



# Installation and Release Notes for *Cisco Performance Monitor 3.0*

---

**Revised: June 13, 2007,**  
**Text Part Number: OL-10799-02**

When you purchase Cisco Security Manager 3.0 or 3.0.1 (Security Manager), your license grants you the right to download, install, and use Cisco Performance Monitor 3.0 (Performance Monitor), which was previously called CiscoWorks Monitoring Center for Performance 2.0.x.



**Note**

---

Windows and Solaris versions of Monitoring Center for Performance are still available for use with CiscoWorks VPN/Security Management Solution 2.x (VMS). VMS customers are entitled to upgrade to Security Manager at no cost. See <http://www.cisco.com/go/csmanager>.

---

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 version of *Installation Guide for Cisco Security Manager* that you received with your copy of Security Manager. Although your version of 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. See the installation guide for the version of Security Manager that you use:

- [Installation Guide for Cisco Security Manager 3.0](#)
- [Installation Guide for Cisco Security Manager 3.0.1](#)



---

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

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

This guide contains:

- A comparison of Performance Monitor and Monitoring Center for Performance.
- High-level descriptions of the hardware and software requirements for installation.
- High-level instructions for installing, upgrading to, and uninstalling Performance Monitor.
- Instructions for migrating your device inventory from Monitoring Center for Performance.
- Bug ID numbers and headlines for problems in Monitoring Center for Performance that were fixed for this release of Performance Monitor.
- 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

The following table describes and categorizes the major differences between Performance Monitor 3.0 and Monitoring Center for Performance:

Category	Comparison
Extended support for devices, services, features, and software versions	<p>Performance Monitor adds:</p> <ul style="list-style-type: none"> <li>• Device support for: <ul style="list-style-type: none"> <li>– 800, 1800, 2800, and 3800 Series routers.</li> <li>– ASA 5500 Series appliances.</li> </ul> </li> <li>• Software version support for: <ul style="list-style-type: none"> <li>– PIX 7.0 and 7.1.</li> <li>– FWSM 2.2, 2.3, and 3.1.</li> <li>– ASA 5500 Series appliances.</li> <li>– VPN Shared Port Adapters (VPN SPA).</li> </ul> </li> <li>• Service and feature monitoring support for: <ul style="list-style-type: none"> <li>– VPN services on PIX appliances.</li> <li>– Firewall services and remote-access VPN services on Cisco IOS routers.</li> <li>– Site-to-site VPN services on VPN 3000 Series concentrators, PIX appliances, and ASA appliances.</li> <li>– DMVPN services.</li> <li>– Easy VPN services.</li> <li>– Multicontext firewall services.</li> </ul> </li> </ul>
Compatibility and coexistence	<ul style="list-style-type: none"> <li>• Performance Monitor runs on CiscoWorks Common Services (Common Services) 3.0.3 or 3.0.4 for Windows and supports coexistence on the same server with Security Manager 3.0 or 3.0.1.</li> <li>• We no longer support coexistence on the same server with any component in, or release of, VMS.</li> <li>• We no longer support coexistence on the same server with any version of Common Services earlier than 3.0.3.</li> <li>• Performance Monitor does not support Solaris as an operating system for servers.</li> </ul>
Importing device credentials	<ul style="list-style-type: none"> <li>• Performance Monitor imports device attributes from a Device Credentials Repository (DCR) server on which SSL is enabled. A DCR is an inventory of credentials and other attributes for network devices that Common Services maintains for use by other applications, such as Security Manager or Resource Manager Essentials (RME).</li> <li>• We no longer support any direct importing of device attributes from CiscoWorks Management Center for VPN Routers (Router MC) or RME.</li> </ul>
User interface (GUI)	The Performance Monitor GUI does not include any Java applets.
Security enhancements	HTTPS now secures all communications between Performance Monitor and the devices in your network.

# 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 3.0.3 (patched) or 3.0.4, or Performance Monitor cannot work.

Performance Monitor by default uses SNMP trap port 162.


