



# CHAPTER 8

## Post Installation Server Tasks

The following topics are tasks to complete after you install Security Manager or its related applications on a server.

- [Server Tasks To Complete Immediately](#), page 8-1
- [Verifying That Required Processes Are Running](#), page 8-2
- [Best Practices for Ongoing Server Security](#), page 8-4
- [Verifying an Installation or an Upgrade](#), page 8-4
- [Where To Go Next](#), page 8-5

### Server Tasks To Complete Immediately

Make sure that you complete the following tasks immediately after installation.

✓	Task
<input type="checkbox"/>	<p><b>1. Reenable or reinstall antivirus scanners and similar products.</b> If you uninstalled or temporarily disabled any server security software, such as an antivirus tool or Cisco Security Agent, reinstall or restart that software now, then restart your server if required.</p> <p><b>Note</b> If you see that your antivirus software is reducing the efficiency or responsiveness of a Security Manager server, see your antivirus software documentation for recommended settings.</p>
<input type="checkbox"/>	<p><b>2. Reenable the services and server processes that you disabled for installation.</b> Do not reenable IIS.</p>
<input type="checkbox"/>	<p><b>3. Reenable any mission-critical applications that you disabled for installation, including those that use any Sybase technology or software code.</b></p>
<input type="checkbox"/>	<p><b>4. On the server, add a self-signed certificate to the list of trusted certificates.</b> To learn how, see your browser documentation.</p>
<input type="checkbox"/>	<p><b>5. Check for updates on Cisco.com for Security Manager and its related applications.</b> If you learn that updates are available, install the ones that are relevant to your organization and network.</p>

✓	Task
	<p>6. Do the following if your server has two or more network interface cards configured:</p> <ol style="list-style-type: none"> <li>Select <b>Start &gt; Settings &gt; Control Panel &gt; Administrative Tools &gt; Services</b>, then stop Cisco Security Manager Daemon Manager.</li> <li>Find <i>NMSROOT</i>\lib\vbroker\gatekeeper.cfg, where <i>NMSROOT</i> is the path to the Security Manager installation directory (the default is <b>C:\Program Files\CSCOpX</b>), then open the file in a text editor.</li> <li>Edit these lines: <pre data-bbox="267 531 1109 688">#vbroker.gatekeeper.backcompat.callback.host=external-IP-address #vbroker.se.exterior.host=external-IP-address #vbroker.se.iiop_tp.host=external-IP-address #vbroker.se.interior.host=external-IP-address</pre> <p>so that you delete the # character in every instance and replace the IP address in every instance with the DNS-configured, external, static IP address of the Security Manager server that the client uses for communication.</p> </li> <li>Save your edited version of gatekeeper.cfg, then quit the text editor.</li> <li>Select <b>Start &gt; Settings &gt; Control Panel &gt; Administrative Tools &gt; Services</b>, then restart Cisco Security Manager Daemon Manager.</li> </ol>

## Verifying That Required Processes Are Running

You can run the **pdshow** command from a Windows command prompt window to verify that all required processes are running correctly for the Cisco server applications that you choose to install. Process requirements differ among the applications.



### Tip

To learn more about **pdshow**, see the Common Services documentation.

Use [Table 8-1](#) to understand which applications require which processes.

**Table 8-1** Application Process Requirements

This application:	Requires these Daemon Manager processes:
Common Services 3.1.1	Apache CmfDbEngine CmfDbMonitor CMFOGSServer CSRegistryServer DCRServer diskWatcher EDS EDS-GCF EDS-TR ESS EssMonitor jrm LicenseServer Proxy RmeGatekeeper RmeOrb Tomcat TomcatMonitor
Cisco Security Manager 3.2.1	AthenaOGSServer VmsBackendServer vmsDbEngine vmsDbMonitor
Auto Update Server 3.2.1	AusDbEngine AusDbMonitor CNSEventGateway
Resource Manager Essentials 4.1.1	ChangeAudit ConfigMgmtServer CTMJrmServer EssentialsDM ICServer NCTemplateMgr NetShowMgr RMECSTMServer RMEDbEngine RMEDbMonitor RMEOGSServer SyslogAnalyzer SyslogCollector

**Tip**

To verify that the Windows service called “Cisco Security Agent” is running on your server, select **Start > Settings > Control Panel > Administrative Tools > Services**.

