Deployment Planning Guide for Cisco Security Manager 4.12

First Published: August 8, 2016

Introduction

This document provides guidance on planning a deployment of Cisco Security Manager 4.12. It encompasses these topics: included applications, recommended server hardware, client hardware, sizing and software based on reference networks, deployment options for the set of applications included with Security Manager, advanced Security Manager server tuning options, and licensing. For more information about Security Manager software features, refer to product documentation located at http://www.cisco.com/go/csmanager.

This document complements other Security Manager user documentation such as the *User Guide for Cisco Security Manager 4.12* and the *Installation Guide for Cisco Security Manager 4.12*.

Cisco Security Manager 4.12 Applications

Each Cisco Security Manager 4.12 installation has six main applications and one application designed for mobile devices:

- Configuration Manager
- Event Viewer
- Report Manager
- Health and Performance Monitor
- Image Manager
- Dashboard
- CSM Mobile

Cisco Systems, Inc.
www.cisco.com

Configuration Manager

Configuration Manager enables you to centrally manage security policies for over 250 different types and models of Cisco security devices. Security Manager supports integrated provisioning of firewall, IPS, and VPN (most Site-to-site, Remote Access and SSL) services across:

- IOS/ISR/ASR routers
- Catalyst switches
- ASA and PIX security appliances
- Catalyst Service Modules related to firewall, VPN, and IPS
- IPS appliances and various service modules for routers and ASA devices

For a complete list of devices and OS versions supported by Security Manager, please refer to *Supported Devices and Software Versions for Cisco Security Manager* on Cisco.com.

Event Viewer

The high-performance and easy-to-use integrated Event Viewer allows you to centrally monitor events from IPS, ASA, and FWSM devices and correlate them to the related configuration policies. This helps you identify problems and troubleshoot configurations. Then, using Configuration Manager, you can make adjustments to the configurations and deploy them. Event Viewer supports event management for Cisco ASA, IPS, and FWSM devices.

In addition to the Primary Event Data Store, events can be copied and stored in the Extended Event Data Store. The Extended Event Data Store can be used to back up and archive a larger number of events. This is useful for historical review and analysis of events where Event Viewer can gather event data from both the Primary Event Data Store and the Extended Event Data Store. The Extended Event Data Store can be enabled in Event Management in Security Manager's Administration settings.

For supported platforms and more information, refer to the "Monitoring, Reporting, and Diagnostics" part of the *User Guide for Cisco Security Manager 4.12* and *Supported Devices and Software Versions for Cisco Security Manager* on Cisco.com.

Report Manager

The integrated Report Manager application allows you to generate and schedule ASA, IPS, and Remote Access VPN reports. Reports for ASA and IPS devices are created by aggregating and summarizing events collected by Event Viewer. Security reports can be utilized to efficiently monitor, track, and audit network use and security problems reported by managed devices. Users can use Report Manager to develop and customize reports for Cisco ASA and IPS devices.

For supported platforms and more information, refer to the "Monitoring, Reporting, and Diagnostics" part of the *User Guide for Cisco Security Manager 4.12* and *Supported Devices and Software Versions for Cisco Security Manager* on Cisco.com.

Health and Performance Monitor

The Health and Performance Monitor has the following features:

- Provides monitoring capabilities for ASA, VPN, and IPS devices
- Provides trending graphs for critical metrics
- Provides a summary panel for consolidated health, alert, and metric value information within a view
- Provides an alert mechanism for different monitoring parameters
- Provides a set of pre-defined monitoring views
- Allows users to create, edit, and delete custom monitoring views

Image Manager

The Image Manager provides for complete image management for ASA devices. Specifically, it helps the user in the various stages of the ASA image upgrade process by doing the following:

- Downloading and maintaining a repository of the different types and versions of images
- Evaluating the images
- Analyzing the impact of upgrading these images to the devices (the analysis includes the impact of upgrade on device configuration)
- Preparing and planning the upgrade
- Providing a reliable and stable way to upgrade devices with sufficient fallback and recovery mechanisms built in, ensuring minimal downtime

Dashboard

The Dashboard is a configurable launch point for Security Manager that makes IPS and FW tasks more convenient for you. In addition to the original dashboard, you can create new, additional dashboards, and you can customize all dashboards. By using the dashboard, you can accomplish in one place many tasks that are found in several other areas of Security Manager, such as the IPS Health Monitor page, Report Manager, Health and Performance Monitor, and IP Intelligence Settings.

CSM Mobile

CSM Mobile allows you to access device health summary information from mobile devices. The information available to you in this way is the same as that available in the Device Health Summary widget in the Dashboard: current high or medium severity active alerts generated by HPM. Alerts can be grouped by Alert-Description, Predefined-Category, Device, or Alert Technology.

The principal users of CSM Mobile are expected to be those who use an Apple iPad, an Apple iPhone, the Google Chrome browser, or the Apple Safari browser.

Syslog Relay

In addition to events being received by the Security Manager server, they can be forwarded to a maximum of two external/remote controllers (syslog hosts). This feature, syslog relay, will forward the received messages to another syslog host using the UDP syslog protocol.

Retain the original source address of the message

This feature provides the option of preserving the original source IP address of the message. That is, if the user wants to show the events received on the remote controller source IP address. This is the default configuration.

Use CSM server IP address as source IP address

When this option is enabled in the config file, all syslog messages forwarded from the Security Manager server will have the Security Manager server's IP address as the source IP address of the syslog message.

