



Deployment Planning Guide for Cisco Security Manager 3.2.1

Revised: August 26, 2008, and July 29, 2009, OL-17273-01

Contents

- Introduction, page 2
- Cisco Security Manager 3.2.1 Applications, page 2
- Related Applications, page 3
- Installers, page 4
- Understanding Security Manager Licensing, page 4
 - Licensing Overview, page 4
 - Licensing Examples, page 5
- Factors which Affect Application Performance, page 6
- Deployment Scenarios, page 7
 - Single Server, page 8
 - Multiple Servers, page 8
 - High-Availability/Disaster Recovery, page 8
 - VMware Deployments, page 9
 - Client Deployment, page 9
- Reference Networks, page 9
 - Small Enterprise Reference Network, page 10
 - Medium Enterprise Reference Network, page 11
 - Large Enterprise Reference Network, page 11
- Number of Simultaneous Users, page 12
- Server and Client Hardware Recommendations, page 13
 - Server Sizing, page 13
 - Client Sizing, page 13
- Security Manager Tuning, page 14
 - Java Virtual Machine Heap Size, page 14
 - Thread Counts, page 15
- Summary of Security Manager Scalability, page 15



Introduction

This document provides guidance on planning a deployment of Cisco Security Manager 3.2.x. It includes these topics: recommended server and client sizing based on reference networks, deployment options for the set of applications included with Security Manager, licensing, and advanced Security Manager tuning options.

This document complements other Security Manager user documentation such as the Cisco Security Manager user guide and the installation guide.

Cisco Security Manager 3.2.1 Applications

Cisco Security Manager 3.2.1 includes the following applications:

- Common Services 3.1.1

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 applications that include:

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

Common Services is required for all the applications included with Security Manager listed below.

For more information about Common Services you can visit:

<http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/index.html>.

- Cisco Security Manager 3.2.1

Cisco Security Manager is an enterprise-class management application designed to configure firewall, VPN, and intrusion prevention system (IPS) security services on Cisco network and security devices. Security Manager uses a rich-client graphical user interface and requires Common Services 3.1.1

- Auto Update Server 3.2.1

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.
- Cisco IOS routers that use dynamic IP addresses can use AUS in combination with the CNS Gateway protocol to retrieve device IP addresses.

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 3.1.1.

For more information about AUS you can refer to the AUS documentation located at the Security Manager site: <http://www.cisco.com/go/csmanager>.

- Resource Manager Essentials 4.1.1

To support life cycle management, RME provides the ability to manage device inventory and audit changes, configuration files, software images—as well as syslog analysis. RME uses a browser-based graphical user interface. RME is also included with the CiscoWorks LAN Management Solution (LMS). There is useful deployment information about RME included in the *CiscoWorks LAN Management Solution — Deployment Guide 3.0*, although be aware that some information does not apply in the case of RME bundled with Security Manager.

- Performance Monitor 3.2.1

Performance Monitor is a health and performance monitoring application with a special emphasis on security devices and services. Performance Monitor supports the ability to proactively detect network performance issues before they become critical; helps identify portions of the network which are overloaded and potentially require extra resources; and provides rich historical health and performance information for after-the-fact investigations and analyses. Performance Monitor supports monitoring remote-access VPNs, site-to-site VPNs, firewall, web server load-balancing, and SSL termination. Performance Monitor uses a browser-based, graphical user interface and requires Common Services 3.1.1

For more information about Performance Monitor, you can refer to the Performance Monitor documentation located at the Security Manager site: <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 Security Monitoring Analysis and Response System (MARS) — Security Manager supports policy <> event cross-linkages with MARS for firewall and IPS. Using the Security Manager client you highlight specific firewall rules or IPS signatures and request to see the events related to those rules or signatures, respectively. Using the MARS interface you can select firewall or IPS events and request to see the matching rule or signature in Security Manager. These policy <> event cross-linkages are especially useful for network connectivity troubleshooting, identifying unused rules, and signature tuning activities. The policy <> event cross-linkage feature is explained in detailed in the *User Guide for Cisco Security Manager 3.2*. For more information about MARS you can visit <http://www.cisco.com/go/mars>.
- Cisco Secure Access Control Server (ACS) — 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 authorization control and ability to restrict users to specific sets of devices. For details on configuring Security Manager and ACS integration refer to the *User Guide for Cisco Security Manager 3.2*. For more information about ACS you can visit <http://www.cisco.com/go/acs>.
- Cisco CNS Configuration Engine — Security Manager supports the use of the Cisco Configuration Engine as a mechanism for deploying device configurations. Security Manager deploys the configuration file to the Cisco Configuration Engine, where it is stored for later retrieval from the device. Devices, such as Cisco IOS routers, PIX Firewalls, and ASAs that use a Dynamic Host Configuration Protocol (DHCP) server, contact the Cisco Configuration Engine for configuration (and image) updates. For more information about the Configuration Engine you can visit <http://www.cisco.com/en/US/products/sw/netmgts/ps4617/index.html>.

