



FAQs and Troubleshooting Guide for Cisco Performance Monitor 3.x

Last Modified: August 15, 2006

This document answers common questions about, and contains troubleshooting information for, Cisco Performance Monitor 3.x (Performance Monitor).

What do you want to troubleshoot?

- [Installation](#)
- [Importing, Validating, and Managing Devices](#)
- [Administration](#)
- [Reports](#)
- [Debugging](#)
- [General FAQs](#)



Note

The online help for Performance Monitor includes interactive troubleshooting topics. Open the online help from any Performance Monitor page, then click **Troubleshooting**.

Installation

- [What should I do if errors prevent the installation?](#)
- [What prevents Performance Monitor from loading in my browser?](#)
- [Why do I see a 500 Error when I try to run Performance Monitor?](#)
- [How do I verify that Performance Monitor is running properly?](#)
- [How do I change the status of Performance Monitor processes?](#)



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002–2006 Cisco Systems, Inc. All rights reserved.

What should I do if errors prevent the installation?

The following message might appear when you try to install Performance Monitor.

Error Message You must install CiscoWorks Common Services 3.0.3 before installing Performance Monitor 3.0.

Conditions Common Services is not detected, or the detected version is too old for Performance Monitor to use.

Workaround Install a supported version of Common Services. Check your installation documentation to see which Common Services versions are supported by the version of Performance Monitor that you use.

Calling the Technical Assistance Center (TAC)

- If you had problems installing Performance Monitor, do the following before you call TAC:
 - Make sure that your server satisfies all installation requirements (including free disk space). To review the requirements, see [Installation and Release Notes for Cisco Performance Monitor 3.0](#).
 - Make sure that the MD5 checksum of your downloaded **fcs-mcp-v3.0-w2k-k9.exe** file matches the MD5 checksum value shown on Cisco.com in the Details area of the Software Download page for fcs-mcp-v3.0-w2k-k9.exe. To obtain the URL for that page, see [Installation and Release Notes for Cisco Performance Monitor 3.0](#).
- TAC representatives might ask you to send them these files from your Performance Monitor server:
 - `NMSROOT\MDC\log\mcp.log`
 - `NMSROOT\MDC\tomcat\logs\stdout.log`

where *NMSROOT* is the full pathname of the subdirectory in which you installed Common Services.
- If you installed Performance Monitor on a server where Security Manager is installed, you can start Security Manager, then select **Tools > Security Manager Diagnostics** to capture many kinds of diagnostic information for TAC.
- Even if Security Manager is not installed, you can use the MDCSupport.exe utility to capture many kinds of diagnostic information for TAC. See your Common Services user documentation to learn more about MDCSupport.exe.
- To create a Server Info report, go to **https://server_name/cwhp/collect.do** (where *server_name* is the DNS name or IP address of your Performance Monitor server), then click **Create**. When the Collect Server Information window opens, select every check box, then click **OK**. In the Collect Server Information page, click the link for the report that you created. When the Server Info window opens, press **Ctrl-A** to Select All, then press **Ctrl-C** to Copy. Then paste the report into an email message to TAC, using the TAC email address that you find in [Installation and Release Notes for Cisco Performance Monitor 3.0](#).
- These other files might also help TAC (or you) to troubleshoot problems on your Performance Monitor server:
 - `NMSROOT\log*.*`
 - `NMSROOT\mcp\log*.*`
 - `NMSROOT\MDC\tomcat\logs*.*`

- `NMSROOT\MDC\tomcat\webapps\mcp\mcgui.log`
- `NMSROOT\setup\CSCOmcp.info`

What prevents Performance Monitor from loading in my browser?

When you start or restart your server, required processes take about 5 minutes to initialize. If you try to load the Performance Monitor GUI in your browser while those processes are initializing, you might see an error message like one of these:

- Could not connect to JRun Connector Proxy
- Internal Server Error
The server encountered an internal error or misconfiguration and was unable to complete your request.

If you see a message of this kind, we recommend that you wait a few minutes, then try again to start Performance Monitor. If you still cannot start it, contact the system administrator.

Why do I see a 500 Error when I try to run Performance Monitor?