**Note**

If you install Common Services 3.0.3 from the Security Manager 3.0 installation DVD, you automatically apply a special patch to it. Performance Monitor requires this special patch when you use Common Services 3.0.3 and cannot run on any server where Common Services 3.0.3 is unpatched. The required patch is available *only* on the Security Manager 3.0 installation DVD. For detailed information, see *Installation Guide for Cisco Security Manager 3.0*.

Alternatively, you can install and use Common Services 3.0.4 without any patch.

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	Minimum Requirement
System hardware	<ul style="list-style-type: none"> <li>• IBM PC-compatible with a 2 GHz or faster processor.</li> <li>• Color monitor with at least 1024 x 768 resolution and a video card capable of 16-bit colors.</li> <li>• DVD-ROM drive.</li> <li>• 100BaseT (100 Mbps) or faster network connection; single interface only.</li> </ul> <p><b>Note</b> We do not support installations of Performance Monitor on servers with more than one network interface card (NIC). For related information, see <a href="#">IP Address, page 5</a>.</p> <ul style="list-style-type: none"> <li>• Keyboard.</li> <li>• Mouse.</li> </ul>
File system	NTFS.
Memory (RAM)	2 GB.

**Table 1** Installation Requirements and Restrictions (continued)

Component	Minimum Requirement
System software	<p>One of the following:<sup>1</sup></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2003 Server: <ul style="list-style-type: none"> <li>– Enterprise Edition with SP1.</li> <li>– Standard Edition with SP1.</li> </ul> </li> <li>• Microsoft Windows 2000: <ul style="list-style-type: none"> <li>– Advanced Server with SP4.</li> <li>– Server with SP4.</li> <li>– Professional with SP4.</li> </ul> </li> </ul> <p><b>Tip</b> In addition, client systems can use Microsoft Windows XP with SP1 or higher.</p> <p><b>Note</b> Performance Monitor supports only the US-English and Japanese versions of Windows. Select <b>Start &gt; Settings &gt; Control Panel &gt; Regional Settings</b>, then set the default locale.</p> <p>Microsoft ODBC Driver Manager 3.510 or later is also required, so that your server can work with Sybase database files. To confirm the installed ODBC version, find and right-click ODBC32.DLL, then select <b>Properties</b> from the shortcut menu. The file version is listed under the Version tab.<sup>2</sup></p>
Browser	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6.0 with SP1 (6.0.2800).</li> <li>• Mozilla 1.7 or 1.7.5.</li> </ul>
Compression software	WinZip 9.0 or compatible.
Hard Drive Space	20 GB.
IP Address	<p>One static IP address.</p> <p>If the server has more than one IP address, disable all but one address. The Performance Monitor installer displays a warning if it detects any dynamic IP addresses on the target server. Dynamic addresses are not supported.</p>

1. To confirm the installed Windows version from the Start menu, select **Run**, then enter either **ver** or **winver**.

2. Alternatively, after you install Performance Monitor, 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 3.0.3 or 3.0.4 on a Windows domain controller.

Do not install this product in an encrypted directory. Common Services 3.0.3 and 3.0.4 do 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 3.0.3 and 3.0.4 support only the Remote Administration mode for Terminal Services.

# Scalability

The following table describes Performance Monitor scalability.

**Table 2** Cisco Performance Monitor Scalability

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

## 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 in order 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 4](#).

The Performance Monitor installation utility does not include any version of Common Services, which you must install before you install Performance Monitor. We recommend that you use your Security Manager installation DVD to install Common Services.

### Before You Begin



### Caution

If *both* of the following statements are true, you must complete Steps 1 through 5 in [Migrating Inventory from Monitoring Center for Performance, page 7](#), *before* you start this procedure:

- You run Monitoring Center for Performance on a Windows server and will re-use its device inventory.
- Your Monitoring Center for Performance server will become your Performance Monitor server.

- 
- Step 1** Go to Cisco.com and log in to your account.
- 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-v3.0-w2k-k9.exe**.
- Step 4** To start the installation, double-click your downloaded copy of the utility, then follow the prompts.

- Step 5** When the installer prompts you to select your license options and enter your license key, you can use a free evaluation license or use the license file on your Security Manager DVD, at `\license_files\mcpULperm.lic`. Until you apply your license to your copy of Performance Monitor, you are limited to the free 90-day evaluation period.
- Step 6** (Optional) Complete Step 7 in [Migrating Inventory from Monitoring Center for Performance, page 7](#).