# Best Practices for Ongoing Server Security

The least secure component of a system defines how secure the system is. The steps in the following checklist can help you to secure a server and its OS after you install Security Manager:

✓	Task
☐	<p><b>1. Monitor server security regularly.</b> Log and review system activity. Use security tools such as the Microsoft Security Configuration Tool Set (MSCTS) and Fport to periodically review the security configuration of your server. Review the log file for the standalone version of Cisco Security Agent that is installed sometimes on a Security Manager server.</p> <p><b>Tip</b> You can obtain MSCTS from the Microsoft website and Fport from the Foundstone/McAfee website.</p>
☐	<p><b>2. Limit physical access to your server.</b> If your server contains removable media drives, set the server to boot from the hard drive first. Your data can be compromised if someone boots your server from a removable media drive. You can typically set the boot order in the system BIOS. Make sure you protect the BIOS with a strong password.</p>
☐	<p><b>3. Do not install remote access or administration tools on the server.</b> These tools provide a point of entry to your server and are a security risk.</p>
☐	<p><b>4. Set a virus scanning application to run automatically and continuously on the server.</b> Virus scanning software can prevent trojan horse applications from infecting your server. Update the virus signatures regularly.</p>
☐	<p><b>5. Back up your server database frequently.</b> Store all backups in a secure location with restricted access.</p>

## Verifying an Installation or an Upgrade

You can use Common Services to verify that you installed or upgraded Security Manager successfully.

- 
- Step 1** Use a browser on the client system to log in to the Security Manager server at: **http://<server\_name>:1741**. (To learn which browsers and browser versions are supported, see [Client Requirements, page 2-6](#).)
- Step 2** From the Cisco Security Management Suite page, click the **CiscoWorks** link in the upper right corner.
- Step 3** From the Common Services home page, select **Server > Admin**.  
The administrative GUI appears.
- Step 4** To display the Process Management page, click **Processes**.  
The resulting list names all the server processes and describes the operational status of each process. The following processes must be running normally:
- vmsDbEngine
  - vmsDbMonitor
  - EDS

**Note**

- To learn whether an installed application might require other processes, such as RmeOrb and RmeGatekeeper for RME, read the documentation for that application on Cisco.com. For product documentation URLs, see:
  - [Common Services Documentation](#), page xiv.
  - [Auto Update Server Documentation](#), page xiv.
  - [Resource Manager Essentials Documentation](#), page xiv.
- If you are trying to verify the installation because the Security Manager GUI does not appear or is not displayed correctly, see “[Q.The Security Manager GUI does not appear, or is not displayed correctly, or certain GUI elements are missing. What happened?](#)” in Appendix A, “[Troubleshooting](#).”

## Where To Go Next

If you want to:	Do this:
Understand the basics	See the interactive <i>JumpStart</i> guide that opens automatically when you start Security Manager.
Get up and running with the product quickly	See the “Getting Started with Security Manager” topic in the online help, or see <a href="#">Chapter 1</a> of <i>User Guide for Cisco Security Manager 3.2.1</i> .
Complete the product configuration	See the “Completing the Initial Security Manager Configuration” topic in the online help, or see <a href="#">Chapter 1</a> of <i>User Guide for Cisco Security Manager 3.2.1</i> .
Manage user authentication and authorization	See the following topics in the online help, or see <a href="#">Chapter 2</a> of <i>User Guide for Cisco Security Manager 3.2.1</i> . <ul style="list-style-type: none"> <li>• <a href="#">Setting Up User Permissions</a></li> <li>• <a href="#">Integrating Security Manager with Cisco Secure ACS</a></li> </ul>
Bootstrap your devices	See the “Preparing Devices for Management” topic in the online help, or see <a href="#">Chapter 5</a> of <i>User Guide for Cisco Security Manager 3.2.1</i> .
Install entitlement applications	Your Security Manager license grants you the right to install certain other applications—including specific releases of RME and Performance Monitor—that are not installed when you install Security Manager. You can install these applications at any time. See <a href="#">Introduction to Component Applications, page 1-1</a> .