For configuration and setup details, refer to *User Guide for Cisco Security Manager 4.12* on Cisco.com.

Caution Spoofing IP addresses can be achieved only if it has been allowed by network policy.

Common Services 4.2.2

CiscoWorks Common Services 4.2.2 (Common Services) is required for Security Manager 4.12 and Auto Update Server 4.12 to work. Common Services is installed by default when you select Security Manager 4.12 or Auto Update Server 4.12 for installation.

Common Services provides the framework for data storage, login, user role definitions, access privileges, security protocols, and navigation. It also provides the framework for installation, data management, event and message handling, and job and process management. Common Services supplies essential server-side components to Security Manager that include the following:

- SSL libraries
- An embedded SQL database
- The Apache web server
- The Tomcat servlet engine
- The CiscoWorks home page
- Backup and restore functions

For more information, refer to the Common Services documentation that is included with the Security Manager installation. To do this, log on to the server where you installed Security Manager, double-click the Cisco Security Manager icon, log on, click **Server Administration**, and then click **Help**.

Local RBAC Using Common Services

Prior to Security Manager 4.3, the major advantages of using Cisco Secure ACS were (1) the ability to create highly granular user roles with specialized permission sets (for example, allowing the user to configure certain policy types but not others) and (2) the ability to restrict users to certain devices by configuring network device groups (NDGs). These granular privileges (effectively “role-based access control,” or RBAC) were not available in Security Manager 4.2 and earlier versions, unless you used

Cisco Secure ACS. These granular privileges (RBAC) are available in Security Manager 4.3 and later versions because they use Common Services 4.0 or later, in which local RBAC is available without the use of ACS. For more information, refer to the *Installation Guide for Cisco Security Manager 4.12*.

Auto Update Server 4.12

Auto Update Server (AUS) enables you to upgrade device configuration files and software images on PIX Security Appliance (PIX) and Adaptive Security Appliance (ASA) devices that use the auto update feature. AUS supports a pull model of configuration that you can use for device configuration, configuration updates, device OS updates, and periodic configuration verification. In addition, supported devices that use dynamic IP addresses in combination with the Auto Update feature can use AUS to upgrade their configuration files and pass device and status information.

In this method, Security Manager deploys configuration updates to the AUS server, and the managed device contacts the AUS server to download new configuration updates using a periodic time interval, a specific date and time, or on demand.

AUS increases the scalability of your remote security networks, reduces the costs involved in maintaining a remote security network, and enables you to manage dynamically addressed remote firewalls.

AUS uses a browser-based, graphical user interface and requires Common Services 4.2.2. For more information about AUS, refer to the documentation located at http://www.cisco.com/go/csmanager.

Related Applications

Other applications are available from Cisco that integrate with Security Manager to provide additional features and benefits:

Cisco Secure Access Control Server (ACS) 4.2.x

You can optionally configure Security Manager to use ACS for authentication and authorization of Security Manager users. ACS supports defining custom user profiles for fine-grained role-based access control (RBAC) and the ability to restrict users to specific sets of devices or operations.

For details on configuring Security Manager and ACS integration refer to the *Installation Guide for Cisco Security Manager 4.12*. For more information about ACS you can visit http://www.cisco.com/go/acs.

Cisco CNS Configuration Engine 3.5 and 3.5(1)

Security Manager supports the use of Cisco Configuration Engine 3.5 and 3.5(1) as a mechanism for deploying device configurations. Security Manager deploys the delta configuration file to the Cisco Configuration Engine, where it is stored for later retrieval from the device. Devices such as Cisco IOS routers, PIX, and ASA firewalls that use a Dynamic Host Configuration Protocol (DHCP) server contact the Cisco Configuration Engine for configuration (and image) updates. Security Manager also supports management of devices which have a static IP address via CNS configuration engine. In such cases, the discovery is done live and the deployments to the device happen via the CNS configuration engine.

For more information about the Configuration Engine you can visit http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-engine/index.html.

Minimum Hardware and Software Requirements

Each Security Manager server installation requires a single dedicated physical server or virtual machine for Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, Image Manager, and Dashboard. Auto Update Server, an optional component, can be installed on the same or a separate system.

Table 1 is the list of minimum hardware and software specifications for Cisco Security Manager server software and other, optional module installation. While Security Manager software can be installed on a system with minimum specifications, its performance and capacity is limited to smaller deployment (managing up to 25 devices). For larger deployments, you should use a physical server with the specifications recommended in the Recommended Hardware and Software Specifications section.

Table 1 Minimum Server Hardware and Software

Minimum Server Hardware	
Recommended Server	Cisco UCS C220 M3 or equivalent
CPU	1 x Intel Xeon Four-core 5600 Series. This four-core (quad-core) CPU is the minimum. Additional cores provide better performance.
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 Viewer 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 Viewer and Report Manager, presuming that you do not plan to use them. Configuration Management will be usable in such systems. Although not recommended, you can enable Event Viewer and Report Manager 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 Viewer and Report Manager 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. **Note** Memory utilization on the server, as shown by Windows Task Manager, may be 99% while performing configuration operations. This does not indicate a problem; this is normal because all processes and functions of Security Manager use or allocate their respective allocated memory.