## Migrating Inventory from Monitoring Center for Performance



### Note

- We support device inventory migrations from Windows versions of Monitoring Center for Performance, but not from Solaris versions.
- Monitoring Center for Performance users cannot upgrade directly to Performance Monitor.
- You cannot migrate your Monitoring Center for Performance database into Performance Monitor.

A PerlScript that you download from Cisco.com and run on your server can convert all of the device attributes in your Monitoring Center for Performance inventory into a CSV file that Performance Monitor can import easily.

However, Performance Monitor uses HTTPS to secure its communications with routers in your network—which Monitoring Center for Performance did not do. For this reason, the generated CSV output can be edited, and you must manually insert HTTPS credentials for every router that you plan to import into Performance Monitor.



### Caution

The CSV file that you create is *plaintext*—confidential but unencrypted information about the devices in your network. We recommend that you secure the file.

- Step 1** To download the device inventory conversion script, do the following:
- From the Windows server on which you run Monitoring Center for Performance, go to Cisco.com and log in to your account.
  - Download the installation utility for Performance Monitor, **DeviceExport.zip**.
- Step 2** When the download is finished, double-click the **DeviceExport.zip** archive to decompress its contents on your server, then open the readme file.
- Step 3** Follow the instructions in the readme file that tell you:
- How and where to install.
  - How to run **ExportToCSV.pl**.

The PerlScript generates your CSV file at `NMSROOT\mcp\conf\devices\ExportedBackup.csv`, where `NMSROOT` is the directory in which you installed Common Services 2.x. The default is `C:\Program Files\CSCOpX`.

- Step 4** Do one of the following:
- If you are installing Performance Monitor on the *same* server on which you installed Monitoring Center for Performance, move **ExportedBackup.csv** to a secure location, so that it is available for your use when you are ready to use it. Otherwise, it will be erased when you install Performance Monitor.
  - If you are installing Performance Monitor on a *different* server than the one on which you installed Monitoring Center for Performance, use SFTP or another method that you trust to transfer the **ExportedBackup.csv** file from your old server to your new server.
- Step 5** If you are installing Performance Monitor on the *same* server on which you installed Monitoring Center for Performance:
- Uninstall Monitoring Center for Performance, Common Services 2.x, and every application that uses Common Services 2.x. See *Installing Monitoring Center for Performance 2.0.1 on Windows*: [http://www.cisco.com/en/US/docs/security/security\\_management/vms/mcp/2.0.2/install/guide/windows/install.html](http://www.cisco.com/en/US/docs/security/security_management/vms/mcp/2.0.2/install/guide/windows/install.html).
  - Install a supported version of Common Services. If you install version 3.0.3, we recommend that you install Common Services from your Security Manager 3.0 installation DVD so that all required patches are installed automatically. See the installation guide for the Security Manager version that you use: [http://www.cisco.com/en/US/products/ps6498/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html).
  - Install Performance Monitor. See *Installing Performance Monitor*, page 6.
- Step 6** (Optional) If you are importing the attributes of routers from the CSV file into your Performance Monitor device inventory:
- Open the CSV file in a text editor.
  - Edit the attributes for every router to insert the HTTPS username in column 15 and the HTTPS password in column 16, as shown in this example:

Unedited (Monitoring Center for Performance)	Edited (Performance Monitor)
10.77.211.6,,,,,,,,,public,,,,,,,,,	10.77.211.6,,,,,,,,,public,,,,,,,,,admin,lab,,,,,,,,
10.77.211.22,,,,,,,,,public,,,,,,,,,	10.77.211.22,,,,,,,,,public,,,,,,,,,

- Save a copy of the edited CSV file.

**Step 7** To learn how to import device attributes from a CSV file, see the “Using the Importing Devices Wizard to Import or Add Devices” topic in the Performance Monitor online help.

