



CHAPTER 2

Requirements and Dependencies

You can install and use Security Manager as a standalone product or in combination with several other Cisco security management applications—including optional applications that you can select in the Security Manager installer or download from Cisco.com. Requirements for installation and operation vary in relation to the presence of other software on the server and according to the way that you use Security Manager.



Caution

If you are upgrading to Security Manager 3.1 from an earlier version, you must make sure that the existing Security Manager database does not contain any pending data, meaning data that has not been committed to the database. If the existing Security Manager database contains pending data, you must commit or discard all uncommitted changes before upgrading. For instructions, see [Upgrading Server Applications, page 4-8](#).

CiscoWorks Common Services 3.0.5 is required for Security Manager to work. You install Common Services automatically when you install Security Manager server software. Security Manager cannot coexist on a server with any patched or unpatched Common Services version earlier than 3.0.5. For more information, see

[Common Services, page 1-2](#), and see either the Common Services online help or the Common Services documentation on Cisco.com at <http://www.cisco.com/en/US/products/sw/cscowork/ps3996/>.

**Tip**

We recommend that you synchronize the date and time settings on all of your management servers and all of the managed devices in your network. One method is to use an NTP server. Synchronization is important if you want to correlate and analyze log file information from your network.

The sections in this chapter describe requirements and dependencies for installing Security Manager server and client software:

- [Required Services and Ports, page 2-2](#)
- [Server Requirements, page 2-5](#)
- [Client Requirements, page 2-8](#)

Required Services and Ports

You must ensure that required ICMP (ping), TCP, and UDP ports are enabled and available for use by Security Manager and its associated applications on your server, to support their associated services.

**Tip**

To understand which server processes are associated with the applications that you install from the *Security Manager* installation DVD, see [Verifying That Required Processes Are Running, page 6-3](#).

[Table 2-1](#) sorts the required ports and services numerically, by port.

Table 2-1 *Required Ports and Services*

Service	Used For, or Used By	Port Number/ Range of Ports	Protocol	Inbound	Outbound
Ping	RME	—	ICMP	—	X

Table 2-1 Required Ports and Services (continued)

Service	Used For, or Used By	Port Number/ Range of Ports	Protocol	Inbound	Outbound
SSH	Common Services	22	TCP	—	X
	RME	22	TCP	—	X
Telnet	Common Services	23	TCP	—	X
	DM 6500/7600	23	TCP	—	X
	RME	23	TCP	—	X
TACACS+ (for ACS)	Common Services	49	TCP	—	X
	RME		TCP	—	X
TFTP	Common Services	69	UDP	X	X
HTTP	Common Services	80	TCP	—	X
	DM 6500/7600		TCP	—	X
SNMP (polling)	Common Services	161	UDP	—	X
SNMP (traps)	Common Services	162	UDP	—	X
HTTPs (SSL)	Common Services	443 ¹	TCP	X	—
	Security Manager		TCP	—	X
	AUS		TCP	X	—
Syslog	Common Services	514	UDP	X	—
Remote Copy Protocol	Common Services		TCP	X	X
VisiBroker IIOP port for gatekeeper	Common Services	1683/ 1684	TCP	X	X
HTTP	Common Services	1741	TCP	X	—
	Security Manager		TCP	X	—
MySQL ²	Security Manager	3306, 5501	MyS QL	X	X
Cisco IPS Event Viewer ³	Security Manager server	60002, 60003	TCP	X	X
	Security Manager client	5001	TCP	X	X

Table 2-1 Required Ports and Services (continued)

Service	Used For, or Used By	Port Number/ Range of Ports	Protocol	Inbound	Outbound
HIPO port for CiscoWorks gatekeeper	Common Services	8088	TCP	X	X
Tomcat shutdown	Common Services	9007	TCP	X	—
Tomcat Ajp13 connector	Common Services	9009	TCP	X	—
Database	Security Manager	10033	TCP	X	—
License Server	Common Services	40401	TCP	X	—
Daemon Manager	Common Services	42340	TCP	X	X
Osagent	Common Services	42342	UDP	X	X
Database	Common Services	43441	TCP	X	—
DCR and OGS	Common Services	40050–40070	TCP	X	—
Event Services	Software Service	42350/ 44350	UDP	X	X
	Software Listening	42351/ 44351	TCP	X	X
	Software HTTP	42352/ 44352	TCP	X	X
	Software Routing	42353/ 44353	TCP	X	X
Transport Mechanism (CSTM)	Common Services	50000–50020	TCP	X	—

1. To share and exchange information with a Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance, Security Manager uses HTTPS over port 443 by default. You can choose whether to use a different port for this purpose.
2. Do not delete or move the C:\my.cnf file, which the MySQL server requires.
3. The Cisco IPS Event Viewer service depends on MySQL services. If you want to stop retrieving and storing IPS event alerts, you can stop the Cisco IPS Event Viewer service. Later you can restart the Cisco IPS Event Viewer service to resume retrieving and storing alerts.

Server Requirements


Note

See [Required Services and Ports, page 2-2](#), for a complete list of the service ports that you must enable in order to use your Security Manager server.