Table 1 Minimum Server Hardware and Software (continued)

Hard drive space	Use a suitable combination of HDDs 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. **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.
Supported Devices	up to 25
Network adapter	1 Gbps

Table 1 Minimum Server Hardware and Software (continued)

Minimum Server Software	
Operating System	One of the following: • 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

Table 2 is the list of minimum hardware and software specifications for Cisco Security Manager client software installation. Cisco recommends installing the Security Manager client software on a dedicated machine:

Table 2 Minimum Client Hardware and Software

Minimum Client Hardware	
CPU	Dual-Core 2.0 GHz or better
Memory	For 32 bit systems: • Minimum: 2 GB • Recommended: > 2 GB For 64 bit systems: • Minimum: 4 GB • Recommended: > 4 GB.
HDD	10 GB free space
Display	1280 x 1024
Network adapter	1 Gbps

Table 2 Minimum Client Hardware and Software (continued)

Minimum Client Software	
Operating System	One of the following: • Microsoft Windows 8—64-bit and 32-bit • Microsoft Windows 8.1 Enterprise Edition—64-bit and 32-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 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.)
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 (that is, the checkbox is checked), attempts to download the client will fail. • Firefox 15.0.1 and above supported and recommended

Virtual Machine Hardware and Software Requirements

For virtual machine hardware and software requirements, refer to Table 3, Recommended OS Support by VMware ESXi versions.

Recommended Hardware and Software Specifications

Performance improvements with Security Manager have been observed when going from a single processor (or core) server to a multiple-processor (or core) server. Cisco recommends that you use proper hardware and software specifications to have optimal performance. Cisco also recommends sizing the server for future expansions.

For best performance, a Security Manager server with a 2.66-MHz Intel Xeon quad-core processor (with Hyper-Threading) or faster is recommended at a minimum. If Event Management is used, it is highly recommended to have a dedicated hard disk or storage volume to be used for Security Manager applications and a dedicated disk or volume for event storage. For a Security Manager client system, you can use the minimum hardware specifications specified in the Minimum Hardware and Software Requirements section of this document.

The following specifications are lists of recommended specifications for a Security Manager server for different sizes of deployments:

- VM Support by Operating System

- Small Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0
- Small Deployment with Hyper-V and Windows Server 2012 R2
- Medium Enterprise Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0
- Medium Enterprise Deployment
- Large Enterprise Deployment
- Large Retail Deployment

These specifications are general guidelines on the proper hardware and software to support such deployments based on the number of devices; performance results might vary depending on other factors discussed in the Deployment Scenarios section of this document. These hardware and software requirements for Security Manager are the same for new installations and for upgrading to version 4.12 from previous versions of Security Manager.

VM Support by Operating System

Recommended OS support by VMware ESXi versions are listed in Table 3:

Table 3 Recommended OS Support by VMware ESXi versions

	ESXI Versions							
Guest OS	**4**	**4.1**	**5**	**5.1**	**5 Update 2**	**5.1 Update 2**	**5.5**	**6.0**
Windows Server 2012 R2	No	No	No	No	Yes	Yes	Yes	Yes
Windows Server 2012	No	No	No	No	Yes	Yes	Yes	Yes
Windows Server 2008 R2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Server 2008	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Small Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Recommended specifications for a Security Manager server for a small deployment with VMware ESX 5.1U2 and VMware ESXi versions up to ESXi 6.0 are listed in Table 4:

Table 4 Small Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Note VMware performance is gated by the load generated by other VMs on the same host system, so these VM sizing figures are based on a system that is not under heavy load by other VMs.	
Recommended Host Server	Cisco UCS C220 M3 or equivalent
Virtual CPU	6 vCPUs. Having more vCPUs provides better performance.
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 Viewer 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 Viewer and Report Manager, presuming that you do not plan to use them. Configuration Management will be usable in such systems. Although not recommended, you can enable Event Viewer and Report Manager 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 Viewer and Report Manager 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. **Note** Memory utilization on the server, as shown by Windows Task Manager, may be 99% while performing configuration operations. This does not indicate a problem; this is normal because all processes and functions of Security Manager use or allocate their respective allocated memory.

Table 4 Small Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Hard drive space	Use a suitable combination of HDDs 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 7GB. 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. **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.
Host Server HDD RAID	RAID inside a VM is not applicable since it uses a virtualized file system on top of the underlying host system's HDD configuration. Also, software-based RAID cannot be used with a VMware ESX VM. For more information, refer to documentation published by VMware, Inc.

Table 4 Small Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Network adapter	1 Gbps
Operating System	One of the following: • 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
Recommended Sizings	
Max number of devices	up to 100
Maximum Cumulative EPS Supported	5000 Events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 4500 syslog + 500 SDEE)]
Max concurrent users	Two concurrent users at most (one configuration-only user and one user using event and/or reporting screens)

Small Enterprise Deployment

Recommended specifications for a Security Manager server for a small enterprise deployment are listed in Table 5:

Table 5 Small Enterprise Deployment

Recommended Server	Cisco UCS C220 M3 or equivalent
CPU	1 x Hex Core (X5670 or equivalent series recommended)

Table 5 Small Enterprise Deployment (continued)

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. 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. **Note** Memory utilization on the server, as shown by Windows Task Manager, may be 99% while performing configuration operations. This does not indicate a problem; this is normal because all processes and functions of Security Manager use or allocate their respective allocated memory.

