 2 Rename the DFM.log file or copy it to a new location and delete it from the Operations Manager server. You can find the DFM.log file in the *NMSROOT*/objects/smarts/logs/ directory.

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

Step 3 Allow 15 minutes to elapse from the time you completed step 1, then restart the CiscoWorks daemon manager by entering the following command:

```
net start crmdmgtd
```

A new DFM.log file will be created.

Using SNMP to Monitor Operations Manager

Operations Manager supports the host resources and system application MIBs. This support enables you to monitor Operations Manager using a third-party SNMP management tool, so that you can:

- Consistently monitor multiple platforms—One platform on which Operations Manager resides and one or more on which applications in the IP Telephony Environment Monitor (ITEM) suite reside.
- Access complete hardware and operating system information using the host resources MIB.
- Assess application health using the system application MIB, which provides the following information:
  - Applications that Operations Manager installed.
  - Processes associated with applications and current process status.
  - Processes that ran previously and application exit state.

For MIB implementation details and sample MIB walk, see Appendix H, “Operations Manager Support for SNMP MIBs.”

Note You cannot uninstall MIB support; however, you can stop Windows SNMP service and set the startup type to either Manual or Disabled. See Enabling and Disabling Windows SNMP Service, page 19-29.

Configuring Your System for SNMP Queries

To enable SNMP queries, SNMP service must be installed and enabled.

Step 1 Verify that SNMP service is installed and enabled on the server where Operations Manager is installed. See Determining the Status of Windows SNMP Service, page 19-29.

Step 2 If you determined that SNMP service was not installed, install Windows SNMP Service; see Installing and Uninstalling Windows SNMP Service, page 19-29.

Determining the Status of Windows SNMP Service

Windows SNMP service is a Windows component that you can add or remove when you want to. To enable SNMP queries against the MIBs that Operations Manager supports, SNMP service must be installed and enabled. You can verify the status of Windows SNMP service as follows.

Step 1 Open the Windows administrative tool Services window.

Step 2 Verify the following:

- SNMP Service is displayed on the Windows administrative tool Services window; if so, Windows SNMP service is installed.

  Note To install Windows SNMP service, see Installing and Uninstalling Windows SNMP Service, page 19-29.

- SNMP Service startup type is Automatic or Manual; if so, Windows SNMP service is enabled.

  Note To enable Windows SNMP service, see Enabling and Disabling Windows SNMP Service, page 19-29.

Installing and Uninstalling Windows SNMP Service

Windows online help provides instructions for adding and removing Windows components, such as Windows SNMP service. To locate the instructions, try selecting the Index tab in Windows online help and entering a keyword or phrase, such as *installing SNMP service*.

To uninstall Windows SNMP service, follow instructions in Windows help for removing Windows components.

Note When you uninstall Windows SNMP service from the server where Operations Manager is installed, you also remove support for the host resources and system application MIBs. If you want to install support again, see Configuring Your System for SNMP Queries, page 19-28.

Enabling and Disabling Windows SNMP Service

You can enable or disable Windows SNMP service using the Windows administrative tool Services. For instructions to open the Services window, see Windows online help.

Step 1 Locate SNMP Service in the Services window. The status and startup type are displayed.

Note If SNMP Service is not displayed, Windows SNMP service is not installed; see Installing and Uninstalling Windows SNMP Service, page 19-29.

Step 2 Right-click SNMP Service and select Properties. The SNMP Service Properties window opens:

- To disable SNMP service, set Startup Type to Disable and click **OK**.
- To enable SNMP service, set Startup Type to Automatic or Manual and click **OK**.

Note To start SNMP service after you enable it, right-click SNMP Service and select Start.

Configuring Security for SNMP Queries

To improve security, the SNMP set operation is not allowed on any object ID (OID). You should also edit the credentials for SNMP service to not use a default or well-known community string.

Note You do not need to restart SNMP service to edit credentials for it.

You can edit SNMP service credentials using the Windows administrative tool Services.

Step 1 Locate SNMP Service in the Services window.

Step 2 Right-click SNMP Service and select Properties. The SNMP Service Properties window opens.

Step 3 Select the Security tab.

Step 4 Edit the accepted community names and click **OK**.

Viewing the System Application MIB Log File

The system application MIB log file, SysAppl.log, is located on the server where Operations Manager is installed in *NMSROOT*\log.

Note NMSROOT is the directory where CiscoWorks is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

Changing the Hostname on the Operations Manager Server

To change the hostname on the Operations Manager server, you must update several files, reboot the server, and regenerate the self-signed security certificate. Afterward, if you have a licensed copy of Service Monitor, you must update the configuration for it.