Installers

Security Manager includes four different installers:

- The Security Manager installer which is responsible for installing the following:
 - Common Services 3.1.1
 - Cisco Security Agent 5.2
 - Security Manager 3.2.1 Server (optional)
 - AUS 3.2.1 (optional)
 - Security Manager 3.2.1 Client (optional)—for installing the client on the server
- The Security Manager client installer, which is also available as a standalone installer for the client. The most common way to access this installer is to log in to the server using a web browser and click on the client installer. The client installer executable can also be found on the server at `$NMSROOT\MDC\tomcat\vms\desktop\CSMClientSetup.exe` or on the product DVD under `csm3_2_win_client\CSMClientSetup.exe`.
- The RME installer, which is responsible for installing RME. This installer requires that you have already installed Common Services 3.1.1 using the Security Manager installer.
- Performance Monitor installer, which is responsible for installing Performance Monitor. This installer requires that you have already installed Common Services 3.1.1 using the Security Manager installer.

Detailed use of the Security Manager installer and RME installer is included in the [Installation Guide for Security Manager 3.2.1](#), while use of the Performance Monitor installer is covered in the [Installation and Release Notes for Cisco Performance Monitor 3.2](#).

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. This section provides an overview of Security Manager licensing and some specific license examples.

Licensing Overview

There are three base versions of Cisco Security Manager Enterprise Edition:

- Standard-5
- Standard-25
- Professional-50.

The versions provide management for 5, 25, and 50 devices, respectively.

The Professional version supports incremental device license packages available in increments of 50, 100, 500, and 1000 devices. The Professional version also includes support for the management of Cisco Catalyst® 6500 Series switches and associated services modules; the Standard versions do not include this support.

Security Manager consumes a device license for the following:

- Each added physical device
- Each added Cisco Catalyst 6500 Series services module
- Each security context
- Each virtual sensor

Advanced Inspection and Prevention Security Services Modules (AIP-SSMs), IDS Network Modules, and IPS Advanced Integration Modules (IPS AIM) installed in the host device do not consume a license; however, additional virtual sensors (added after the first sensor) do consume a license.

In the case of a Firewall Services Module (FSWM), the module itself consumes a license and then consumes an additional license for each additional security context. For example, an FSWM with two security contexts would consume three licenses: one for the module, one for the admin context, and one for the second security context. If the Cisco Catalyst chassis itself is added to Cisco Security Manager, it, too, will consume a license.

Unmanaged Devices

In Security Manager you can add unmanaged devices to the device inventory. An unmanaged device is a device for which you have deselected Manage in Cisco Security Manager under Device Properties. An unmanaged device does not consume a license.

Another class of unmanaged device is an object that is added to a topology map. You can use the Map > Add Map Object to add different types of objects on the map such as Clouds, Firewalls, Host, Network, and Router. These objects do not appear in the device inventory and do not consume a device license.

Active and Standby Servers

The license allows the use of the software on a single server. A standby Cisco Security Manager server, such as used in a high-availability or disaster recovery configuration, does not require a separate license if only one server is active at any one time.

Licensing for RME and Performance Monitor

Cisco Security Manager also includes a separate license file for RME and Performance Monitor. You are entitled to use these applications for the same number of devices you have purchased for Cisco Security Manager. When you order a Security Manager base product you receive a second Product Authorization Key (PAK) for the RME and Performance Monitor license.

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: Fifteen device licenses are required. Since there are no Catalyst 6500 services modules involved and there are fewer than 50 devices, order Standard-25 (CSMST25-3.2-K9).

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 two modules). Although Standard-25 might appear to be sufficient, because a Catalyst 6500 services module is involved, Pro-50 (CSMPR50-3.2-K9) as a minimum is required.

Example 3

Description of Managed Network: 350 ASAs operating in single-mode.