Table 5 Small Enterprise Deployment (continued)

Hard drive space	Use a suitable combination of HDDs 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. **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.
Network adapter	1 Gbps

Table 5 Small Enterprise Deployment (continued)

Operating System	One of the following: • 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
Recommended Sizings	
Max number of devices	up to 100
Maximum Cumulative EPS Supported	5000 Events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 4500 syslog + 500 SDEE)]
Max concurrent users	Four concurrent users at most (two configuration-only users and two users using event and/or reporting screens)

Small Deployment with Hyper-V and Windows Server 2012 R2

Recommended Server	Cisco UCS C220 M3 or equivalent
Hyper-V Server Core	Hyper-V Server 2012 R2
Virtual CPU	6 vCPUs. Having more vCPUs provides better performance
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. 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. **Note** Memory utilization on the server, as shown by Windows Task Manager, may be 99% while performing configuration operations. This does not indicate a problem; this is normal because all processes and functions of Security Manager use or allocate their respective allocated memory.

Hard drive space	Use a suitable combination of HDDs 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. **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.
Network adapter	1 Gbps

Operating System	One of the following: • 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
Recommended Sizings	
Max number of devices	up to 100
Maximum Cumulative EPS Supported	5000 Events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 4500 syslog + 500 SDEE)]
Max concurrent users	Four concurrent users at most (two configuration-only users and two users using event and/or reporting screens)

Medium Enterprise Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Recommended specifications for a Security Manager server for a medium deployment with VMware ESX 5.1U2 and VMware ESXi versions up to ESXi 6.0 are listed in Table 6:

Table 6 Medium Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Note VMware performance is gated by the load generated by other VMs on the same host system, so these VM sizing figures are based on a system that is not under heavy load by other VMs.	
Recommended Host Server	Cisco UCS C220 M3 or equivalent
Virtual CPU	12 vCPUs. Having more vCPUs provides better performance.
Memory (RAM)	• 16 GB for Configuration Manager only • 24 GB for all functions **Note** Memory utilization on the server, as shown by Windows Task Manager, may be 99% while performing configuration operations. This does not indicate a problem; this is normal because all processes and functions of Security Manager use or allocate their respective allocated memory.

Table 6 Medium Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Hard drive space	Use a suitable combination of HDDs 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. **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.
Host Server HDD RAID	RAID inside a Hyper-V is not applicable since it uses a virtualized file system on top of the underlying host system's HDD configuration. Also, software-based RAID cannot be used with a VMware ESX VM. For more information, refer to documentation published by VMware, Inc.

Table 6 Medium Deployment with VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0

Network adapter	1 Gbps
Operating System	One of the following: • 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
Recommended Sizings	
Max number of devices	up to 200
Maximum Cumulative EPS Supported	10000 Events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e.9000 syslog + 1000 SDEE)]
Max concurrent users	Two concurrent users at most (one configuration-only user and one user using event and/or reporting screens)

Medium Enterprise Deployment

Recommended specifications for a Security Manager server for a medium enterprise deployment are listed in Table 7:

Table 7 Medium Enterprise Deployment

Recommended Server	Cisco UCS C220 M3 or equivalent
CPU	1 x Hex Core (X5670 or equivalent series recommended)
Memory (RAM)	• 16 GB for Configuration Manager only • 24 GB for all functions **Note** Memory utilization on the server, as shown by Windows Task Manager, may be 99% while performing configuration operations. This does not indicate a problem; this is normal because all processes and functions of Security Manager use or allocate their respective allocated memory.

Table 7 Medium Enterprise Deployment (continued)

Hard drive space	Use a suitable combination of HDDs 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. **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.
Network adapter	1 Gbps

Table 7 Medium Enterprise Deployment (continued)

Operating System	One of the following: • 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
Recommended Sizings	
Max number of devices	up to 200
Maximum Cumulative EPS Supported	10,000 Events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 9000 syslog + 1000 SDEE)]
Max concurrent users	Seven concurrent users at most (five configuration-only users and two users using event and/or reporting screens)

Large Enterprise Deployment

Recommended specifications for a Security Manager server for a large enterprise deployment are listed in Table 8:

Table 8 Large Enterprise Deployment

Recommended Server	Cisco UCS C220 M3 or equivalent
CPU	2 x Hex Core (X5670 or equivalent series recommended)
Memory (RAM)	• 24 GB for Configuration Manager only • 32 GB for all functions **Note** Memory utilization on the server, as shown by Windows Task Manager, may be 99% while performing configuration operations. This does not indicate a problem; this is normal because all processes and functions of Security Manager use or allocate their respective allocated memory.

Table 8 Large Enterprise Deployment (continued)

Hard drive space	Use a suitable combination of HDDs 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. **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.
Network adapter	1 Gbps

Table 8 Large Enterprise Deployment (continued)

Operating System	One of the following: • 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
Recommended Sizings	
Max number of devices	up to 500
Maximum Cumulative EPS Supported	10,000 Events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 9000 syslog + 1000 SDEE)]
Max concurrent users	Ten concurrent users at most (five configuration-only users and five users using event and/or reporting screens)

Note For enabling event archival, additional storage capacity the same size as the primary store or bigger is required.

Note The above sizing guidelines are based on firewall devices having an average of 3000-5000 rules. If the number of rules is much larger than this number, either the number of devices supported in the deployment should be reduced or the next higher hardware should be considered.

