Requirements and Dependencies

You can install and use Security Manager as a standalone product or in combination with several other Cisco Security Management Suite 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.

Tip We recommend that you synchronize the date and time settings on all your management servers and all 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 server applications such as Security Manager, Auto Update Server, and Security Manager client software:

Required Services and Ports

Note Security Manager will use predefined and dynamic ports for its internal operation. Port scanners might block those ports and will not let Security Manager to execute those processes. Therefore port scanners such as Qualys should not be enabled. If enabled, it may result in a Security Manager process crash issue which in turn may require a complete reinstallation of Security Manager.

You must ensure that required ports are enabled and available for use by Security Manager and its associated applications on your server so that the server can communicate with clients and servers running associated applications.

The ports that need to be open depend on whether you are using CiscoWorks for AAA or an external server (such as ACS), and whether you are configuring Security Manager to interact with certain other applications:

- **Basic Required Ports**—Table 3-1 lists the basic ports that must be opened, assuming that you have not customized your configuration to use non-default ports. If you are using CiscoWorks for AAA (user authorization) services, and you do not use any of the optional applications, these should be the only ports you need to open.

Table 3-1 Basic Required Ports to Open on the Security Manager Server

Communication	Service	Protocol	Port	In	Out
Security Manager Client to the Security Manager Server.	HTTP, HTTPS	TCP	1741/443	X	—
Security Manager Client to device managers included in the product (such as ASDM).	HTTPS	TCP	443	X	—
Security Manager to Cisco.com for IPS signature and engine update downloads.	HTTP	TCP	80	—	X
	HTTPS	TCP	443	—	X
Security Manager Server to Devices. **Tip** HTTPS and SSH ports are required, but open the Telnet port only if you use Telnet as the transport protocol for one or more devices. Because Telnet transmits passwords in clear text, we recommend that you never use Telnet, and that you do not open the Telnet port.	HTTPS	TCP	443	—	X
	SSH	TCP	22	—	X
	Telnet	TCP	23	—	X
Security Manager Server to Device for configuration rollback operations on IOS devices.	TFTP	UDP	69	X	X
Security Manager to an e-mail server. This port is required only if you configure e-mail notification settings for any of the various functions that can provide these notifications.	SMTP	TCP	25	—	X
Syslog service used by the Security Manager Event Viewer.	Syslog	UDP	514	X	—
Health and Performance Monitor	HTTP, HTTPS	TCP	2012 and 4444	X	X

- **Ports Required By Optional Applications**—If you are using Security Manager with other applications, other ports also need to be opened, as shown in Table 3-2. Open only ports required by applications that you are actually using.

Table 3-2 Ports Required for Optional Server Applications

Communication	Service	Protocol	Port	In	Out
Security Manager Server to and from CS-MARS.	HTTPS	TCP	443	X	X
Security Manager Server to Cisco Secure Access Control Server (ACS).	HTTP, HTTPS	TCP	• 2002 • If port restriction is enabled on the ACS server, allow all ports in the range for HTTP/HTTPS communication. • If port restriction is disabled, allow all HTTP/HTTPS traffic between the Security Manager server and ACS.	—	X

Table 3-2 Ports Required for Optional Server Applications (continued)

Communication	Service	Protocol	Port	In	Out
Security Manager Server to an External AAA Server (configurable in a non-ACS mode).	RADIUS LDAP Kerberos	TCP	1645, 1646, 1812(new), 389, 636 (SSL), 88	—	X
Security Manager Server to Configuration Engine.	HTTPS	TCP	443	—	X
Security Manager Server to AUS.	HTTPS	TCP	443	—	X
Device to AUS. Used to retrieve images and configurations.	HTTP	TCP	1751	X	—
Security Manager Server to TMS Server.	FTP	TCP	21	—	X
Internet browser running on a client system to the browser interface on the Security Manager or AUS server.	HTTP, HTTPS	TCP	1741/443	X	—

Windows Firewall Configuration Script

Beginning with Version 4.4, Security Manager included a Windows Firewall configuration script in the server installer. This script automates the process of opening and closing the ports necessary for Windows Firewall to work correctly and securely; its purpose is to harden your Security Manager server.

