



Installation and Release Notes for Cisco Performance Monitor 3.2.2

Revised: August 4, 2009
Text Part Number: OL-18076-02



Note

This document has been updated to include information for Cisco Performance Monitor 3.2.2 Service Pack 3 which provides fixes for various problems. For more information about the fixes included in Service Pack 3, see [Table 3 Resolved Problems in Performance Monitor 3.2.2 Service Pack 3, page 11](#). For instructions on installing Service Pack 3, see [Downloading and Installing Service Pack 3, page 4](#).

A service pack is also available for Cisco Security Manager 3.2.2. For more information, see http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2.2/release/notes/csmrn322.html.

When you purchase Cisco Security Manager 3.2.2 (Security Manager), your license grants you the right to download, install, and use Cisco Performance Monitor 3.2.2 (Performance Monitor).

Performance Monitor is a browser-based tool that monitors and troubleshoots the health and performance of services that contribute to network security. It helps you to isolate, analyze, and troubleshoot events in your network as they occur, so that you can increase service availability. Supported service types are remote-access VPN, site-to-site VPN, firewall, web server load-balancing, and proxied SSL.

This guide supplements the [Installation Guide for Cisco Security Manager 3.2.2](#) that you received with your copy of Security Manager. Although that guide does not describe any installation procedure for Performance Monitor specifically, it does describe a broad framework of prerequisites, best practices, checklists, troubleshooting tips, and other material to ensure that all of your Security Manager software—including Performance Monitor—can be installed successfully.

This guide contains:

- High-level descriptions of the hardware and software requirements for installation.
- High-level instructions for installing, upgrading to, and uninstalling Performance Monitor.
- Bug ID numbers and headlines for problems that were fixed for this release of Performance Monitor.



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

- Bug ID numbers, headlines, and descriptions for known problems that might affect you as a Performance Monitor user. If you access this document in HTML or PDF form, you can click any ID number to see the release note enclosure in the Bug Toolkit on Cisco.com. A release note enclosure contains symptoms, conditions, and workaround information.

**Note**

Before you install Performance Monitor, we recommend that you read and follow all of the relevant guidance in the Security Manager installation guide.

New and Changed Features in this Release

**Note**

A service pack for Performance Monitor 3.2.2 is available that provides fixes for various problems. For more information about the fixes included in this service pack, see [Table 3 Resolved Problems in Performance Monitor 3.2.2 Service Pack 3, page 11](#). For instructions on installing the service pack, see [Downloading and Installing Service Pack 3, page 4](#).

This section describes new and changed features in the Performance Monitor 3.2.2 release.

- Performance Monitor 3.2.2 supports FWSM software release 4.0 in backward compatibility mode.
- Performance Monitor 3.2.2 requires Common Services 3.2.

Installation Requirements

You can use Performance Monitor as a standalone product or install it on the same server with Security Manager, Cisco Auto Update Server (AUS), RME, or all three. In any of these installations, you must also install Common Services 3.2, or Performance Monitor cannot work.

Performance Monitor by default uses SNMP trap port 162.

**Note**

CiscoWorks Common Services 3.2 is required for Performance Monitor to work. You can install Performance Monitor only after you install Common Services from the Security Manager 3.2.2 installation DVD. Performance Monitor cannot coexist on a server with any patched or unpatched Common Services version earlier than 3.2. If you are upgrading to Performance Monitor 3.2.2 from an earlier version, you must upgrade Common Services to 3.2 before you upgrade Performance Monitor.

Requirements for installation and operation vary in relation to the presence of other software on your server and according to the way you use Performance Monitor.

You can install Performance Monitor on a Windows-based server that uses one CPU or multiple CPUs.

Table 1 describes server requirements and restrictions.