If you see the following error message when you try to start Performance Monitor, you are probably using the Cisco Secure ACS Server (ACS) for authentication and authorization (AAA):

```
Error: 500
Location: /mcp/goHome.do
Internal Servlet Error:
java.lang.ArrayIndexOutOfBoundsException: 0 >= 0
```

If you use ACS for AAA, do the following to verify that ACS and Performance Monitor are configured correctly to work together:

-
- Step 1** Make sure that your Performance Monitor server is configured to use your ACS Server for AAA:
- a. From a browser, log in to your Performance Monitor server.
 - b. Change the URL to **`https://server_name/cwhp/loginModule.do`**, where *server_name* is the DNS name or IP address of your Performance Monitor server.
- The ACS radio button should be selected in the AAA Server Information page and the required credentials should be present.
- Step 2** Make sure that your ACS server is configured to work with Performance Monitor. A corresponding ACS username must exist for every Performance Monitor username.
- a. Verify that every ACS user who will access Performance Monitor belongs to a group that is authorized to access Performance Monitor. See the Cisco Secure ACS user guide for details.
 - b. Edit the ACS group to which the Performance Monitor users belong. Verify that the MCP check box and the Assign Performance Monitor for Any Network Device radio button are selected. See the Cisco Secure ACS user guide for details.
-

How do I verify that Performance Monitor is running properly?

Performance Monitor runs properly only when its required server processes are also running.



Note

- From a browser, only users with administrator privileges can start and stop processes.
- From the server, only users with local administrator privileges can start and stop processes.

-
- Step 1** From a browser, log in to your Performance Monitor server.
- Step 2** Select **Common Services > Server > Admin > Processes**.
- Step 3** Make sure these processes are running:
- Apache
 - Tomcat
 - MCP
 - McpDbEngine
- Step 4** If a required process is not running, you can start the process. See [How do I change the status of Performance Monitor processes?](#)
-

How do I change the status of Performance Monitor processes?

If any process is not running, you can do *one* of the following:

- [Restart processes from a browser](#)
- [Restart processes from the server](#)

Restart processes from a browser

-
- Step 1** Log in to your Performance Monitor server.
- Step 2** Do *one* of the following:
- From a browser—Select **Common Services > Server > Admin > Processes**, then select a process and click either **Start** or **Stop**.
 - From the server—From `NMSROOT\bin` in the CLI, enter `pdexec <Process Name>` at the prompt. (The process name is case-sensitive.)
- Step 3** From the Start Process page, select **System** to start all processes, or select the specific process to start.



Note

If you select specific processes, the process dependencies do not start automatically.

- Step 4** Wait 5 minutes for the processes to start.
- Step 5** If the problem persists, restart all processes from the server.

Restart processes from the server

To restart processes from the server CLI, you must stop them, then start them again. From *NMSROOT*\bin:

- To stop processes, enter **net stop crmdmgtd**.
- To start processes, enter **net start crmdmgtd**.



Note

If stopping and starting all processes does not correct the problem you are trying to solve, contact your system administrator.

How do I forward SNMP traps to a different port if port 162 is already in use?

If another application on your server uses UDP port 162 to receive SNMP traps, you must use the *modifyTrapReceiverPort.pl* script to specify a different port number in the *Fault.properties* file for Performance Monitor.



Tip

If you do not know which specific application uses UDP port 162 on your server (or even know whether any application uses that port), you can use the Windows command **netstat -o -p udp** to associate a process ID number (PID) with that port, then use the Task Manager (Ctrl-Shift-Esc) to associate the PID with a named application.

- Step 1** To stop the CiscoWorks Server daemon manager, enter this command at the Windows command line:
- ```
net stop crmdmgtd
```
- Step 2** Configure the application that forwards SNMP traps to forward them to your Performance Monitor server on a UDP port that you choose. The UDP port number must be above 1024. Remember this UDP port number.
- Step 3** Enter the following at the command line to configure Performance Monitor to receive SNMP traps on the UDP port that you chose in Step 2:
- ```
NMSROOT\mcp\bin\modifyTrapReceiverPort.pl disable port_number
```
- where *NMSROOT* is the full pathname of the subdirectory where you installed Common Services and *port_number* is the actual UDP port number on which your Performance Monitor server will receive SNMP traps.
- Step 4** Restart the CiscoWorks Server daemon manager by entering the following at the command line:
- ```
net start crmdmgtd
```

# Importing, Validating, and Managing Devices

- Why does import from DCR fail?
- Why does the import of an SSL service module from a CSV file fail?
- Why does import from a CSV file fail?
- Why is a device that I imported missing from the Device Validation Tasks page?
- Why do I see an error message when I try to import a PIX Firewall device?
- What prevents me from adding PIX Firewall devices to Performance Monitor?
- What prevents me from viewing a device under the Monitor tab?
- What does the Device Not Reachable message mean?
- What should I do if I see an SNMP Timeout error message/event?