## 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 9](#)
- [Reinstalling Performance Monitor, page 10](#)

# 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**.

**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 `\CSCOPx\bin` when you uninstall Performance Monitor, the uninstaller cannot delete `\CSCOPx\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:*

- a. If a folder exists at `C:\Program Files\CSCOPx`, delete, move, or rename the folder.
- b. If the `C:\CMFLOCK.TXT` file exists, delete it.
- c. 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 the Installation” chapter in [Installation and Setup Guide for CiscoWorks Common Services 3.0.3 \(Includes CiscoView\) on Windows](#).

**Step 6** (Optional) 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 “CiscoWorks-ACS Task Registration During Upgrade and Re-installation” in *Installation and Setup Guide for CiscoWorks Common Services 3.0.3 (Includes CiscoView) on Windows*.

To reinstall Performance Monitor or related applications, see [Installing Performance Monitor, page 6](#).

## Resolved Problems

Table 3 lists problems that have been resolved since the release of Monitoring Center for Performance 2.0.2 on Windows. To obtain more information about a resolved problem, click the ID number or use the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

**Table 3**      *Resolved Problems in Cisco Performance Monitor 3.0*

<a href="#">CSCec05521</a> —Notifications are sent only on default ports
<a href="#">CSCec56300</a> —User-defined groups display on every report page
<a href="#">CSCed74579</a> —Find and Search do not work in the event browser
<a href="#">CSCed78301</a> —Event browser does not include errors from a VPN services module
<a href="#">CSCee39642</a> —Authorization not enforced properly when using ACS server
<a href="#">CSCee54033</a> —Cannot use ~ and ^ characters in the device read community string
<a href="#">CSCef77126</a> —Import of Cisco IOS router fails when using the loopback IP address
<a href="#">CSCsa10214</a> —Error when using ACS for AAA but user does not exist on the ACS server
<a href="#">CSCsa14572</a> —The MCP and McpDbEngine processes are both down
<a href="#">CSCsa45319</a> —Fields are empty in the Report page
<a href="#">CSCsa64688</a> —No support for ISR routers in Performance Monitor
<a href="#">CSCsb05674</a> —Cannot delete duplicate devices

# 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 3.0. 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 3.0 Known Problems

<b>CSCeb57907—Cannot import an SSL service module from a CSV file</b>
<b>Description:</b> 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.
<b>CSCec17725—SNMP version 2 traps are required for interface-down events</b>
<b>Description:</b> 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.
<b>CSCec28656—32 KB-rows in a User Session report take 5 minutes or more to load</b>
<b>Description:</b> If the search result is more than 10,000 entries, the User Session report takes 5 minutes or more to load.
<b>CSCec28918—User logged in once but two sessions are displayed in the report</b>
<b>Description:</b> 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.
<b>CSCec49471—User session state marked Active instead of Completed</b>
<b>Description:</b> 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.
<b>CSCed36700—STS: no CPU/mem usage for 831/803 with 12.3(2)T and 12.3(5b)</b>
<b>Description:</b> 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.
<b>CSCed57697—Page Not Found error appears when you start Performance Monitor</b>
<b>Description:</b> You see a Page Not Found error when you try to start Performance Monitor from a supported browser.
<b>CSCed68244—Performance Monitor cannot clear Interface State event in PIX failover</b>
<b>Description:</b> If a PIX device is configured as part of a failover pair, Performance Monitor misinterprets some of the syslog information it receives.
<b>CSCee59388—Cannot see load-balancing Interface Down event</b>
<b>Description:</b> The load-balancing Interface Down event is not displayed in the event browser.
<b>CSCeh54686—A multi-homed Performance Monitor server cannot monitor imported devices</b>
<b>Description:</b> If your Performance Monitor server has more than one NIC, you cannot monitor devices that you import.
<b>CSCsa48691—Import operation does not seem to finish</b>
<b>Description:</b> After you import a device, the GUI describes the status as Running and the import does not seem to finish.