Table 1 *Installation Requirements and Restrictions*

Component	Requirement
System hardware	<ul style="list-style-type: none"> • IBM PC-compatible with a 2 GHz or faster processor. • Color monitor with at least 1024 x 768 resolution and a video card capable of 16-bit colors. • DVD-ROM drive. • 100BaseT (100 Mbps) or faster network connection; single interface only. • Keyboard. • Mouse.
System software	<p>Microsoft Windows 2003:^{1, 2}</p> <ul style="list-style-type: none"> • Enterprise Edition with SP1 and SP2. • Standard Edition with SP1 and SP2. • R2 Enterprise Edition with SP1 and SP2. • R2 Standard Edition with SP1 and SP2. <p>Security Manager supports only the US-English and Japanese versions of Windows. From the Start Menu, open the Control Panel for Windows³, open the panel where you configure region and language settings⁴, then set the default locale. (We do not support English as the language in any Japanese version of Windows.)</p> <p>Microsoft ODBC Driver Manager 3.510 or later is also required, so your server can work with Sybase database files. To confirm the installed ODBC version, find and right-click ODBC32.DLL, then select Properties from the shortcut menu. The file version is listed under the Version tab.⁵</p>
Memory (RAM)	2 GB.
File system	NTFS.
Browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 6.0 Service Pack 2. • Internet Explorer 7.0 • Firefox 2.0.
Compression software	WinZip 9.0 or compatible.
Hard Drive Space	20 GB.
IP Address	<p>One static IP address.</p> <p>The Performance Monitor installer displays a warning if it detects any dynamic IP addresses on the target server. Dynamic addresses are not supported. If the server has more than one IP address, you do not need to disable any of the multiple network interface cards before installation.</p>

1. To confirm the installed Windows version from the Start menu, select **Run**, then enter either **ver** or **winver**.
2. Security Manager and its included applications is not supported on 64-bit Windows operating systems or on virtual machines such as VMware.
3. To open the Control Panel for Windows from the Start Menu, you follow a path that varies according to your Windows version and configuration.
4. The panel where you specify region and language settings for Windows has a name that varies according to your Windows version and configuration.
5. Alternatively after you install Security Manager, select **Server > Admin** from the Common Services desktop, click **Selftest**, then click **Create**. When the table is refreshed, click the newest entry in the *SelfTest Server Information* column. When the “Server Info” window opens, scroll to the *odbc.pl* section to see the installed ODBC version.

**Caution**

Do not install this product on a primary or backup domain controller. We do not support any use of Common Services 3.2 on a Windows domain controller.

Do not install this product in an encrypted directory. Common Services 3.2 does not support directory encryption.

Do not install this product if Terminal Services is enabled in Application mode. In such a case, you must disable Terminal Services, then restart the server before you install. Common Services 3.2 supports only the Remote Administration mode for Terminal Services.

Scalability

The following table describes Performance Monitor scalability.

Table 2 Cisco Performance Monitor Scalability

Number of devices	Supports up to 500 devices, including security contexts.
Number of users	Supports up to 5 simultaneous users.
VPN restrictions	<ul style="list-style-type: none"> We recommend that you monitor only the hubs, not the spokes, in any hub-and-spoke VPNs that you monitor. We recommend that you monitor no more than 5,000 tunnels.

Downloading and Installing Service Pack 3

Cisco Performance Monitor 3.2.2 Service Pack 3 provides fixes for various problems. For more information about the fixes included in this service pack, see [Table 3 Resolved Problems in Performance Monitor 3.2.2 Service Pack 3, page 11](#).

**Note**

A service pack is also available for Cisco Security Manager 3.2.2. For more information, see http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2.2/release/notes/csmrn322.html.

**Note**

This service pack cannot be uninstalled.

- Step 1** To download the service pack, log in to Cisco.com.
- Step 2** Go to <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=280033778>.
- Step 3** Go to "Latest Releases" and click on 3.2.2sp3. The Performance Monitor image is seen on the right-hand side.
- Step 4** Download the file fcs-mcp-322-sp3-win-k9.exe.
- Step 5** Close all open applications before you begin installation.

Step 6 If Cisco Security Agent is installed on your server, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 7 Install the Performance Monitor 3.2.2 FCS build on your server if you have not already done so.