## Why does import from DCR fail?

There are two possible explanations:

- If SSL is not enabled on the DCR server from which you failed to import device credentials, enable SSL on that DCR server, then try again to import.
- If the DCR server has an incorrect record for the SNMP configuration and login credentials that a device uses, correct that record on the DCR server, then try again to import.

## Why does the import of an SSL service module from a CSV file fail?

You cannot import an SSL service module from a CSV file, but you can add one to Performance Monitor manually.

To learn how to add an SSL service module manually, read the “Using the Importing Devices Wizard to Import or Add Devices” topic in the online help, or go to the equivalent section in the user guide: [http://www.cisco.com/en/US/products/ps6498/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html).



### Note

If the SSL service module has a DNS name, make sure a DNS server is configured on Performance Monitor. This enables Performance Monitor to convert the DNS name to an IP address.

## Why does import from a CSV file fail?

This can be because you are using an incorrect CSV file format. To see a sample CSV file that uses the supported format, go to [https://<server\\_name>/mcp/device\\_CSV\\_sample.htm](https://<server_name>/mcp/device_CSV_sample.htm), where *server\_name* is the DNS name or IP address of your Performance Monitor server:

You can generate a CSV file from the Device Credentials Repository (DCR) in Common Services or from RME. Performance Monitor supports only CSV version 3.0, not any earlier versions.

## Why is a device that I imported missing from the Device Validation Tasks page?

There are two likely explanations if no new tasks are displayed in the Device Validation Tasks page (Devices > Importing Devices) after you complete all of the required steps in the import devices wizard, or if devices that are being imported are not visible in other interface pages:

- Your Performance Monitor server is multihomed. See the entry for CSCeh54686 in the Cisco Bug Toolkit at <http://tools.cisco.com/Support/BugToolKit/>.
- The MCP process is not running. The MCP process is responsible for validating and polling devices. If this process is not running, the Device Validation Tasks page does not display the new validation tasks and the Import Devices page does not display any relevant error message.

- 
- Step 1** To determine whether the MCP process is running:
- a. Log in to your Performance Monitor server.
  - b. Do *one* of the following:
    - From a browser—Select **Common Services > Server > Admin > Processes**.
    - From the server—From *NMSROOT*\bin in the CLI, enter **pdshow MCP** at the prompt. (MCP must be capitalized.)
- Step 2** If the MCP process is not running, do *one* of the following:
- From a browser—Select **Common Services > Server > Admin > Processes** and, from the Start Process page, select the MCP process, then click **Start**.
  - From the server—From *NMSROOT*\bin in the CLI, enter **pdexec MCP** at the prompt. (MCP must be capitalized.)
- Wait 2-3 minutes for the MCP process to start.
- Step 3** From the Performance Monitor interface, select **Devices > Importing Devices**.
- Step 4** Click **Refresh**.
- 

## Why do I see an error message when I try to import a PIX Firewall device?

You see the following error message because you are using the enable password instead of the user password while importing a PIX Firewall device:

```
The Device <device name> could not be imported. Either the firewall HTTPS interface was
not enabled or the credentials are not correct. One device failed to be imported. To
monitor this device, you must import it again.
```

To resolve this problem, use the user password instead of the enable password.

## What prevents me from adding PIX Firewall devices to Performance Monitor?

If Microsoft Windows Certificate Services generated the certificates on your PIX Firewalls, any malformed URLs in the certificates—or malformed Microsoft universal naming convention (UNC) names—might cause problems in Performance Monitor.

In the following example, a UNC in the last line of text is incorrectly represented as a file:// URL. This kind of error can cause problems in Performance Monitor:

```
[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://yourtest01/CertEnroll/TestConnect.crl
URL=file://\\yourtest01\CertEnroll\TestConnect.crl
```

To work around problems of this kind, check your PIX Firewall certificates. If they contain any malformed URLs or misrepresented UNC's, generate a new certificate that contains no errors, then add the device to Performance Monitor.

