



Administering the System and Managing Data

This section contains the following topics:

- [Understanding Service Monitor Database Purging, page 6-1](#)
- [Understanding Sensor Archive File Purging, page 6-3](#)
- [Managing Log Files, page 6-3](#)
- [Configuring Users \(ACS and Non-ACS\), page 6-5](#)
- [Starting and Stopping Service Monitor Processes, page 6-8](#)
- [Using SNMP to Monitor Service Monitor, page 6-8](#)
- [Changing the Hostname on the Service Monitor Server, page 6-11](#)
- [Changing the IP Address on the Service Monitor Server, page 6-13](#)
- [Changing the Time on the Service Monitor Server, page 6-14](#)

Understanding Service Monitor Database Purging

Cisco Unified Service Monitor (Service Monitor) can receive, process, and store call metrics in its database from these sources:

- The Cisco 1040s that are registered to it.
- The Cisco Unified CallManager clusters that are configured to allow database access to Service Monitor or to send data to Service Monitor (when configured as an Application Billing Server). For more information, see [Cisco Unified CallManager Configuration, page B-1](#).

Service Monitor stores the data for 30 days and runs a job daily to purge older data from the database. You can back up and restore the entire Service Monitor database.

-

Starting a Database Backup

Use this procedure to perform an immediate backup or a scheduled backup of the Service Monitor database.

-
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
- Step 2** In the Common Services pane, select **Server > Admin > Backup**, click Help, and follow the instructions.
-

Restoring the Database

To restore the database, you must use the command-line interface (instructions are available in online help) and you need to know the backup directory structure, which is described in [Table 6-1](#).

Use this procedure to locate the online help for restoring the database.

-
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
- Step 2** In the Common Services pane, select **Server > Admin > Backup**, click Help, and click the Help link to the Restoring Data topic.
-



Note

When you restore the database, logging settings return to the default value. As a result, only error messages are written to the log files. If you need additional information written to your log files to debug a problem, reset your logging settings. See [Managing Log Files and Enabling and Disabling Debugging](#), page 6-4.

The backup directory structure for the Service Monitor database includes the suite name, which is *qovr*:

- Format—*/generation_number/suite[/directory]/filename*
- Example—*/1/qovr/qovr.db*

The backup directory structure is described in [Table 6-1](#).

Table 6-1 Service Monitor 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 Service Monitor application suite is <i>qovr</i> .
directory	What is being stored	Suite applications (if applicable).
filename	Specific file that has been backed up	Files include database (.db). For Service Monitor, the following file is listed directly under <i>generationNumber/suite</i> : <i>qovr.db</i>

Changing the Password for the Service Monitor Database

A command line script is available to change database passwords, including the password for the Service Monitor database, `govr.db`. Instructions are available in online help.

-
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
- Step 2** Click Help. The help window opens.
- Step 3** Select the Index tab, scroll down to the entries for D, and select *database password changes*.
-

Understanding Sensor Archive File Purging

**Note**

This topic is applicable to systems with sensors.

Optionally, Service Monitor archives call metrics data to files in a directory on the server. To enable and disable archiving, see [Setting Up the Sensor Default Configuration, page 4-4](#).

When archiving is enabled, by default, Service Monitor does the following:

- Creates a new data file daily at midnight.
- Creates a new data file whenever the current data file size exceeds 3 MB. When a file reaches this limit, Service Monitor does the following:
 - Backs it up—Appends *.n* to the filetype; for example, *.csv.1*, *.csv.2*, and so on up to the limit of 50 per day.
 - Creates a new data file—Retains the original filetype: *(.csv)*.
- Retains the data files for 30 days before deleting them. If you want to retain the data files for a longer period, you can back up the Service Monitor data files using the same method you use to back up your file system. (Common Services backs up the Service Monitor database only and does not include Service Monitor data files.)

Managing Log Files

This section includes the following topics:

- [Understanding Sensor Syslog Handling, page 6-3](#)
- [Maintaining the Sensor History Log File, page 6-4](#)
- [Managing Log Files and Enabling and Disabling Debugging, page 6-4](#)

Understanding Sensor Syslog Handling

Service Monitor receives and processes syslog messages from Cisco 1040s. After processing syslog messages, Service Monitor writes them to the syslog file, `syslog.log`, in `NMSROOT\log\govr`.

Maintaining the Sensor History Log File

The history log file, `ServiceMonitorHistory.log`, contains records of Cisco 1040 events such as Cisco 1040 reset, configuration update, and errors. The history log file accumulates records and grows in size. If the file becomes too large, you should rename it to enable Service Monitor to start a fresh history log file.


Note

Service Monitor does not back up the history log file. If you want to back it up, use the same method you use to back up your file system.

Managing Log Files and Enabling and Disabling Debugging

This information is provided for troubleshooting purposes. Service Monitor log files (see [Table 6-2](#)) are located in the `NMSROOT\log\qovr` directory.


Note

`NMSROOT` is the folder where Service Monitor is installed on the server. If you selected the default directory during installation, it is `C:\Program Files\CSCOpX`.

Use this procedure to increase or decrease the type—and quantity—of messages written to log files.