Step 8 Stop the Daemon Manager by executing the following command at command prompt:

```
net stop crmdmgtd
```

Step 9 Run the fcs-mcp-322-sp3-win-k9.exe file that you previously downloaded.



Note This service pack cannot be uninstalled.

Step 10 After the updated files have been installed, click **Close** to complete the installation.

Step 11 Start the Daemon Manager by executing the following command at command prompt:

```
net start crmdmgtd
```

Installing Performance Monitor



Note

United States law requires Cisco Systems to limit access to any software that uses advanced encryption technologies. Therefore, you must have and use a Cisco.com user account to download the Performance Monitor installation utility.

You can install Performance Monitor on:

- A standalone server, after you install a supported version of Common Services.
- The same server on which you installed Security Manager, AUS, RME, or all three.

For related information, see [Installation Requirements, page 2](#).

The Performance Monitor installation utility does not include Common Services, which you must install before you install Performance Monitor. You must use the Security Manager installer included in your Security Manager 3.2.2 installation DVD to install Common Services. The Security Manager installer supports the installation of only Common Services if you do not want to run any other application on the server besides Performance Monitor, such as Security Manager or Auto Update Server. If you are installing Performance Monitor 3.2.2 on a server that has a version of Common Services other than 3.2 installed, you must upgrade Common Services to 3.2 before you install Performance Monitor.

The Performance Monitor license is a separate file from the Security Manager license file and includes the license for RME 4.2 too. The Security Manager media kit contains the Software License Claim Certificate for the Performance Monitor and RME. You can install the license either before or after you install Performance Monitor. For instructions on how to obtain and install the license file, see the *User Guide for CiscoWorks Common Services 3.2* at the following URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html.

You can install Performance Monitor from either the Security Manager DVD or Cisco.com. The following sections describe how to install and enter license details for Performance Monitor:

- [Installing from the DVD, page 6](#)
- [Installing from Cisco.com, page 6](#)
- [Updating License from the Common Services GUI, page 6](#)

Installing from the DVD

This procedure describes how to install Performance Monitor from the Security Manager installation DVD.

Procedure

- Step 1** Insert the DVD into the DVD-ROM drive.
 - Step 2** From the mcp3_2_2 folder, double-click **Setup.exe** to start the installation utility.
 - Step 3** Click **Yes** to confirm that you are installing Performance Monitor.
 - Step 4** Follow the prompts in the installation wizard.
 - Step 5** When you are prompted to select the licensing information, select one of the following:
 - **License File Location**—Enter the full pathname of the license file or click **Browse** to find it. You can specify the permanent license file if you have previously staged it on the server.
 - **Evaluation Only**—Enables the free 90-day evaluation period.
-

Installing from Cisco.com

This procedure describes how to install Performance Monitor from Cisco.com

Procedure

- Step 1** Log in to your Cisco.com account at <http://www.cisco.com/cgi-bin/login>.
 - Step 2** Go to <http://www.cisco.com/go/csmanager>, then click **Download Software**.
 - Step 3** Download the installation utility for Performance Monitor, **fcs-mcp-322-win-k9.exe**.
 - Step 4** To start the installation, double-click your downloaded copy of the utility, then follow the prompts.
 - Step 5** When you are prompted to select the licensing information, select one of the following:
 - **License File Location**—Enter the full pathname of the license file or click **Browse** to find it. You can specify the permanent license file if you have previously staged it on the server.
 - **Evaluation Only**—Enables the free 90-day evaluation period.
-

Updating License from the Common Services GUI

After you complete the installation, you can also use the License Information page of the Common Services GUI to enter the Performance Monitor license details. You can view details of your current software license, or update to a new license from the License page.

This procedure describes how to update to a new Performance Monitor license from the Licensing page.

Before You Begin

You should place your license file on the target server prior to installation. You will be prompted to select this file during installation.