Required Licensing: 350 device licenses are required. You can order exactly 350 licenses by ordering Pro-50 (CSMPR50-3.2-K9) and 3 Inc-100s (CSMPR-LIC-100). However, it is less expensive to order Pro-50 and 1 Inc-500 (CSMPR-LIC-500), because the larger the incremental the lower the average cost per device license. Therefore, in some cases it is less expensive to order more licenses than actually required.

Example 4

Description of Managed Network: You have Security Manager Standard Edition - 5 device, but now you need to manage 20 ASAs operating in single-mode.

Required Licensing: Order CSMST25-3.2-K9 and optionally CON-SAS-CSMST253 for SAS coverage. There is no upgrade part number from Standard Edition - 5 device; however, you do not lose your original investment in the Standard Edition - 5 device, because you can combine the Standard 5 license with the Standard 25 license for a net result of Standard Edition - 30 device.

Example 5

Description of Managed Network: 20 ASAs deployed in a combination of active/standby and active/active pairs each with 5 security contexts.

Required Licensing: When deploying a pair of devices for redundancy, you only need to add the active device or context into Security Manager. As such the number of required device licenses is 10 devices x (5 contexts plus 1 chassis each) for a total of 60 licenses. Order Pro-50 and one Inc-50.



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 application minor release updates at no charge.

Factors which Affect Application Performance

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

- 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 configurations
- Number and complexity of policy objects
- Number of simultaneous users and the specific activities the users are performing
- 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
- Security Manager version, due to the addition of new features which can affect performance as well as the introduction of performance enhancements

These topics are discussed in this document. However, 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, due to 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.

Effect of Number of Processors/Cores on Performance

In general, the Security Manager architecture does not leverage multiple processors or cores. However, we do see performance improvements with Security Manager in the range of 30-50 percent when going from a single processor/core to a dual processor/core server. Adding additional processors/cores above two does not significantly improve Security Manager performance.

Effect of Memory Size on Performance

Security Manager operations tend to be bound by different resources. For example, firewall provisioning is primarily a memory-bound process, when IPS signature updating is primarily an I/O bound process. As such additional memory may only benefit certain Security Manager operations which are primarily memory bound and there are ceilings after which additional memory does not improve performance.

Deployment Scenarios

There are various deployment scenarios possible for Security Manager applications. When deciding on a deployment scenario you should consider the following items:

- Which specific applications included with Security Manager do you need to deploy?
- How many devices which each application manage?

If one of the applications you are using is approaching its scale limits (Table 5), it is a good idea to dedicate a server to that application. For obvious reasons of resource allocation and task distribution, it is best not to have other applications using valuable CPU and memory resources if you are trying to manage a large number of devices.

- 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 configuration. 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.

- Do you require the application to be highly available or survivable in the event of a site disaster or outage?

If you reach the scale limits of a specific application installed on a dedicated server, you need to consider deploying multiple instances of the application on different servers. Each running instance of the application needs to be separately purchased and licensed.

Single Server

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 administrator, a single-server deployment is usually adequate.

Multiple Servers

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 (Configuration/Inventory)
 - Common Services
 - Security Manager
 - RME
- Server B (Monitoring)
 - Common Services
 - Performance Monitor
- Server C (Autoupdate)
 - Common Services
 - AUS

Server A is dedicated for the Configuration and Inventory Management applications, namely Security Manager and RME. Server B is dedicated for monitoring. Monitoring tends to place a continuous and potentially heavy load on a server, so there are advantages to using a dedicated set of resources for monitoring. Server C is dedicated for AUS. Since AUS is intended to manage to remote firewalls, it can be resource intensive when many remote devices are contacting AUS for configuration, OS, or DM updates. Also, AUS should normally be placed in the DMZ of the network, so this recommendation alone can lead to dedicating a server for AUS.

For situations where you are reaching the scale limits of either Security Manager or RME, you may also need to split these applications onto dedicated servers. For example, RME also includes a syslog analyzer that can be performance intensive depending on the rate of syslog messages directed at the server. If you intend to use the RME syslog analyzer function you may want to dedicate a server to RME.

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 the [High Availability Installation Guide for Cisco Security Manager 3.1](#).

VMware Deployments

Security Manager supports running in VMware ESX Server 3.5 beginning with Security Manager 3.2.1. 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 3.5 introduces a modest amount of application performance degradation which varies based on the size of the reference network involved and the specific test case. In a few test cases the performance actually improved, but this was more the exception than the rule. One area where the performance degradation was unusually large was the case of performing a deployment to a PIX or ASA device with a large number of rules (on the order of 5 to 50 thousands rules). In this case the deployment took roughly twice as long.