## What prevents me from viewing a device under the Monitor tab?

Verify that the device is being monitored and check the Validation Task Details page for error messages.

- 
- Step 1** Select **Devices > Managing Devices**.
- Verify that the device is present in the Managing Devices page and is being monitored.
- Step 2** Select **Devices > Importing Devices**.
- Step 3** Click the radio button for the device in the Device Validation Tasks list, then click **Details**.  
The Validation Task Details window displays the historical validation results.
- Step 4** To update the Validation Task Details window, click **Refresh**.  
See “Validation Details” in the online help, or go to the equivalent section in the user guide:  
[http://www.cisco.com/en/US/products/ps6498/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html).
- 

## What does the Device Not Reachable message mean?

The poller could not retrieve all information from the device; therefore, some device data might be unavailable. This happens when:

- **IP connectivity to the device is lost.** Look for and fix network problems that might affect IP connectivity. If the device is too busy to respond to SNMP requests, see its technical documentation to learn how to analyze the problem and tune the device.
- **Community strings on the device have changed.** Correct the relevant entries in Performance Monitor, then try again to poll the device.
- **MIB variables on the device have restricted access.** Confirm whether the installed OS version supports the MIBs that Performance Monitor uses. If any newer OS versions are available for the device, consider upgrading to the latest OS version.



## What should I do if I see an SNMP Timeout error message/event?

To increase the SNMP Timeout parameters, do *one* of the following:

- Change the parameters when you import the device under **Devices > Importing Devices**. See “Using the Importing Devices Wizard to Import or Add Devices” in the online help, or go to the equivalent section in the user guide:  
[http://www.cisco.com/en/US/products/ps6498/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html)
- Edit the device under **Devices > Managing Devices**. See “Editing a Device” in the online help, or go to the equivalent section in the user guide:  
[http://www.cisco.com/en/US/products/ps6498/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html).

*SNMP Retries* refers to the maximum number of retries. A retry means that there is a failure to talk to the device SNMP agent; therefore, Performance Monitor makes the request again.

*SNMP Timeout* refers to the interval that the device waits between requests. Subsequent retry intervals are computed using the following logic: The retry policy is to double the previous timeout value. For example, if the initial timeout is 3 seconds and the retry count is 3, the timeout values between each retry are 3, 6, 12—a total of 21 seconds.

## Administration

- [What prevents me from receiving notifications?](#)
- [How do I disable notifications?](#)
- [How do I prevent polling information from filling the disk?](#)
- [What prevents SNMP Traps from generating events?](#)

## What prevents me from receiving notifications?

The notifications are probably not configured.

- 
- Step 1** Select **Admin > Notifications**.
- Step 2** From the selection tree, select **Site-to-Site VPN**.
- Step 3** Verify that the Email Recipients, Trap Recipients, and Syslog Recipients notifications are configured. If they are not configured, configure them. See “Configuring Notification Settings for a Service” in the online help, or go to the equivalent section in the user guide:  
[http://www.cisco.com/en/US/products/ps6498/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html).
- 

## How do I disable notifications?

- 
- Step 1** Select **Admin > Notifications**.
- Step 2** Click the relevant service folder in the selection tree.
- The Service Notifications page displays Email Recipients, Trap Recipients, and Syslog Recipients notifications.

**Caution**

Notifications are disabled immediately. There is no undo function.

**Step 3**

Select the notification to disable, then do *one* of the following:

- If your selection is an email recipient, click **Delete** in the Email Recipients area.
- If your selection is a SNMP trap recipient, click **Delete** in the Trap Recipients area.
- If your selection is a syslog recipient, click **Delete** in the Syslog Recipients area.

## How do I prevent polling information from filling the disk?

To prevent information from gathering at a high polling rate and filling the disk, configure the number of days that polled data is stored.

**Step 1**

Select **Admin > System Parameters**.

**Step 2**

Reduce the values, then click **Apply**. See “Working with System Parameters” in the online help, or go to the equivalent section in the user guide:

[http://www.cisco.com/en/US/products/ps6498/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html)

## What prevents SNMP Traps from generating events?

When SNMP traps do not generate events, the cause can be one or both of the following:

- Another application in addition to Performance Monitor uses UDP port 162 on your server.
- The device might not be configured to send SNMP traps.