Large Retail Deployment

Recommended specifications for a Security Manager server for a large retail deployment are listed in Table 9:

Table 9 Large Retail Deployment

Recommended Server	Cisco UCS C460 M2 or equivalent
CPU	4 x 8-Core

Table 9 Large Retail Deployment (continued)

Memory (RAM)	64 GB (minimum in all cases). For more detailed information, please refer to the Notes on the UCS C460 memory configuration that appear immediately below this sentence. **Notes** **1)** The application may not use all the higher RAM specified here, but having a larger RAM configuration with higher-end models such as the Cisco UCS C460 (in which most of the DIMM modules are populated) provides better hardware performance. The UCS C460 M1 user documentation makes the following very important point: "There are 16 DIMM slots per CPU (8 per memory riser board). System performance is optimized when memory type and quantity are equal for all memory channels on all CPUs. (The UCS C460 M1 server has four memory channels per CPU)." (http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/spec_sheet_c17-644207.pdf) **2)** The UCS C460 M1 user documentation recommends 64 GB RAM for average performance and 128 GB RAM for "good" performance. (http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/spec_sheet_c17-644207.pdf) **3)** The UCS 460 M1 and the UCS 460 M2 specification documents can be used to further understand memory configurations on the UCS 460 servers: – UCS 460 M1: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/spec_sheet_c17-644207.pdf – UCS 460 M2: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps11587/spec_sheet_c17-662220.pdf

Table 9 Large Retail Deployment (continued)

Hard drive space	Use a suitable combination of HDDs 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. Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. Set the write policy for sequential operation (which is not most cases) to write back; otherwise, set the write policy to write through always. Setting the write policy to write through will improve performance as well. For the application partition, use RAID 1/0. **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.
Network adapter	1 Gbps

Table 9 Large Retail Deployment (continued)

Operating System	One of the following: • 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
Recommended Sizings	
Max number of devices	up to 2500 retail branch firewalls
Maximum Cumulative EPS Supported	15,000 Events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 13,500 syslog + 1500 SDEE)]
Max concurrent users	Five (5) concurrent users at most (accounting for both configuration-only users and users using event and/or reporting screens)

Note For enabling event archival, additional storage capacity the same size as the primary store or bigger is required.

Note **1)** The above sizing guidelines are based on firewall devices having an average of 600 rules with approx. 20,000 associated objects in total. If the number of rules is much larger than this number, either the number of devices supported in the deployment could be reduced or you could consider partitioning the device management across multiple servers.

2) Please note that when performing a configuration change deployment to a large number of devices in a single job, the total time for deployment depends on the actual device response (i.e., the time taken for Security Manager to connect to the device, fetch the latest configuration, etc.). Therefore, it is advisable to consider deployment jobs with under one hundred (< 100) devices per job.

To increase the deployment scalability, you could also consider the following:

a) AUS for ASA-based branch firewalls; see Auto Update Server 4.12, page 5.

b) Cisco CNS CE for IOS-based branch devices; see Cisco CNS Configuration Engine 3.5 and 3.5(1), page 5.

3) It is also possible to tune the Security Manager server to increase the total number of devices to which deployment updates can occur in parallel. This depends on the configuration size of the devices in the inventory, device response times/locations, etc. To tune such parameters for large retail deployments, please get in touch with the Cisco Technical Assistance Center (TAC).

Deployment Scenarios

There are various deployment scenarios possible for Security Manager applications. When deciding on a deployment scenario, you should consider the following important factors, which can affect system performance:

How many devices will Security Manager manage?

Each Security Manager installation does not have a hard limit for number of devices that it manages; however, it is recommended to have fewer than 500 enterprise-class firewalls, or 2500 retail-branch firewalls, per Security Manager server with recommended hardware and software. You should use recommended specifications listed in previous section to manage proper amount of devices per server. The number of devices could be smaller if managed devices have very large configuration. For example, large number of firewall devices with 20,000 – 50,000 rules, large IPS signature set or very large and complex VPN policies with 1000s of branches can cause Security Manager to run under sub-optimal performance. If needed, multiple Security Manager servers should be deployed to manage a larger number of devices and network.

How can policies, objects and devices be managed across multiple Security Manager servers?

Shared policies, objects and devices can be exported and imported from one Security Manager server to others with Policy Export/Import feature. This feature makes it easy to synchronize shared policies and objects across multiple servers. It also can be used to migrate (move) managed devices from one server to another when needed.

What type of devices will be managed with Security Manager? Will performance be varied for different type of devices?

Many types of devices can be managed with Security Manager, but among the most common are firewalls, IPS sensors, and VPN devices; these types of devices provide good examples of how performance can be different for different types of devices.

Some types of devices require policy changes more frequently than other types of devices. For example, devices such as firewalls and IPS sensors require policy changes more frequently than VPN devices; therefore, firewalls and IPS sensors require much more resources than VPN devices. The result is that Security Manager can, in general, manage more devices in a VPN environment than in a firewall or IPS environment.

What is the common size of configuration?

For small environment, this could vary from 100 to 1000s of lines. For medium environment, this could vary from 1000s to 5000 ACLs while some large environment; this number can be from 5000 ACLs to 50,000 ACLs or more. In larger environment, you should consider to reduce number of devices per Security Manager server to prepare enough headroom for future growth.

How many events can Security Manager manage? What are the right settings for firewall and IPS logging?

Event Management can consume a lot of system resources especially in a large environment with many users and devices. While a single Security Manager server can manage up to 10,000 events per second with the right hardware and software specifications, it is recommended that you configure the devices to send only important logs that are required for your operation. Recommended logging levels for firewall devices are from 0:Emergencies to 5:Notifications where 0 produces the least amount of logs to be sent to Security Manager. For additional logging, you can always turn them on per device when necessary for troubleshooting and debugging purposes. Be cautious when using 7:Debugging or 6:Informational level for logging. These should be turned on at only device's console or Device Manager when needed and turned off when done. For IPS device, signature settings can be tuned from Low, Medium, High or Informational. These settings vary in different environments and can affect system performance. Refer to IPS configuration guide for more information.