You should allocate 4 GB of memory to the virtual machine you use with Security Manager for all reference network sizes. In general you should follow the best practices documented in the VMware document: [Performance Tuning Best Practices for ESX Server 3](#). However, you should avoid tuning any of the advanced VMware parameters, as the default values or settings are generally optimum.

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 3.5 on an Intel® Xeon® X5365 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).

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 3.1.1 and 3.2.1 on the same machine. It is possible, though, to run multiple instances of the client if you need to simultaneously access more than one Security Manager server. You can install and use the client on the server; however, this practice is suitable only for an SE size network and is not recommended for the larger ME or LE size networks.

As mentioned in [Factors which Affect Application Performance, page 6](#), it may be necessary to deploy the client on a terminal server located near to the server to maintain acceptable performance, in the event that end users are located a large distance from the server which introduces significant latency (for example, intercontinental distances).

Reference Networks

Application performance and server and client sizing recommendations are affected by the size and composition of the network under management. Application performance was characterized for three different reference network configurations: Small Enterprise (SE), Medium Enterprise (ME), and Large Enterprise (LE) and a corresponding server and client specification. The characteristics of the three reference networks are defined below.

These reference networks consist of a mixture of dedicated firewall devices (for example, PIX, FWSM), dedicated IPS devices (for example, IPS 4200 Series), and multi-service (firewall, VPN, and IPS) routers. You should understand the following when you compare these reference networks to the makeup of your own network.

- In general you can equate like types of devices. For example, if the reference network refers to a PIX 535, this is comparable to similar devices such as other PIX models or the ASA 5500 Series with a similar number of rules defined. Likewise an IDS 4250 Sensor is comparable to similar IPS devices such as the AIP-SSM or IPS AIM. Finally a Cisco 2801 router is comparable to other IOS-based routers.
- In general you cannot add additional devices to one category (for example, firewall appliances) by not using devices of another category (for example, IPS appliances). So for example, even if you do not use IPS devices, if you add additional PIX devices beyond the specified number it will increase the load on the server beyond what has been tested for that particular reference network.
- In general Security Manager does not have any fixed scalability limitations. For example, we do not impose any fixed limit on the number of devices you can add of any type (assuming you have sufficient licenses) or on the number of policy objects of a given type. However, exceeding the limits identified in these reference networks would place you in an untested, uncharacterized situation.

Small Enterprise Reference Network

The Small Enterprise Reference Network has the following makeup:

- 10 PIX 535s (vc1 - vc10)
 - PIX 7.0
 - 5 interfaces on each firewall: inside, outside, DMZ-slot0 ~ DMZ-slot2
 - 200 ACEs in each PIX Firewall rule table
- 50 Cisco 2801s (ios1 - ios50)
 - IOS 12.4
 - 2 interfaces on each router: FastEthernet0, FastEthernet1
 - 20 ACEs in each router rule table
 - IOS IPS Enabled
- 10 IDS 4250 Sensors
 - IPS 5.1
 - 4 virtual sensors per device (10 total virtual sensors)
- Full Mesh VPN
 - Technology: Regular IPsec VPN
 - Size: 3 routers (ios1 - ios3)
- 4,500 access-list rules
- 100 user-defined network objects, where each object contains a single IP entry. 50 of the network objects are referenced by an access-list rule.
- 25 user-defined service objects, where each object contains one service port and all 25 service-objects are referenced by an access-list rule.

The Small Enterprise (SE) Reference Network database file sizes were recorded as 2.396 MB for the Cmf.db and 54.932 MB for the Vms.db. These files are located under the \$NMSROOT\databases directory on the server.

Medium Enterprise Reference Network

The Medium Enterprise Reference Network has the following makeup:

- 21 PIX 535s (vc1 - vc21)
 - PIX 7.0
 - 5 interfaces on each firewall: inside, outside, DMZ-slot0 - DMZ-slot2
 - 500 ACEs in each PIX Firewall's rule table
- 2 FWSM
 - FWSM 2.3
 - 3 interfaces on each FWSM: inside, outside, DMZ1
 - 20 ACEs in its rule table
- 100 Cisco 2801 (ios1 - ios100)
 - IOS 12.4
 - 4 interfaces on each router: FastEthernet0 - FastEthernet3
 - 50 ACEs in each router's rule table
 - IOS IPS Enabled
- 15 IDS 4250 Sensors
 - IPS 5.1
 - 4 virtual sensors per device (60 total virtual sensors)
- Hub and Spoke VPN
 - Technology: Regular IPsec VPN
 - Size: 1 hub (vc1), 20 spokes (vc2 - vc21)
- 44,000 access-list rules
- 650 user-defined network objects, where each object contains a single IP entry. 150 of the network objects are referenced by an access-list rule.
- 75 user-defined service objects, where each object contains one service port and all 75 service-objects are referenced by an access-list rule.