Tip

We recommend that you install Security Manager on a dedicated server in a controlled environment. For additional best practices and related guidance, see [Chapter 3, “Preparing a Server for Installation.”](#)

You can install Security Manager on a Windows-based server that uses one CPU or multiple CPUs. [Table 2-2](#) describes server requirements and restrictions.

Table 2-2 **Server 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.

Table 2-2 Server Requirements and Restrictions (continued)

Component	Requirement
System software	<p>One of the following:^{1, 2}</p> <ul style="list-style-type: none"> • Microsoft Windows 2003 Server³: <ul style="list-style-type: none"> – Enterprise Edition with SP1 <i>or</i> Enterprise Edition, Release 2. – Standard Edition with SP1 <i>or</i> Standard Edition, Release 2. • Microsoft Windows 2000³: <ul style="list-style-type: none"> – Advanced Server with SP4. – Server with SP4. – Professional with SP4. <p>Note Security Manager supports only the US-English and Japanese versions of Windows. From the Start Menu, open the Control Panel for Windows⁴, open the panel where you configure region and language settings⁵, 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.⁶</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 (6.0.2600). • Microsoft Internet Explorer 6.0 with SP1 (6.0.2800). • Mozilla 1.7.13.
Compression software	WinZip 9.0 or compatible.
Hard Drive Space	20 GB.

Table 2-2 Server Requirements and Restrictions (continued)

Component	Requirement
IP Address	<p>One static IP address.</p> <p>If the server has more than one IP address, disable all but one address. The Security Manager installer displays a warning if it detects any dynamic IP addresses on the target server. Dynamic addresses are not supported.</p> <p>Note You can reenable additional network interface cards after installation, but you must perform the steps outlined in the Server Tasks To Complete Immediately, page 6-2 if you plan to use multiple network interface cards on your Security Manager server.</p>

1. To confirm the installed Windows version from the Start menu, select **Run**, then enter either **ver** or **winver**.
2. Security Manager does *not* support Windows OS virtualization.
3. Security Manager is not supported on 64-bit Windows operating systems.
4. To open the Control Panel for Windows from the Start Menu, you follow a path that varies according to your Windows version and configuration.
5. The panel where you specify region and language settings for Windows has a name that varies according to your Windows version and configuration.
6. 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 on a Windows domain controller.

Do not install this product in an encrypted directory. Common Services 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 supports only the Remote Administration mode for Terminal Services.

Client Requirements

Table 2-3 describes Security Manager Client requirements and restrictions.

Table 2-3 *Client Requirements and Restrictions*

Component	Requirement
System hardware	<ul style="list-style-type: none"> • IBM PC-compatible with a 1 Ghz or faster processor. • Color monitor with video card set to 24-bit color depth. <p>Tip An older video (graphics) card might fail to display the Security Manager GUI correctly until you upgrade its driver software. To test whether this problem might affect your client system, right-click My Computer, select Properties, select Hardware, click Device Manager, then expand the Display adapters entry. Double-click the entry for your adapter to learn what driver version it uses. You can then do one of the following:</p> <ul style="list-style-type: none"> – If your client system uses an ATI MOBILITY FireGL video card, you might have to obtain a video driver other than the driver that came with your card. The driver that you use must be one that allows you to configure Direct 3D settings manually. Any driver lacking that capability might stop your client system from displaying elements in the Security Manager GUI. – For any video card, go to the web sites of the PC manufacturer and the card manufacturer to check for incompatibilities with the display of modern Java2 graphics libraries. In most cases where a known incompatibility exists, at least one of the two manufacturers provides a method for obtaining and installing a compatible driver. <ul style="list-style-type: none"> • Keyboard. • Mouse.

Table 2-3 Client Requirements and Restrictions (continued)

Component	Requirement
System software	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Windows XP Professional with SP1 or higher.¹ • Microsoft Windows 2003¹: <ul style="list-style-type: none"> – Server Edition with SP1. – Enterprise Edition with SP1. • Microsoft Windows 2000^{1, 2}: <ul style="list-style-type: none"> – Advanced Server with SP4. – Professional with SP4. <p>Note 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>
Memory (RAM)	1 GB.
Virtual Memory/ Swap Space	512 MB.
Hard Drive Space	10 GB.
Browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 6.0 (6.0.2600). • Microsoft Internet Explorer 6.0 with SP1 (6.0.2800). • Mozilla 1.7 or 1.7.5.

Table 2-3 **Client Requirements and Restrictions (continued)**

Component	Requirement
Java	<p>Security Manager Client includes an embedded and completely isolated version of Java. This Java version does not interfere with your browser settings or with other Java-based applications.</p> <p>Note To verify the installed versions of JVM and the Java plug-in, do one of the following:</p> <ul style="list-style-type: none"> • (Internet Explorer) Select Tools > Sun Java Console. • (Mozilla) Select Tools > Web Development > Java Console. • (From a prompt) Enter java -version.

1. Security Manager is not supported on 64-bit Windows operating systems.
2. Security Manager uses and requires a cipher strength of 128 bits for SSL communication. Internet Explorer cannot use 128-bit encryption on systems that run Windows 2000 without Service Pack 4. If your client system uses Windows 2000 without SP4, its copy of Internet Explorer uses 56-bit encryption for SSL connections, and therefore cannot communicate with Security Manager.
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.