**Step 1**

If another application on your server uses UDP port 162 to receive SNMP traps, you must reconfigure Performance Monitor to receive traps on a different port. From the Windows command line, enter:

```
NMSROOT\bin\perl.exe NMSROOT\mcp\bin\modifyTrapReceiverPort.pl port
```

where *NMSROOT* is the full pathname of the subdirectory in which you installed Common Services and *port* is the numeric value of the port that you will use. (This command edits the Fault.properties file for Performance Monitor.)

**Step 2**

Restart Performance Monitor.

After you restart it, Performance Monitor listens for traps on the new port number.

**Step 3**

Make sure that the device is configured to send SNMP traps. To learn what steps are required, see “Bootstrapping Devices” in the online help, or go to the equivalent section in the user guide:

[http://www.cisco.com/en/US/products/ps6498/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html). You can:

- Set up SNMP traps to generate the Real Server Status load balancing event.
- Set up SNMP traps to generate the following site-to-site VPN events:
  - Crypto Map Binding
  - Crypto Map Change

- ISAKMP Policy Change
  - Tunnel Status
  - Interface Status
- 

## Reports

- [I deleted a device, then added it back. Then I ran a report and noticed that it displayed data earlier than the time I added the device. Why?](#)
- [Why would the User Session Report for a VPN 3000 concentrator omit SSL VPN \(WEBVPN\) user login details?](#)
- [Why is the User Session Report empty for a VPN 3000 concentrator?](#)

### I deleted a device, then added it back. Then I ran a report and noticed that it displayed data earlier than the time I added the device. Why?

When you delete a device, it is marked as Deleted in the database, but the data related to that device is removed only after 2 hours. Every 2 hours, a background process updates the database and removes data for deleted devices. If you add the device back sooner than 2 hours (before the database removes the related data) and run a report the next day, you have information for that day as well as for the previous days of the week (except for the less-than-2-hour span when the device was deleted).

### Why would the User Session Report for a VPN 3000 concentrator omit SSL VPN (WEBVPN) user login details?

You must enable the WEBVPN syslog classname on the concentrator:

- 
- Step 1** Log in to the VPN 3000 Concentrator Series Manager.
  - Step 2** Select **Configuration > System > Events > Classes**.
  - Step 3** Click **Add**.
  - Step 4** From the Class Name list, select **WEBVPN**, then select the **Enable** check box.
  - Step 5** From the Events to Syslog list, select **1-5**, then click **Add**.
  - Step 6** Click **Save Needed**—located in the upper right corner.
  - Step 7** Click **OK**.
  - Step 8** Enable syslog. See [Why is the User Session Report empty for a VPN 3000 concentrator?](#) for instructions.
-

## Why is the User Session Report empty for a VPN 3000 concentrator?

This could be because syslog is not enabled on the VPN 3000 concentrator. To enable syslog:

- 
- Step 1** Log in to the VPN 3000 Concentrator Series Manager.
  - Step 2** Select **Configuration > System > Events > Classes**, then click **Add**.
  - Step 3** From the Class Name list, select **AUTH**, then select the **Enable** check box.
  - Step 4** From the Severity to Syslog list, select **1-5**, then click **Add** twice.
  - Step 5** From the Class Name list, select **IKE**, then select the Enable check box.
  - Step 6** From the Severity to Syslog list, select **1-5**, then click **Add**.
  - Step 7** Click **Save Needed**, in the upper right corner, then click **OK**.
  - Step 8** Select **Configuration > System > Events > Syslog Servers.**, then click **Add**.
  - Step 9** In the Syslog Server field, enter the IP address of your Performance Monitor server, then click **Add**.
  - Step 10** **(Optional)** To improve performance in the Performance Monitor application itself if it is the only application to which the concentrator will send syslog messages:
    - a. Select **Configuration > System > Events > General**.
    - b. Select **None** from the Severity to Syslog list.
    - c. Click **Apply**.
- 

## Debugging

- [How do I turn on debugging?](#)
- [How do I debug a problem related to importing a device?](#)