Procedure

-
- Step 1** Log in to the Cisco Security Management Server desktop.
- Step 2** Click the Server Administration panel. The CiscoWorks home page is displayed.
- Step 3** From the CiscoWorks UI, select **Common Services > Server > Admin > Licensing**.
The License Information page displays the license name, license version, status of the license, and the expiration date of the license.
- Step 4** Click **Update**.
Enter the path to the new license file in the License field, or click **Browse** to locate the new file.
- Step 5** Click **OK**.
The system verifies whether the license file is valid, and updates the license. The updated licensing information appears in the License Information page. Otherwise, an error message is displayed.
-

Uninstalling and Reinstalling Performance Monitor

**Note**

To learn which data files are essential to Common Services operation and understand how to archive that data, see the Common Services online help or read the documentation on Cisco.com. We recommend that you back up copies of all essential data files from your server before you uninstall or reinstall Performance Monitor.

To uninstall or reinstall applications on your server, see:

- [Uninstalling Performance Monitor, page 7](#)
- [Reinstalling Performance Monitor, page 8](#)

Uninstalling Performance Monitor

**Caution**

A server that is infected with a virus might be unstable after you uninstall software from it and reboot. If your server is not stable after an uninstallation and reboot, we recommend that you scan it for viruses and other kinds of malware.

Before You Begin

If any version of Windows Defender (which was known in its public beta test versions as both Microsoft AntiSpyware and Giant AntiSpyware) is installed, disable it before you uninstall Performance Monitor. Otherwise, the uninstallation application cannot run.

- Step 1** Select **Start > Programs > Cisco Security Manager > Uninstall Cisco Security Manager** or **Start > Programs > Performance Monitor > Uninstall Performance Monitor** (if installed individually).
- Step 2** From the list of applications, select **Cisco Performance Monitor**.
- Step 3** (Optional) Select any other components to uninstall.
- Step 4** Click **Next** twice.

The uninstaller removes Performance Monitor and every other component that you selected.



Note If a Windows command line prompt window is open in `\CSCOp\bin` when you uninstall Performance Monitor, the uninstaller cannot delete `\CSCOp\bin`. In this case, you can choose whether and how to delete the directory.

- Step 5** *Only after you uninstall* Performance Monitor, Common Services, and *all* related applications, assuming that you uninstall all server applications:
- If a folder exists at `C:\Program Files\CSCOp`, delete, move, or rename the folder.
 - If the `C:\CMFLOCK.TXT` file exists, delete it.
 - Use a Registry editor to delete these Registry entries before you reinstall Performance Monitor or any related applications:
 - `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager`
 - `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\MDC`



Tip Although no reboot is required, we recommend that you reboot the server after an uninstallation so that Registry entries and running processes on the server are in a suitable state for a future reinstallation.



Note If the uninstallation causes an error, see the “Troubleshooting and FAQs” chapter in *Installing and Getting Started With CiscoWorks LAN Management Solution 3.0*:
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html.

- Step 6** If you disabled Windows Defender before uninstalling Performance Monitor, reenable it now.

Reinstalling Performance Monitor



Caution

Although the Security Manager installation utility performs a full, mandatory backup automatically if you use it to reinstall Security Manager, AUS, or Common Services, *no* such backup occurs when you use the Performance Monitor installation utility to reinstall Performance Monitor. We recommend that you follow the backup instructions in the Common Services online help before you reinstall Performance Monitor.

**Note**

- If you install Common Services and Performance Monitor on a server, then reinstall Common Services later, you must also reinstall Performance Monitor.
- During reinstallation, you might see a warning message that says:

The application that you are installing requires new tasks to be registered with ACS. If you have already registered this application with ACS from another server, you do not need to register it again. However if you re-register the application, you will lose any custom roles that you had created earlier for this application in ACS.

In this case, log in to your Cisco.com account and see “Impact of Installing CiscoWorks Applications in ACS Mode” in *Installing and Getting Started With CiscoWorks LAN Management Solution 3.0*, at

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html.

To reinstall Performance Monitor or related applications, see [Installing Performance Monitor, page 5](#).