How many users will use these applications?

Active user sessions also place a load on the server and should be factored in when deciding on the deployment size. For example, an application may not have reached its limit due to the number of devices, but could be nearing maximum load due to simultaneous user sessions, which may warrant dedicating a server to the application. Security Manager supports more than five concurrent users, however maximum number of five real-time event views in Event Viewer can be opened by users at anytime. Event Server does not limit the number of Event Viewer instances connecting to it but places a hard-limit of 5 concurrent real-time event views across all active Event Viewers.

Do you need to deploy AUS with Security Manager?

If you need to deploy AUS with Security Manager, do you require AUS to be highly available or survivable in the event of a site disaster or outage? If you reach the scale limits of AUS installed on a dedicated server, you need to consider deploying more than one instance of it, and on more than one servers.

Does Cisco Security Manager support IPv6 devices?

Prior to Cisco Security Manager 4.12, the Security Manager server communicated with managed devices only over IPv4 addresses. Beginning with version 4.12, Cisco Security Manager supports communication between the Security Manager Server and managed devices over either IPv6 address or IPv4 address. This feature is available only for ASA or FWSM firewall devices. To enable communication over IPv6 addresses, you must first enable IPv6 address on the Security Manager server. For more information refer to the **Getting Started with Security Manager** chapter in the *User Guide for Cisco Security Manager 4.12*.

Cisco Security Manager now supports IPv6 devices but ASA devices do not support an IPv6 Syslog server. In this scenario how does Event Manager work?

Beginning with Cisco Security Manager 4.12, a device added with an IPv6 address will only have an IPv6 address in the Device Inventory. If a device is configured in dual stack then Security Manger communicates with it on the IPv6 address but the device will still use a management IPv4 address to forward syslog packets.

Event Manager internally retrieves the management IPv4 address of the device from its discovery details.Whenever a syslog is received from the device (on the IPv4 address), it automatically matches it to the corresponding IPv6 device display name and displays it in the Event Manager UI.

Note If there are some firewall devices that are reachable only over an IPv6 address from Cisco Security Manager, these devices can be managed by Cisco Security Manager but Event Manager cannot be used for these devices since syslogs cannot be sent over an IPv6 address.

Factors that Affect Application Performance

There are many factors that affect application performance. These include, but are not limited to the followings:

- Server and client hardware (for example, processor, memory, and storage technology)
- Number of managed devices, including the type of the devices, and the complexity of the device and size of configurations (such as large number of ACLs)
- Event management engine, event volume reported by manage device and logging level
- Number and complexity of policy objects

- Number of simultaneous users and the specific activities the users are performing
- Frequency of configuration deployment or IPS signature update for large number of devices
- Number of devices present in a deployment job
- Network bandwidth and latency, such as between Security Manager clients and the server and between the server and the managed devices
- Use of virtualization technology such as VMware ESX
- Use of ACS server for AAA services
- Number of scheduled reports
- Reporting engine, event volume reported by managed devices, and event aggregation

Large geographic distances between a Security Manager client and server results in poor client responsiveness due to the latency introduced. For example, it is not recommended to use a client in India with a server located in California because of the large latency involved. In such cases, we recommend that you employ a remote desktop or terminal server arrangement, where the running clients are co-located in the same datacenter as the server or nearby at least.

Single Server Installation

A single server is the simplest deployment scenario, where you install all Security Manager applications of interest on the same server. For small-scale security environments with one or two network security administrators, a single-server deployment is usually adequate.

Multiple Servers Installation

In some large environment with hundreds or thousand of devices, a single server cannot manage all devices efficiently. For performance reasons you may choose to deploy the Security Manager applications of interest across multiple servers. One possible distribution of the applications is as follows:

Server A: Firewall Policy & Device Management

- Common Services
- Security Manager
- Event/Log Monitoring
- Report Manager
- Auto Update Server *(optional)*
- Image Manager

Server B: IPS Policy & Device Management

- Common Services
- Security Manager
- Event/Log Monitoring
- Report Manager
- Health and Performance Monitor

Server C: VPN Policy & Device Management

- Common Services
- Security Manager
- Event/Log Monitoring
- Report Manager
- Health and Performance Monitor

Server A is dedicated for the Configuration and Event Management for all ASA/PIX/FWSM firewall devices. Server B is dedicated for the Configuration and Event Management for all IPS devices while Server C is dedicated for VPN policy management for ASA/IOS/ISR VPN devices; Server C will also manage firewall devices because those are the ones that will be part of the VPN topology. With this deployment method, the needs of sharing policy data between servers is minimized since each server will use mostly same policy data within itself. However, this deployment is not suitable for network where Security Manager servers might be deployed in great distance away from managed devices, which can affect monitoring, configuration discovery and deployment.

Another method is to divide the devices by region so that each Security Manager will only manage smaller amount of devices for the region (US-West, US-Central, US-East, Europe, or Asia, as examples). This provides optimal performance for management console, event monitoring and configuration deployment of managed devices from their local Security Manager server.