**Table 4** Performance Monitor 3.0 Known Problems (continued)

<b>CSCsc43213</b> —Performance Monitor doesn't discover all security contexts
<b>Description:</b> Some security contexts (virtual firewalls) do not appear if you select <b>Monitor &gt; Firewall</b> .
<b>CSCsc95585</b> —Different CPU usage shown for PIX in STS and Firewall monitoring pages
<b>Description:</b> 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.
<b>CSCsd28035</b> —Tunnel table is empty for Easy VPN server
<b>Description:</b> If you select <b>Monitor &gt; Site-to-Site VPN</b> , then click <b>Tunnels</b> in the TOC, the displayed information does not include Easy VPN tunnels that are configured on IOS routers.
<b>CSCse11165</b> —No memory usage data available for VPN 3000 concentrators
<b>Description:</b> VPN 3000 Series concentrators do not provide any way to poll memory usage statistics. Therefore, if you select <b>Monitor &gt; Site-to-Site VPN</b> , the displayed <i>Memory Usage %</i> value for these concentrators is always zero.
<b>CSCse17747</b> —SNMP access outage on VPN SPA doesn't generate event
<b>Description:</b> 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.
<b>CSCse61189</b> —An error message misrepresents how you obtain a valid license file
<b>Description:</b> An error message tells you to obtain a Performance Monitor license from Cisco.com, but your license file is on your Security Manager installation DVD.
<b>CSCsc95489</b> —Unable to monitor Easy VPN tunnels on PIX 6.3
<b>Description:</b> If you select <b>Monitor &gt; Remote Access VPN</b> , the displayed information does not include Easy VPN tunnels that are configured on PIX 6.3 devices.
<b>CSCsj19705</b> —License error with Perf. Monitor 3.0 on a Security Manager 3.0.2 server
<b>Description:</b> If you choose the free evaluation license when you perform a fresh installation of Performance Monitor 3.0 on a server running Security Manager 3.0.2, an invalid license error is displayed when you start Performance Monitor from the Cisco Security Management Suite page.

## 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 14.

**Table 5** Product Documentation

Document Title	Available Formats
<b>Cisco Security Manager 3.0; Cisco IPS Manager 3.0; Cisco Auto Update Server 3.0</b>	
<i>Installation Guide for Cisco Security Manager 3.0</i>	<ul style="list-style-type: none"> <li>PDF on the product DVD-ROM.</li> <li>On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/installation/guide/ig.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/installation/guide/ig.html</a></li> </ul>

**Table 5 Product Documentation (continued)**

<b>Document Title</b>	<b>Available Formats</b>
<i>User Guide for Cisco Security Manager 3.0</i>	<ul style="list-style-type: none"> <li>PDF on the product DVD-ROM.</li> <li>On Cisco.com at this URL: <a href="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</a></li> </ul>
<i>Supported Devices and Software Versions for Cisco Security Manager 3.0</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/compatibility/information/smdev.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/compatibility/information/smdev.html</a>
<i>FAQs and Troubleshooting Guide for Cisco Security Manager 3.0</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/troubleshooting/guide/trblsht.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/troubleshooting/guide/trblsht.html</a>
<i>Migrating from CiscoWorks VPN/Security Management Solution to Cisco Security Manager</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/migration/guide/migr_gd.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/migration/guide/migr_gd.html</a>
<i>User Guide for Auto Update Server 3.0</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.0/user/guide/ausrvr.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.0/user/guide/ausrvr.html</a>
<i>Supported Devices and Software Versions for Auto Update Server 3.0</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.0/compatibility/information/aus_dev.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.0/compatibility/information/aus_dev.html</a>
<i>User Guide for Cisco IPS Manager 3.0</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/ips_manager/3.0/user/guide/ipsmug.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/ips_manager/3.0/user/guide/ipsmug.html</a>
Context-sensitive online help	Click the Help button in a window or dialog box.
<b>Cisco Performance Monitor 3.0</b>	
<i>Installation and Release Notes for Cisco Performance Monitor 3.0</i> (this document)	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.0/installation/guide/pm3irn.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.0/installation/guide/pm3irn.html</a>
<i>User Guide for Cisco Performance Monitor 3.0</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.0/user/guide/pmug.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.0/user/guide/pmug.html</a>
<i>Supported Devices and Software Versions for Cisco Performance Monitor 3.0</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.0/compatibility/information/pm30dev.html">http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.0/compatibility/information/pm30dev.html</a>
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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

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.

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