Upgrading Performance Monitor

You can upgrade to Performance Monitor 3.2.2 from any of the following previous versions: 3.1, 3.2, or 3.2.1. Performance Monitor supports two types of upgrades, namely, inline and backing up and restoring of data. Inline upgrade refers to running the installation for the version to which you want to upgrade without uninstalling the previous version of Performance Monitor from a server. Upgrade using backup and restore refers to backing up the database from the server running a previous version of Performance Monitor and restoring the backed up data on the server you want to upgrade after installing the later version of Performance Monitor. If you are performing an upgrade using the backup and restore method on the same server, you must uninstall the previous version after backing up the data and then perform restoration of the database after installing the new version.

When you upgrade from an earlier version of Performance Monitor to 3.2.2, both the evaluation and permanent licenses are preserved and hold good. If you want to update your existing license file, you must use the License Information page of the Common Services GUI. See [Updating License from the Common Services GUI, page 6](#) for more information.

**Note**

Performance Monitor 3.2.2 requires that you use Common Services 3.2. Therefore, if you upgrade from an earlier Performance Monitor version, the installed Common Services version must be upgraded to 3.2 before you upgrade Performance Monitor. You can use the Security Manager installer included in your Security Manager 3.2.2 installation DVD to upgrade Common Services.

The following sections describe the procedure to upgrade to Performance Monitor 3.2.2 using inline and backup and restore methods:

- [Upgrading to Performance Monitor 3.2.2 Using Inline Method, page 10](#)
- [Upgrading to Performance Monitor 3.2.2 by Backing Up and Restoring the Database, page 10](#)

Upgrading to Performance Monitor 3.2.2 Using Inline Method

To use the inline method to upgrade to Performance Monitor 3.2.2 on a server where Performance Monitor 3.1, 3.2, or 3.2.1 is installed, first upgrade Common Services to 3.2 and then simply run the installer for Performance Manager 3.2.2. For step-by-step instructions, see [Installing Performance Monitor, page 5](#). You can use the Security Manager installer included in your Security Manager 3.2.2 installation DVD to upgrade Common Services.

Upgrading to Performance Monitor 3.2.2 by Backing Up and Restoring the Database

The following procedure describes how to back up the database on a server where Performance Monitor 3.1, 3.2, or 3.2.1 is installed and restore it after installing Performance Monitor 3.2.2 on the server.

-
- Step 1** Create a backup of the database for Performance Monitor 3.1, 3.2, or 3.2.1 by selecting **Tools > Backup**.



Note You cannot perform a backup of the database on Performance Monitor servers placed across sites or locations by using a mapped network drive.

- Step 2** Uninstall Performance Monitor 3.1, 3.2, or 3.2.1. See [Uninstalling Performance Monitor, page 7](#).
- Step 3** Upgrade Common Services to 3.2. You can use the Security Manager installer included in your Security Manager 3.2.2 installation DVD to upgrade Common Services.
- Step 4** Install Performance Monitor 3.2.2. See [Installing Performance Monitor, page 5](#).
- If you want to restore the backed up database on a different server than the one running Performance Monitor 3.1, 3.2, or 3.2.1, skip [Step 4](#) and proceed to [Step 5](#).
- Step 5** Restore the database from the backup corresponding to the version to which you want to upgrade. See [Restoring the Performance Monitor Database, page 10](#).
-

Restoring the Performance Monitor Database

You can restore your database by running a script from the command line. You have to shut down and restart CiscoWorks while restoring data. This procedure describes how you can restore the backed up Performance Monitor database on your server. A single backup and restore facility exists to back up and restore all applications installed on a CiscoWorks server.; you cannot back up or restore individual applications on a CiscoWorks server. Make sure you have the correct permissions, and do the following.