Step 1 From the Service Monitor home page, select **Logging**. The Logging: Level Configuration page appears.


Note

You cannot disable logging. Service Monitor always writes error and fatal messages to application log files.

Step 2 For each Service Monitor functional module, the Error check box is always selected; you cannot deselect it. For a list of modules and related log files, see [Table 6-2](#).

To set all modules to Error, which is 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
 - Informational—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 Service Monitor functional modules.

Table 6-2 lists Service Monitor log files by function or module. If you request assistance, the Technical Assistance Center (TAC) might ask you to send them some of these log files.

Table 6-2 Service Monitor Log Files by Module

Function/Module	Log Files
Data Handler	DataHandler.log DataHandler_stdout.log DataHandler_sterr.log dhError.log LicenseCheck.log ServiceMonitorHistory.log tftpmanager.log trapgen.log
Reports	CVTQReports.log SensorReports.log Note These files are located in NMSROOT\log\qovr\reports.
Skinny Communication	SkinnyServer.log
User Interface	QovrUI.log

Configuring Users (ACS and Non-ACS)

What Service Monitor users can see and do is determined by the user role. There are two different mechanisms or *modes* for authenticating users:

- **Non-ACS**—You select a supported login module to provide authentication and authorization. By default, Common Services uses the CiscoWorks Local login module to assign roles, along with privileges associated with those roles, as described in the Permission Report. (You can generate a Permission Report by clicking the CiscoWorks link in the upper-right corner of the Service Monitor home page and selecting **Common Services > Server > Reports > Permission Report > Generate Report**.) For more information, refer to [Configuring Users Using Non-ACS Mode \(CiscoWorks Local Login Module\)](#), page 6-6.
- **ACS**—In ACS mode, authentication and authorization is provided by Cisco Secure Access Control Server (ACS). Cisco Secure ACS specifies the privileges associated with roles; however, Cisco Secure ACS also enables you to perform device-based filtering, so that users only see authorized devices. To use ACS mode, Cisco Secure ACS must be installed on your network and Service Monitor must be registered with Cisco Secure ACS. For more information, refer to [Configuring Users Using ACS Mode](#), page 6-6.

If Operations Manager uses ACS mode for authentication and authorization and Service Monitor is running on the same system, Service Monitor must also use ACS mode; otherwise, Service Monitor users will not have any permissions.

Configuring Users Using Non-ACS Mode (CiscoWorks Local Login Module)

To add a user and specify the user role using CiscoWorks Local login module, select **Administration > Add Users**. After the Common Services Local User Setup window opens, click the Help button for information on the configuration steps.

Use the Permission Report to understand how each user role relates to tasks in Service Monitor.

-
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
 - Step 2** Select **Common Services > Server > Reports > Permission Report > Generate Report**.
 - Step 3** Scroll down until you find Cisco Unified Service Monitor.
-

Configuring Users Using ACS Mode

To use ACS mode for authentication and authorization, Cisco Secure ACS must be installed on your network and Service Monitor must be registered with Cisco Secure ACS.

-
- Step 1** Verify the authentication, authorization, and accounting (AAA) mode:
 - a.** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window appears.
 - b.** Select **Server > Security > AAA Mode Setup** and check which Type radio button is selected: ACS or Non-ACS.



Note If you select ACS mode, also select the Register all installed applications with ACS check box. Doing so ensures that Service Monitor tasks are exported to the Cisco Secure ACS server.

- Step 2** Verify whether Service Monitor is registered with Cisco Secure ACS (if ACS is selected) by logging in to Cisco Secure ACS.
- Step 3** To modify ACS roles, refer to the Cisco Secure ACS online help (on the Cisco Secure ACS server) for information on modifying roles.



Note If you modify Service Monitor roles using Cisco Secure ACS, your changes will be propagated to all other instances of Service Monitor that are registered with the same Cisco Secure ACS server.

Using Service Monitor in ACS Mode

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



Note

The System Identity Setup user, defined when you installed Service Monitor, must be added to the Cisco Secure ACS, and this user must have Network Administrator privileges. For more information, click the CiscoWorks link in the upper-right corner of the Service Monitor home page and select **Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup**.

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

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

Help Desk	User with this role has the privileges 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: View details for Cisco 1040, setup, and default configuration. (Cannot perform modifications.)
Approver	User with this role does not have any privileges. (Service Monitor does not assign any tasks to this user role.)
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. Example: Set up Service Monitor, add, modify, delete Cisco 1040s.
Network Administrator	User with this role has the privilege to change the network. User can also perform Network Operator tasks. Example: Same as Network Operator.
System Administrator	User with this role has the privilege to perform all system administration tasks. See the Permission report. (Click the CiscoWorks link in the upper-right corner of the Service Monitor home page and select Common Services > Server > Reports > Permission Report > Generate Report .) Example: Enable and disable debugging; set logging level.

Cisco Secure ACS allows you to modify the privileges to these roles. You can also create custom roles and privileges that help you customize Service Monitor to best suit your business workflow and needs. To modify the default privileges, see Cisco Secure ACS online help. (On Cisco Secure ACS, click **Online Documentation > Shared Profile Components > Command Authorization Sets**.)