At the time of installation, this script is copied to *NMSROOT* but not executed. You can run this script manually to configure Windows Firewall on your Security Manager server; doing so will secure the server by blocking unnecessary ports. [*NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx**.]

This script opens only those "IN" ports that are needed for Security Manager to perform its tasks. Hence the "Firewall.txt" file has the ports that are the bare minimum for Security Manager. If, later, you discover that you want some other port to be open, you can do that.

To run the Windows Firewall script, follow this procedure:

Step 1 Make sure Powershell scripts can run unrestricted:

a. Open the Powershell Command Line Tool.

b. Execute the command "Set-ExecutionPolicy Unrestricted"

Step 2 In NMSROOT, open a command prompt and execute firewall.bat:

a. Output will appear in the folder NMSROOT/log.

b. Windows.FW_Config.wfw is the backup of the Windows Firewall configuration before executing the script.

c. initialfirewallsettings.txt lists the ports that were open BEFORE running the script.

d. finalfirewallsettings.txt lists the ports that are open AFTER running the script.

Step 3 Enable Windows Firewall and use private network settings: Control Panel > Windows Firewall > Turn Windows Firewall on or off > [General tab] > On.

Step 4 Disable Powershell scripts for security:

a. Open the Powershell Command Line Tool.

b. Execute the command “Set-ExecutionPolicy Restricted”

Step 5 [optional] Verify added firewall rules by using Windows Firewall with Advanced Security (not available in Windows 2008 Enterprise Server (Service Pack 2)—64-bit)

Server Requirements and Recommendations

Unless otherwise noted, this section applies to all applications (Security Manager and Auto Update Server).

To install Security Manager, you must be an Administrator or a user with local administrator rights; this also applies if you are installing the client only.

We recommend that you install Security Manager on a dedicated server in a controlled environment. For additional best practices and related guidance, see Chapter 4, “Preparing a Server for Installation.”

Recommended Server

Cisco recommends that you install Security Manager on a Cisco UCS C220 M3 server with the components described in Table 3-3. More information on Cisco UCS (Unified Computing System) is available at http://www.cisco.com/go/ucs.

Installation Practices to Avoid:

- Do not install any application on a primary or backup domain controller. Cisco does not support any use of Common Services on a Windows domain controller.
- Do not install any application in an encrypted directory. Common Services does not support directory encryption.
- Do not install any application 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.