Note When you back up the Performance Monitor 3.2.2 database (with a permanent license) from one server to restore to a different server that has been inline-upgraded from Performance Monitor 3.1 to 3.2.2 with an evaluation license, the license that existed before the restore operation is retained. For more information (CSCso92580), log in to the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

Step 1 Stop all processes by entering the following at the command line:

```
net stop crmdmgt
```

Step 2 Restore the database by entering:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl [-t temporary_directory] [-gen generationNumber] [-d backup_directory] [-h]
```

where:

- *NMSROOT*—(Required) Environment variable containing full pathname of the Common Services installation directory (by default, C:\Program Files\CSCOpX, where C: is the System Drive).
- *[-gen generationNumber]*—Optional. By default, it is the latest generation. If generations 1 through 5 exist, then 5 will be the latest.
- *-t temporary_directory*—(Optional) This is the directory or folder used by the restore program to store its temporary files. By default this directory is *NMSROOT/tempBackupData*. You can customize this by specifying your own temporary directory to avoid overloading *NMSROOT*.
- *-d backup_directory*—(Required) The backup directory to use.
- *-h*—(Optional) Provides help. When used with *-d BackupDirectory*, show s correct syntax along with available suites and generations.

To restore the most recent version, enter the following command:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup_directory
```

For example, *-d drive:\var\backup*

Step 3 Examine the log file in the following location to verify that the database was restored by entering:

```
NMSROOT\log\restorebackup.log
```

Step 4 Restart the system by entering:

```
net start crmdmgt
```

Resolved Problems in Performance Monitor 3.2.2 Service Pack 3

Table 3 identifies the problems resolved by Security Manager 3.2.2 (Service Pack 3).



Note

A service pack is also available for Cisco Security Manager 3.2.2. For more information, see http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2.2/release/notes/csmrn322.html.

Table 3 Resolved Problems in Performance Monitor 3.2.2 Service Pack 3

CSCsy71557—Performance monitor may not discover FWSM running 4.0.3.

CSCsz14304—MCP 3.2.2: SSL handshake failure with IOS 12.4(22)T and above.

CSCsz20953—MCP: Device Credential deleted if re-validation fails.

CSCsz77063—Sybase DB outer joins should be enabled for MCP.

CSCta33058—SNMP thread deadlock detected.

Known Problems

This section describes problems known to exist in this release of Performance Monitor.



Note

- The problems and other issues in the following tables are known to affect Performance Monitor 3.2.2. However, some of the problems were found in releases of Monitoring Center for Performance 2.x, so their descriptions or headlines might contain obsolete terms and references. Any such terms and references apply to Performance Monitor as well.
- To obtain more information about known problems, click the ID number or use the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

Table 4 Performance Monitor 3.2.2 Known Problems

CSCeb57907—Cannot import an SSL service module from a CSV file

Description: If you try to import a CSV file that contains the IP address of an SSL service module, the SSL service module is not validated.

CSCec17725—SNMP version 2 traps are required for interface-down events

Description: If you use SNMP version 1 traps for linkUp and linkDown, Performance Monitor cannot generate events in response to changes to the state of an interface.

CSCec28656—32 KB-rows in a User Session report take 5 minutes or more to load

Description: If the search result is more than 10,000 entries, the User Session report takes 5 minutes or more to load.

CSCec28918—User logged in once but two sessions are displayed in the report

Description: The User Session report displays two sessions for the same user even though the user logged in only once within the time selected for the report.

CSCec49471—User session state marked Active instead of Completed

Description: If a completed user session remains in an active state, the User Session report shows two or more sessions with the same username, IP address, and VPN device name.

CSCed36700—STS: no CPU/mem usage for 831/803 with 12.3(2)T and 12.3(5b)f

Description: CPU usage values are not available for a Cisco 800 Series router. A known problem in Cisco IOS prevents Performance Monitor from displaying these statistics.

CSCed57697—Page Not Found error appears when you start Performance Monitor

Description: You see a Page Not Found error when you try to start Performance Monitor from a supported browser.

CSCed68244—Performance Monitor cannot clear Interface State event in PIX failover

Description: If a PIX device is configured as part of a failover pair, Performance Monitor misinterprets some of the syslog information it receives.

CSCee59388—Cannot see load-balancing Interface Down event

Description: The load-balancing Interface Down event is not displayed in the event browser.