Note You will reboot the server twice during this procedure. You will also stop the CiscoWorks daemon manager and syslog manager to perform some steps.

Step 1 Change the hostname on the server as follows:

a. Stop the CiscoWorks daemon manager by entering the following command:

```
net stop crmdmgtd
```

b. Change the hostname at **My Computer > Properties > Computer Name > Change**.

c. Prevent the daemon manager and syslog manager services from restarting after reboot. From Control Panel, or from Start, open Services and change the startup mode to Manual for both of these services:

- CW2000 Daemon Manager
- CWCS syslog service

d. Reboot the server.

Step 2 Change the hostname in the md.properties file (*NMSROOT*\lib\classpath\md.properties).

Note NMSROOT is the directory where you installed Operations Manager. If you selected the default, it is C:\Program Files\CSCOpx.

Step 3 Change the hostname in the following registry entries:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet.
- HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager.

Note Look for all instances of the old hostname under these registry entries, and replace them with the new hostname.

Step 4 Change the hostname in these files:

- regdaemon.xml (*NMSROOT*\MDC\etc\regdaemon.xml):
  - Note the old hostname. You will need it to complete Step 5.
  - Enter the new hostname in uppercase.
- web.xml (*NMSROOT*\MDC\tomcat\webapps\classic\WEB-INF\web.xml).

Step 5 Create a file, *NMSROOT*\conf\cmic\changehostname.info, containing the old hostname and new hostname in uppercase in the following format:

```
OLDHOSTNAME:NEWHOSTNAME
```

Note Hostnames in this file are case-sensitive; they must be entered in uppercase; the new hostname must exactly match the hostname entered in regdaemon.xml.

Step 6 Delete the gatekeeper.ior file from this directory:

NMSROOT\www\classpath

Step 7 Change all occurrences of the old hostname in the following files:

- *NMSROOT*\objects\vhmsmarts\local\conf\runcmd_env.sh
- *NMSROOT*\conf\dfm\Broker.info

Step 8 If you do not know the password for the cmf database, reset the password as follows:

a. Open a Command Prompt and go to NMSROOT\bin.

b. Enter the following command:

```
perl dbpasswd.pl dsn=cmf npwd=newpassword
```

where newpassword is the new password.

Note Remember this password. You will need it to complete Step 9.

Step 9 To ensure that devices added before you changed the hostname are properly classified in Device Center, enter the following command:

```
dbisqlc -c "uid=cmfDBA;pwd=dbpassword;eng=cmfEng;dsn=cmf;dbf=NMSROOT\databases\cmf\cmf.db"
-q update PIDM_app_device_map SET app_hostname=`NewhostName' where
app_hostname=`OldhostName'
```

where:

- dbpassword is the Common Services database password.
- NMSROOT is the directory where you installed Operations Manager.
- NewhostName is the new hostname.
- OldhostName is the old hostname.

Step 10 From the Control Panel, or from Start, open Services and change the startup mode to Automatic for both of these services:

- CW2000 Daemon Manager
- CWCS syslog service

Step 11 Reboot the server.

Step 12 Replace the old hostname with the new hostname in the self-signed security certificate and regenerate it by selecting **Common Services > Server > Security > Certificate Setup**.

For more information, click Help.

Step 13 If you have a license for Service Monitor, reconfigure it:

a. Open the Service Monitor home page. (See Configuring a Service Monitor, page 19-9.)

b. Click Help and follow the instructions in the topic *Reconfiguring Service Monitor after a Hostname Change.*

Note Service Monitor online help provides detailed instructions for accomplishing the following tasks:

- Change the IP address or hostname in each of the following configuration files:
  - The default configuration file.
  - The specific configuration file for each Cisco 1040 managed by the Service Monitor.
- Copy the updated configuration files from the Service Monitor server to the TFTP server.
- Reset the Cisco 1040s.
- If Service Monitor is configured to send traps to Operations Manager:
  - If Operations Manager is installed on the same server as Service Monitor, set up Service Monitor to send traps to the new hostname or IP address.
  - If Operations Manager is installed on another server, on Operations Manager, delete the Service Monitor and add it again.

Changing the IP Address on the Operations Manager Server

Step 1 Stop the CiscoWorks daemon manager by entering the following command:

```
net stop crmdmgtd
```

Step 2 Delete the gatekeeper.ior file from this directory:

NMSROOT\www\classpath

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

Step 3 Change the IP address of the Operations Manager server.

Step 4 Allow 15 minutes to elapse from the time you completed step 1, then restart the CiscoWorks daemon manager by entering the following command:

```
net start crmdmgtd
```