Modifying Roles and Privileges in Cisco Secure ACS

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

-
- Step 1** Select **Shared Profile Components > Cisco Unified Service Monitor** and click the Service Monitor roles that you want to modify.
- Step 2** Select or deselect any of the Service Monitor tasks that suit your business workflow and needs.
- Step 3** Click **Submit**.
-

Starting and Stopping Service Monitor Processes

To start and stop Service Monitor processes, select the CiscoWorks link from the upper-right corner of the Service Monitor home page, select **Common Services > Server > Admin > Processes**, and click **Help** for instructions. [Table 6-3](#) provides a complete list of Service Monitor-related processes.

Table 6-3 Service Monitor-Related Processes

Name	Description	Dependency
QOVR	Service Monitor server.	QOVRDbMonitor
QOVRDbMonitor	Service Monitor database monitor.	QOVRDbEngine
QOVRDbEngine	Service Monitor database.	—
QOVRMultiProcLogger	Service Monitor process logging.	—
SSHD	Service Monitor SFTP server.	—

Using SNMP to Monitor Service Monitor

Service Monitor supports the system application MIB. This support enables you to monitor Service Monitor using a third-party SNMP management tool, so that you can:

- Consistently monitor multiple platforms—One platform on which Service Monitor resides and one or more on which applications in the Cisco Unified Management Suite reside.
- Assess the application health using the system application MIB, which provides the following information:
 - Applications that Service Monitor 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 E, “Service Monitor Support for SNMP MIBs.”](#)

**Note**

You cannot uninstall the 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 6-10](#).

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 Service Monitor is installed. See [Determining the Status of Windows SNMP Service, page 6-9](#).
- Step 2** If you determined that SNMP service was not installed, install Windows SNMP Service; see [Installing and Uninstalling Windows SNMP Service, page 6-9](#).
-

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 MIB that Service Monitor 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 6-9](#).

- 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 6-10](#).

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.

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 6-9](#).

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 modify 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 modify credentials for it.

You can modify 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 Service Monitor is installed in *NMSROOT*\log.



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

Changing the Hostname on the Service Monitor Server

To change the hostname for the Service Monitor server, you must update several files, reboot the server, and regenerate the self-signed security certificate. Afterward, you must update the configuration on Service Monitor.

Changing the Hostname, Rebooting the Server, and Regenerating the Certificate


Note

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

Step 1

Change the hostname on the server as follows:

- a. Stop the 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 service from restarting after reboot. From Control Panel, or from Start, open Services and change the startup mode to Manual for the CW2000 Daemon Manager 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 Service Monitor. 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 the 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 letters.
- 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 letters in the following format:

```
OLDHOSTNAME:NEWHOSTNAME
```



Note Hostnames in this file are case-sensitive; they must be entered in uppercase letters; 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 If Service Monitor alone is installed on the server, skip to [Step 8](#). If Service Monitor is installed on the same server with Operations Manager, 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 Service Monitor.
- 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 the CW2000 Daemon Manager 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:

- a. Select **Common Services > Server > Security > Certificate Setup**.
- b. For more information, click Help.


Step 13 Reconfigure Service Monitor. See [Reconfiguring Service Monitor After a Hostname Change, page 6-13](#).

Reconfiguring Service Monitor After a Hostname Change

You must complete this procedure after you complete the procedure [Changing the Hostname, Rebooting the Server, and Regenerating the Certificate](#), page 6-11.

-
- Step 1** 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. See [Setting Up the Sensor Default Configuration](#), page 4-4.
 - If Operations Manager is installed on another server, on Operations Manager, delete the Service Monitor and add it again. For more information, see Operations Manager online help.
- Step 2** If you have Cisco 1040 sensors in your system, complete these steps:
- a. Change the IP address or hostname in each of the following configuration files:
 - The default configuration file—See [Setting Up the Sensor Default Configuration](#), page 4-4.
 - The specific configuration file for each Cisco 1040 managed by the Service Monitor—See [Editing the Configuration for a Specific Sensor](#), page 4-9.
 - b. Reset the Cisco 1040s. See [Resetting a Sensor](#), page 4-11.
- Step 3** If Service Monitor is monitoring a Cisco Unified CallManager version 5.x, update the IP address for Service Monitor configured as an Application Billing Server. For more information, see [Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server](#), page B-4.
-

Changing the IP Address on the Service Monitor Server

-
- Step 1** Stop the 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 Service Monitor 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 Service Monitor server.
- Step 4** Allow 15 minutes to elapse from the time you completed step 1, then restart the daemon manager by entering the following command:
- ```
net start crmdmgtd
```
- Step 5** Reconfigure Service Monitor. See [Reconfiguring Service Monitor After a Hostname Change](#), page 6-13.
-

# Changing the Time on the Service Monitor Server

After you change the time on the server where Service Monitor is installed, stop and start the daemon manager using this procedure.

---

**Step 1** From the command line, issue the following commands:

```
Net stop crmdmgt
Net start crmdmgt
```

---