CSCeh54686—A multi-homed Performance Monitor server cannot monitor imported devices

Description: If your Performance Monitor server has more than one NIC, you cannot monitor devices that you import.

CSCsa48691—Import operation does not seem to finish

Description: After you import a device, the GUI describes the status as Running and the import does not seem to finish.

Table 4 Performance Monitor 3.2.2 Known Problems (continued)

CSCsc43213—Performance Monitor doesn't discover all security contexts

Description: Some security contexts (virtual firewalls) do not appear if you select **Monitor > Firewall**.

CSCsc95585—Different CPU usage shown for PIX in STS and Firewall monitoring pages

Description: The reported CPU usage levels for a PIX appliance show different values under **Monitor > Site-to-Site** and **Monitor > Firewall** because we use two polling methods instead of one.

CSCsd28035—Tunnel table is empty for Easy VPN server

Description: If you select **Monitor > Site-to-Site VPN**, then click **Tunnels** in the TOC, the displayed information does not include Easy VPN tunnels that are configured on IOS routers.

CSCse11165—No memory usage data available for VPN 3000 concentrators

Description: VPN 3000 Series concentrators do not provide any way to poll memory usage statistics. Therefore, if you select **Monitor > Site-to-Site VPN**, the displayed *Memory Usage %* value for these concentrators is always zero.

CSCse17747—SNMP access outage on VPN SPA doesn't generate event

Description: Performance Monitor does not display any Critical Problems or events to show that it has stopped polling a VPN Shared Port Adapter (VPN SPA) on which SNMP community string values have changed.

CSCsc95489—Unable to monitor Easy VPN tunnels on PIX 6.3

Description: If you select **Monitor > Remote Access VPN**, the displayed information does not include Easy VPN tunnels that are configured on PIX 6.3 devices.

CSCsh71213—Software Updates page shows incorrect version number of Perf. Monitor

Description: After you install Performance Monitor 3.2 on a server that runs Security Manager 3.2, the version of Performance Monitor is incorrectly displayed as 3.0 in the Products Installed dialog box on the Software Updates page of the Common Services GUI.

CSCso92580—License not updated after restoring Perf. Monitor 3.2 on inline upgrade

Description: When you back up the Performance Monitor 3.2 database (with a permanent license) from one server to restore to a different server that has been inline-upgraded from Performance Monitor 3.1 to 3.2 with an evaluation license, the license that existed before the restore operation is retained.

Related Documentation

Table 5 describes product documentation that is available for Cisco Security Manager and related applications. For information on ordering printed documents, see [Obtaining Documentation and Submitting a Service Request](#), page 15.

Table 5 *Product Documentation*

Document Title	Available Formats
Cisco Security Manager 3.2.2; Cisco Auto Update Server 3.2.2	
<i>Installation Guide for Cisco Security Manager 3.2.2</i>	<ul style="list-style-type: none"> PDF on the product DVD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html
<i>User Guide for Cisco Security Manager 3.2.2</i>	<ul style="list-style-type: none"> PDF on the product DVD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
<i>Supported Devices and Software Versions for Cisco Security Manager 3.2.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html
<i>FAQ and Troubleshooting Guide for Cisco Security Manager 3.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/prod_troubleshooting_guides_list.html
<i>User Guide for Auto Update Server 3.2.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
<i>Supported Devices and Software Versions for Auto Update Server 3.2.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html
Context-sensitive online help	Click the Help button in a window or dialog box.
Cisco Performance Monitor 3.2.2	
<i>Installation and Release Notes for Cisco Performance Monitor 3.2.2</i> (this document)	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html
<i>User Guide for Cisco Performance Monitor 3.2.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
<i>Supported Devices and Software Versions for Cisco Performance Monitor 3.2.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html
Context-sensitive online help	Click the Help button in a window or dialog box.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with other documentation for Cisco Performance Monitor 3.2.2 listed in [Related Documentation, page 14](#). See <http://www.cisco.com/go/csmanager>.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002-2008 Cisco Systems, Inc. All rights reserved.