In Multiple Servers deployment, shared policies and objects can be exported and imported between different servers using Policy Import/Export feature. Devices also can be migrated (moved) to different server using Policy Import/Export. This helps to scale management while still keeping policies and objects synchronized across large number of devices in different servers.

Installation in VMware's Virtual Machine Environment

Security Manager supports running in VMware ESXi 5.1U2 and VMware ESXi versions up to ESXi 6.0. Other VMware environments such as VMware Server and VMware Workstation are not supported.

You can use any server operating system supported by Security Manager as guest operating system for VMware. The VMware qualification effort involved running the same set of performance and durability tests that are performed on Security Manager running on a regular non-virtualized server. Test results have shown that running Security Manager in VMware ESX Server 4.0 introduces a modest amount of application performance degradation which varies based on the size of the reference network involved and the specific test case. Deployment of Security Manager in VMware environment is only suitable for smaller size of network.

One area where the performance degradation was usually large was the case of performing a deployment to large number of PIX or ASA devices or a device with large number of rules (on the order of 5 to 50 thousands rules). In this case the deployment took much longer than acceptable speed. For VMware performance best practices you should refer to the following document: http://www.vmware.com/pdf/Perf_Best_Practices_vSphere4.1.pdf.

However, you should avoid tuning any of the advanced VMware parameters, as the default values or settings are generally optimal.

It is also recommended to use one of the later generation servers with a processor that includes technology specifically designed to improve the efficiency of virtualization. For example, good results were obtained when testing Security Manager running in VMware ESX Server 4.0 on an Intel® Xeon® X5500 series Quad-core processor, which includes Intel® Virtualization Technology (IVT). AMD offers 64-bit x86 architecture processors with virtualization extensions, which they refer to as AMD Virtualization (AMD-V).

For virtual machine hardware and software requirements, refer to Table 3, Recommended OS Support by VMware ESXi versions.

High-Availability/Disaster Recovery

You can deploy Security Manager in a high-availability or disaster recovery configuration to significantly improve application availability and survivability in the event of a server, storage, network, or site failure. These deployment options are covered in detail in the applicable Security Manager high availability documentation (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html.

Note A single CSM license is enough to use CSM in VMware HA/DR scenario.

Installation Guidelines

For detailed instructions on Security Manager installation, refer to the *Installation Guide for Cisco Security Manager 4.12*.

Installable Modules

The Security Manager server installation applies to several different components, some of which are optional. The Security Manager installer is responsible for installing the following components:

- Common Services 4.2.2 (installed by default when you select Security Manager 4.12 or Auto Update Server 4.12 for installation)
- Security Manager 4.12 Server (required)
- Auto Update Server 4.12 (optional)
- Security Manager 4.12 Client (optional if the client will be installed on a dedicated client machine)

The Security Manager client can be installed by using a standalone installer. The most common way to access this installer is to log in to the server using a web browser (https://server_hostname_or_ip) and click on the client installer.

Detailed use of the Security Manager installer and the Security Manager client installer are described in the *Installation Guide for Cisco Security Manager 4.12*.

IP address, Hostname and DNS name

Cisco Security Manager requires a static IP address instead of a DHCP address. The IP address of a Security Manager server can be changed, after which a system reboot is required. If a DNS server is configured in Security Manager's TCP/IP settings, make sure that the hostname and DNS name of the Security Manager server are identical and are resolvable by configured DNS servers. Before installing Security Manager, you should choose a permanent DNS and computer hostname for the server, because the hostname and DNS name should not be modified after the installation. Changing the hostname of a Security Manager server after the installation might require re-installing Security Manager.

Note Beginning with version 4.12, Security Manager server to device communication for ASA devices is supported over either IPv6 address or over IPv4 address. The IPv6 address is a 128-bit unique address. For IPv6 address, only Static IP Type is supported. Dynamic IP Type is not supported for IPv6 addresses. For more information refer to the **Getting Started with Security Manager** chapter in the *User Guide for Cisco Security Manager 4.12*.

Client Deployment

The normal and recommended practice is to install and run the Security Manager client on a separate client machine. Security Manager only supports installing a single version of the client on a given machine, so you cannot, for example, have the client for both Security Manager 4.10 and 4.12 on the same machine. You can install and use the client on the server; however, this practice is suitable only for a small size network and is not recommended for the larger enterprise networks.

As mentioned in the Factors that Affect Application Performance section, it may be necessary to deploy the client on a terminal server located near the server to maintain acceptable performance in the event that end users are located a large distance from the server and are experiencing significant latency (for example, intercontinental distances).

Security Manager Server Tuning

Security Manager includes several advanced parameters that you can modify to tune the application performance. For medium and large deployments managing 50 devices or more, you can modify the following parameters in Security Manager for optimal performance:

- Disk Defragmentation
- Windows Operating System's Swap-File size
- Sybase Database Registry Parameters

Disk Defragmentation

It is recommended to do disk fragmentation for every 50 GB increase in the disk size for optimal performance.

Caution Frequent defragmentation will also contribute to bad sectors, eventually leading to disk failure.

Windows Operating System's Swap-File size

Virtual memory (the paging file) should be 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 check box "Automatically manage paging file size for all drives". The navigation path to this check box is Control Panel > System > Advanced System Settings > Performance > Settings > Advanced tab > Virtual Memory > Change.

Sybase Database Registry Parameters

For Medium or Large Deployment, following parameters should be tuned to provide optimal performance and scalability.