Table 3-3 Server Hardware Requirements and Recommendations

Component	Description
Operating System	One of the following: • Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit • Microsoft Windows Server 2012 R2 Standard—64-bit • Microsoft Windows Server 2012 Standard—64-bit • Microsoft Windows Server 2012 R2 Datacenter—64-bit • Microsoft Windows Server 2012 Datacenter—64-bit English and Japanese are the only supported languages. For complete information, see Understanding Regional and Language Options and Related Settings, page 3-9. 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 **Properties** from the shortcut menu. The file version is listed under the Version tab.
System Hardware	• Processor: Intel Quadcore Xeon 5600 Series or above • Color monitor with at least 1280 x 1024 resolution and a video card capable of 16-bit colors. For AUS-only servers, you can get by with 1024 x 768 resolution. • DVD-ROM drive. • 1 Gbps network adapter. • Keyboard. • Mouse.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Memory (RAM)	16 GB is the minimum needed to use all features of Security Manager. With less memory, features such as Event Management and Report Management are affected. In particular, if the amount of RAM available to the operating system is less than 8 GB, Event Management and Report Manager are disabled during installation. If the memory available to the OS is between 8 and 12 GB, you can turn off Event Management and Report Management, presuming that you do not plan to use them. Configuration Management will be usable in such systems. **Tip** To turn off Event Management, follow this path: Configuration Manager > Tools > Security Manager Administration > Event Management > Enable Event Management > [clear checkbox]. **Tip** To turn off Report Management, simply close the Report Manager application. Although not recommended, you can enable Event Management and Report Management for low memory systems from the Security Manager client after completing the installation (select Tools > Security Manager Administration > Event Management). Keep in mind that enabling Event Management and Report Management on a system with low memory can severely affect the performance of the entire application. If you install AUS on a separate server, the following minimum applies: • AUS-only server—4 GB. We recommend more than 4 GB.
File system	NTFS.
Disk Optimization	Diskeeper 2010 Server. This is a recommendation, not a requirement. Disk optimization can improve performance if the cause of poor performance is disk fragmentation.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Hard drive space	Use a suitable combination of HDDs in a RAID configuration to achieve the disk space required, which is as follows: • 100 GB for the OS partition is recommended by Cisco. • 150 GB for the application (Security Manager) partition is recommended by Cisco. The *minimum* free disk space required for the Security Manager installation alone is 7 GB. If this is not met, then the installation will be aborted. **Note** Cisco strongly recommends installing the OS and application on separate partitions. **Note** The application partition mentioned above and any other event store partitions may not be relevant when using Veritas in HA (high availability) mode. Please refer to the applicable Security Manager high availability documentation (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) and Veritas documentation for further details. • An additional 1.0 TB for log storage for the Event Viewer on a separate partition: This is a requirement, but ONLY if you plan to use Event Viewer. Cisco recommends creating this separate partition on a directly attached storage device. • An additional 1.0 TB or more: This is a requirement, but ONLY if you plan to enable Event Archival. Event Archival functionality creates a secondary storage of events when log storage is required beyond primary storage capacity (for long term preservation etc.). The Secondary Event Store size is required to be bigger than the configured primary storage size, so an additional 1.0 TB or more of disk space is required to use Event Archival. Both primary & secondary event stores can be on a SAN but it is recommended to create the primary store partition on a directly attached storage (DAS) for optimum performance. For more information on SAN storage, see Using SAN Storage, page 3-10 Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. **Tips** • A sustained 10,000 events per second (EPS) consumes about 86 GB of compressed disk space per day. Log rollover happens when 90% of the disk space allocated for event store (primary/secondary) is filled. Smaller disk size causes quicker rollovers. Based on your expected EPS rate and rollover requirements, you can increase or decrease the minimum disk size when using Event Management.
IP address	One static IP address. Dynamic addresses are not supported. **Tip** Security Manager can have multiple network interface cards (NICs) but teaming of NICs for load balancing is not recommended.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Virtual Memory (Paging File)	1.5 x installed memory. This is a recommendation from Microsoft for Windows platforms. It is not a Cisco requirement. Memory paging is necessitated only if the installed RAM on the system is insufficient to handle the load. **Caution:** You must deselect (clear) the checkbox "Automatically manage paging file size for all drives". (The navigation path to this checkbox is Control Panel > System> Advanced System Settings > Performance > Settings > Advanced tab> Virtual Memory > Change.) **Caution:** A special consideration applies if you are using Windows Server 2012 or 2012 R2 (Standard or Datacenter)—64-bit. You need to be aware of this consideration if your server has two independent partitions (e.g., C: and F:). If you follow these steps, ***the installation will fail***: 1. Uncheck (clear the checkbox for) "Automatically manage paging file size for all drives." 2. On your non-system partition (e.g., F:), create the paging file. 3. On your system partition (e.g., C:), retain the option to automatically manage paging file size. 4. Start installing Security Manager. The installer quits with an error message stating not to use a system-managed paging file size.
Antivirus	Real-time protection disabled. This is a recommendation, not a requirement. The system can have an anti-virus application installed, but Cisco recommends disabling real-time protection because it causes a performance penalty. The user can choose to run a quick scan which is scheduled to run at times when there is not much load on the server. **Note** It is mandatory to exclude the NMSROOT directory and the eventing folder from scanning.
Browser	One of the following: • Internet Explorer 8.x, 9.x, 10.x, or 11.x, but only in Compatibility View **Note** When using Internet Explorer (any version) to download the client, ensure that the following setting is correct: Internet Explorer > Tools > Internet Options > Advanced > Security > clear the "Do not save encrypted pages to disk" checkbox. If this setting is not correct (i.e., the checkbox is checked), attempts to download the client will fail. **Tip** To use Compatibility View in Internet Explorer, navigate to Tools > Compatibility View Settings, and add the Security Manager server as a "website to be displayed in Compatibility View." • Firefox 15.0.1 and above supported and recommended
Java Plug-in	There is no requirement to have JRE installed. It is required to have Java scripts enabled in the web browser.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Optional Virtualization Software	You can, optionally, install the application on a system running the following versions of VMware: ESX 4.1 and ESXi versions up to ESXi 5.5. You should allocate at least the same amount of memory to the virtual machine you use with Security Manager as you would for a non-virtualized server. Use of recent generation CPUs with technology designed to improve virtualization performance is recommended (for example, Intel-VT or AMD-V CPUs). **Tip** Allocate two or more CPUs to the VM image. Some processes, such as system backup, can take an unreasonably long time to complete if you use one CPU.