## How do I turn on debugging?

- 
- Step 1** Start Performance Monitor.
  - Step 2** Change the URL to **https://server\_name/mcp/debuglog.do**, where *server\_name* is the DNS name or IP address of your Performance Monitor server.  
The Enable Debug Log window opens.
  - Step 3** For each log file that matters to you, select **on** from the list in the debug column.
  - Step 4** Click **Submit**, then close the window.
  - Step 5** To turn debugging off when you are done.
    - a. Return to **https://server\_name/mcp/debuglog.do**.
    - b. Select **off** from the list in the debug column.
    - c. Click **Submit**, then close the window.
-

## How do I debug a problem related to importing a device?

- 
- Step 1** Turn debugging on for the following log files:
- validation.log
  - mcpui.log
- See [How do I turn on debugging?](#) for instructions.
- Step 2** Restart Performance Monitor, then try again to import the device.
- Step 3** Select **Admin > Logs > Debugging Log Files**.
- Step 4** Select the validation.log and mcpui.log files, then click **Download**.
- Step 5** Send the downloaded files to the TAC support engineer who is handling your case.
- Step 6** Turn debugging off after you are done.
- Go to **[https://server\\_name/mcp/debuglog.do](https://server_name/mcp/debuglog.do)**, where *server\_name* is the DNS name or IP address of your Performance Monitor server.
  - Select **off** from the list in the debug column.
- 

## General FAQs

- [What platform does Performance Monitor 3.x support?](#)
- [Where can I see the version number for my copy of Performance Monitor?](#)
- [Where can I see the build date for my copy of Performance Monitor?](#)
- [Why are the CPU Usage% and Memory Usage% columns blank for the Cisco 800 series router?](#)
- [How do I back up and restore the Performance Monitor database?](#)

## What platform does Performance Monitor 3.x support?

Performance Monitor 3.x supports the Windows platform. For system requirements and installation instructions, see [Installation and Release Notes for Cisco Performance Monitor 3.0](#).

## Where can I see the version number for my copy of Performance Monitor?

- 
- Step 1** Start Performance Monitor.
- Step 2** Change the URL to **[https://server\\_name/cwhp/psu.swUpdate.do?showDetailsOf=Performance%20Monitor](https://server_name/cwhp/psu.swUpdate.do?showDetailsOf=Performance%20Monitor)**, where *server\_name* is the DNS name or IP address of your server.
- The Details of the Applications, Packages Installed window opens.

The “Applications and Packages installed with Performance Monitor” area identifies the Performance Monitor software version that you installed and identifies any patches that you have applied to Performance Monitor.

---

## Where can I see the build date for my copy of Performance Monitor?

**Step 1** Start Performance Monitor.

**Step 2** Change the URL to **`https://server_name/cwhp/psu.swUpdate.do?showDetailsOf=Performance%20Monitor`**, where *server\_name* is the DNS name or IP address of your server.

The Details of the Applications, Packages Installed window opens.

The “Build Id” text near the top of the window includes the build date (YYYYMMDD) for your installed Performance Monitor software. The build date is in the middle, and is bold in this example: *NT\_MCP3\_0\_20060728\_0234*.

---

## Why are the CPU Usage% and Memory Usage% columns blank for the Cisco 800 series router?

This is a known problem. The management information base (MIB) for Cisco 800 Series routers does not provide CPU usage information and, in some cases (when certain IOS images are installed), does not provide Memory usage information.

## How do I back up and restore the Performance Monitor database?

To back up the database, do one of the following:

- **Security Manager**—If Security Manager is installed on the same server with Performance Monitor, see the Backup and Restore topic in the “Using Tools” chapter from [User Guide for Cisco Security Manager 3.0.1](#).
- **Common Services**—If Security Manager is *not* installed on the same server with Performance Monitor, see the Backing Up Data topic in the “Configuring the Server” chapter from [User Guide for CiscoWorks Common Services 3.0.3](#).

To restore the database, do one of the following:

- **Security Manager**—If Security Manager is installed on the same server with Performance Monitor, see the Backup and Restore topic in the “Using Tools” chapter from [User Guide for Cisco Security Manager 3.0.1](#).
- **Common Services**—If Security Manager is *not* installed on the same server with Performance Monitor, see the Restoring Data topic in the “Configuring the Server” chapter from [User Guide for CiscoWorks Common Services 3.0.3](#).