Step 1 On the Security Manager server, modify <NMSROOT>\databases\vms\orig\odbc.tmpl as follows using a text editor:

Ensure that the parameter "**___Switches**" contains "**-gb high**".

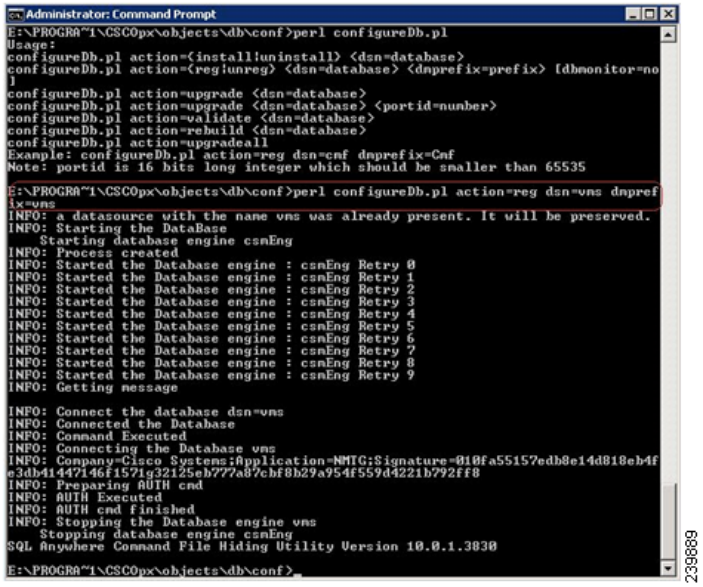
Step 2 Open a command prompt with Administrator rights (right-click on the Command Prompt icon and select "Run as administrator").

Step 3 Shut down Security Manager by entering "**net stop crmdmgtd**" in the command prompt window. Wait until Security Manager is fully shut down before performing the next step.

Step 4 After Security Manager has fully shut down, re-register the database parameters in Windows registry using the configureDb.pl perl utility available in **<NMSROOT>\objects\db\conf**. Here is an example of the command and its syntax:

"**perl configureDb.pl action=reg dsn=vms dmprefix=vms**"

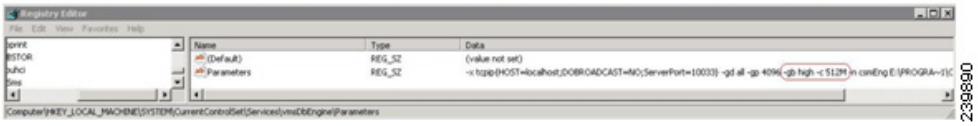
Figure 1 Re-registering Database Parameters



Step 5 Verify that the above parameters are registered properly by checking the following Windows Registry setting:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmsDbEngine\Parameters, there should be **"-gb high –c 512M"** entry:

Figure 2 Verifying Registration of Database Parameters



Step 6 Start Security Manager by entering **"net start crmdmgtd"** in the command prompt window. Wait until Security Manager is fully functional before use.

Understanding Security Manager Licensing

It is important to understand Security Manager licensing when planning a deployment of Security Manager to ensure that you have the correct base license and number of device licenses for the number and type of devices you intend to manage.

For important licensing information, refer to the following documents:

- *Installation Guide for Cisco Security Manager 4.12*
- the product bulletin for the most recent major release of Security Manager at http://www.cisco.com/c/en/us/products/security/security-manager/bulletin-listing.html

Licensing Examples

This section provides some representative licensing examples to help better understand Security Manager licensing.

Example 1

Description of Managed Network: 15 Cisco Integrated Services Routers.

Required Licensing: Enterprise Standard-25 Device license is required. Since there are no Catalyst 6500 services modules involved and there are fewer than 25 devices, order Standard-25 license.

Example 2

Description of Managed Network: 5 IDSM-2 modules, where each module has two virtual sensors.

Required Licensing: Ten licenses are required (10 virtual sensors split between five modules). Although Standard-10 might appear to be sufficient, because a Catalyst 6500 services module is involved, Professional-50 (PRO50) as a minimum is required.

Example 3

Description of Managed Network: 250 pairs of ASAs (500 devices) operating in failover mode.

Required Licensing: Professional-250 license. Alternatively, you could also order a Professional-50 license or a Professional-100 license with suitable incremental ("add-on") device licenses. Incremental device licenses are available in increments of 50, 100, and 250 devices.

Example 4

Description of Managed Network: You have Security Manager Standard-25 device license, but now you need to manage an additional 20 ASA devices operating in single-mode.

Required Licensing: Enterprise Standard-25 to Professional-50 Upgrade license is required.

Example 5

Description of Managed Network: 10 pairs of failover ASA devices (20 devices) deployed in a combination of active/standby or active/active pairs, each has 5 security contexts.

Required Licensing: Enterprise Professional – 50 and Enterprise Professional Incremental 50 Device

When deploying a pair of failover devices for redundancy, you only need to add the active devices and contexts to Security Manager. As such the number of required device licenses is 10 device counts x 5 contexts + 10 chassis for a total of 60 devices license.

Note For complete information on the types of licenses available and the various supported upgrade paths, as well as information about the Cisco Software Application Support service agreement contracts that you can purchase, see the product bulletin for the most recent major release of Security Manager at http://www.cisco.com/c/en/us/products/security/security-manager/bulletin-listing.html.

Note In all the above examples you should consider ordering the corresponding Cisco Service Application Support (SAS) to obtain access to Cisco Technical Assistance Center (TAC) and minor application release updates at no charge.