Understanding Regional and Language Options and Related Settings

Security Manager supports only the U.S. English and Japanese versions of Windows. From the Start Menu, open the Control Panel for Windows, open the panel where you configure region and language settings, then set the default locale. (We do not support English as the language in any Japanese version of Windows.)

Tip For a detailed procedure, refer to How to Set the Locale for the Windows Default User Template to U.S. English, page A-21.

Note You must change the default system locale to U.S. English before installing Security Manager; changing the default system locale and rebooting the server does not change the default profile. It is not sufficient for the current user only to have the proper settings; this is because Security Manager creates a new account (“casuser”) that runs all Security Manager server processes.

In addition, the Regional and Language Options in the server operating system must be set correctly. Also, peripheral devices such as keyboards that use other languages can affect the way Security Manager functions.

The following list contains the Regional and Language Options and related settings that you must adhere to in order to successfully install Security Manager:

- The server locale must be U.S. English or Japanese.
- You must avoid using peripheral devices such as keyboards that use other languages; these devices must not even be connected to the server.
- You must take care not to disturb the server settings while using a non-console RDP session to the server; connecting to the server by using a non-console RDP can lead to the locale of the RDP client machine being applied to the server.
- You must check the Regional and Language Options and verify that the language selected for non-Unicode programs is English (United States); the path to that selection is Control Panel > Regional and Language Options > Advanced > Language for non-Unicode Programs.
- You must ensure that the system locale in the Windows Registry is in a supported language. In order to change it, follow this procedure:
  1. In a command window, execute one of the following commands: **regedit.exe** or **regedt32.exe.**

2. Make sure that the localname is supported. The following example is for U.S. English:

   \HKEY_USERS\.DEFAULT\Control Panel\International

   and change LocaleName to en-US

Note Paths and file names are restricted to characters in the English alphabet. Japanese characters are not supported for paths or file names. When selecting files on a Windows Japanese OS system, the usual file separator character \ is supported, although you should be aware that it might appear as the Yen symbol (U+00A5).

Using SAN Storage

You can use SAN storage with Security Manager provided that the storage has acceptable I/O rates and capacity. The following are the main items within Security Manager that require storage, and the storage options that you have in addition to using disk storage that is directly installed in the server:

- Security Manager installation folder (CSCOpx and subfolders)—The application is best installed on a local drive. However, the folder can be direct attached storage (DAS) or block-based SAN storage (FC, FCoE, iSCSI). The high-availability configuration for Security Manager, described in *High Availability Installation Guide for Cisco Security Manager*, requires a shared cluster volume.
- Primary storage for the Event Manager service—If you use Event Viewer to monitor events, you must specify a primary storage location. The primary storage can be direct attached storage (DAS) or block storage (SAN protocol: FC, FCoE, iSCSI) mapped as a local drive.
- Extended storage for the Event Manager service—Any extended storage location is expected to be on SAN storage. The extended storage should be direct attached storage (DAS) or block storage (SAN protocol: FC, FCoE, iSCSI) mapped as a local drive.

Tips

- CIFS and NFS are not supported.
- The supported network storage types are also supported in VMware configurations.

Requirement for iSCSI Volumes

iSCSI volumes using a software initiator may not be available when Security Manager services are about to start after a system reboot. It may take some time for them to be properly initialized.

If Security Manager services have not started, then you need to configure dependency and service startup settings for them (the Security Manager services).

To configure dependency and startup settings, follow this procedure:

Step 1 Execute the following commands in a Windows command prompt to change the startup type of the Cisco Security Manager Daemon Manager, syslog, and tftp services to “Delayed auto start”:

```
sc config CRMDmgtd start= delayed-auto
sc config crmlog start= delayed-auto
sc config crmtftp start= delayed-auto
```

Step 2 Set the dependency of Microsoft iSCSi to the Cisco Security Manager Daemon Manager service by executing the following command:

```
sc config CRMDmgtd depend= MSiSCSI
```

Tip In these commands, the option name includes the equals sign. A space is required between the equals sign and the value.

Step 3 Verify the dependency settings of the Cisco Security Manager Daemon Manager service by executing the following command. It should display the iSCSI initiator dependency setting as "DEPENDENCIES : MSiSCSI"

```
sc qc CRMDmgtd
```

Client Requirements

Table 3-4 describes Security Manager Client requirements and restrictions.

Note The date and time formats that you select for the client must be the same as those used by your server machine. If they are not, Device View in Security Manager may not load properly.

Table 3-4 Client Requirements and Restrictions

Component	Requirement
System hardware	• One CPU with a minimum speed of 2 GHz. • Color monitor with at least 1280 x 1024 resolution and a video card capable of 16-bit colors. • Keyboard. • Mouse.
Operating System	One of the following: • Microsoft Windows 7 SP1 Enterprise—64-bit and 32-bit • Microsoft Windows 8—64-bit and 32-bit • Microsoft Windows 8.1 Enterprise Edition—64-bit and 32-bit • Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit • Microsoft Windows Server 2012 R2 Standard—64-bit • Microsoft Windows Server 2012 Standard—64-bit • Microsoft Windows Server 2012 R2 Datacenter—64-bit • Microsoft Windows Server 2012 Datacenter—64-bit **Note** Security Manager supports only the U.S. English and Japanese versions of Windows. From the Start Menu, open the Control Panel for Windows, open the panel where you configure region and language settings, then set the default locale. (We do not support English as the language in any Japanese version of Windows.)

Table 3-4 Client Requirements and Restrictions (continued)

Component	Requirement
Memory (RAM)	For 32 bit systems: • Minimum: 2 GB • Recommended: > 2 GB For 64 bit systems: • Minimum: 4 GB • Recommended: > 4 GB.
Virtual Memory (Paging File)	512 MB. **Caution:** You must deselect (clear) the checkbox "Automatically manage paging file size for all drives". (The navigation path to this checkbox is Control Panel > System > Advanced System Settings > Performance > Settings > Advanced tab> Virtual Memory > Change.) **Caution:** A special consideration applies if you are using Windows Server 2012 or 2012 R2 (Standard or Datacenter)—64-bit. You need to be aware of this consideration if your server has two independent partitions (e.g., C: and F:). If you follow these steps, ***the installation will fail***: 1. Uncheck (clear the checkbox for) "Automatically manage paging file size for all drives." 2. On your non-system partition (e.g., F:), create the paging file. 3. On your system partition (e.g., C:), retain the option to automatically manage paging file size. 4. Start installing Security Manager. The installer quits with an error message stating not to use a system-managed paging file size.
Hard Drive Space	10 GB free disk space.
Browser	One of the following: • Internet Explorer 8.x, 9.x, 10.x, or 11.x, but only in Compatibility View **Note** When using Internet Explorer (any version) to download the client, ensure that the following setting is correct: Internet Explorer > Tools > Internet Options > Advanced > Security > clear the "Do not save encrypted pages to disk" checkbox. If this setting is not correct (i.e., the checkbox is checked), attempts to download the client will fail. **Tip** To use Compatibility View in Internet Explorer, navigate to Tools > Compatibility View Settings, and add the Security Manager server as a "website to be displayed in Compatibility View." • Firefox 15.0.1 and above supported and recommended
Java Plug-in	There is no requirement to have JRE installed. It is required to have Java scripts enabled in the web browser. The Security Manager client includes an embedded and completely isolated version of Java (JRE 1.7.x). This Java version does not interfere with your browser settings or with other Java-based applications.

Table 3-4 Client Requirements and Restrictions (continued)

Component	Requirement
Windows user account	You must log into the workstation with a Windows user account that has Administrator privileges to use the Security Manager client. Although some features of the client might work with lesser privileges, only Administrator users are fully supported.