The Medium Enterprise (ME) Reference Network database file sizes were recorded as 2.396 MB for the Cmf.db file and 63.644 MB for the Vms.db. These files are located under the \$NMSROOT\databases directory on the server.

Large Enterprise Reference Network

The Large Enterprise Reference Network has the following makeup:

- 1000 PIX 535s (vc1 - vc1000)
 - PIX 7.0

- 10 interfaces on each firewall: inside, outside, DMZ-slot1- DMZ-slot8
- 2,000 ACEs in each PIX Firewall's rule table
- 48 FWSM
 - FWSM 2.3
 - 3 interfaces on each FWSM: inside, outside, DMZ1
 - 50,000 ACEs in its rule table
- 5100 Cisco 2801 (ios1 - ios5100)
 - IOS 12.4
 - 6 interfaces on each router: FastEthernet0 - FastEthernet5
 - 300 ACEs in each router rule table
 - IOS IPS Enabled on 1000 routers
- 250 IDS 4250 Sensors
 - IPS 5.1
 - 4 virtual sensors per device (1,000 total virtual sensors)
- Layered VPN
 - Technology: Regular IPsec VPN
 - Full Mesh: ios1 - ios4
 - Hub and Spoke #1: ios1 > ios5 - ios1254 (1250 spokes)
 - Hub and Spoke #2: ios2 > ios1255 - ios2504 (1250 spokes)
 - Hub and Spoke #3: ios3 > ios2505 -ios3754 (1250 spokes)
 - Hub and Spoke #4: ios4 > ios3755 - ios5004 (1250 spokes)
- 3,000,000 access-list rules total
- 400,000 access-list rules on a single device
- 5000 user-defined network objects, where each object contains a single IP entry. 50 of the network objects are referenced by an access-list rule.
- 500 user-defined service objects, where each object contains one service port and all 25 service-objects are referenced by an access-list rule.

The Large Enterprise (LE) Reference Network database file sizes were recorded as 2.396 MB for the Cmf.db and 755.588 MB for the Vms.db. These files are located under the \$NMSROOT\databases directory on the server.

Number of Simultaneous Users

Security Manager supports multiple concurrent user sessions and has been specifically tested for 30 simultaneous users where:

- 10 users perform Read-Only actions: view activities/policies/jobs
- 10 users perform Read-Write actions: create activities, modify policies, and submit activities
- 10 users commit jobs and deploy actions

Server and Client Hardware Recommendations

This section provides recommendations for the server and client hardware sizing based on the three reference network configurations.

Server Sizing

[Table 1](#) provides basic recommendations on server sizing for Security Manager 3.2.x based on the reference networks.

Table 1 Server Sizing based on Reference Network

	Small Enterprise (SE)	Medium Enterprise (ME)	Large Enterprise (LE)
CPU	One CPU @ 2.x GHz	One CPU @ 3.x GHz	Two CPUs @ 3.x GHz
Memory	2 GB	4 GB	4 GB
Free Disk Space	20 GB	20 GB	20 GB
Network Interface	100BaseT (100 Mbps) or faster	100BaseT (100 Mbps) or faster	100BaseT (100 Mbps) or faster
Media Drive	DVD	DVD	DVD

Security Manager has only been performance characterized on servers with single-core CPU(s). While adequate performance can be obtained using the server specifications noted in [Table 1](#) for the Small Enterprise and Medium Enterprise reference networks, test results show you can obtain improved performance by using the Large Enterprise server specification also for the Small Enterprise and Medium Enterprise reference networks. For example, performance improvements of 30 to 50 percent were seen when using the Larger Enterprise server specification for the Medium Enterprise performance test cases. Exceeding the server specifications for the Large Enterprise configuration such as by adding more CPUs or memory does not significantly improve performance.

Client Sizing

[Table 2](#) provides basic recommendations on client sizing for Security Manager based on the reference networks and assuming a single client running on the machine.

Table 2 Client Sizing Based on Reference Network

	Small Enterprise	Medium Enterprise	Large Enterprise
CPU	One CPU @ 2.x GHz	One CPU @ 2.x GHz	One CPUs @ 2.x GHz
Memory	1 GB	1 GB	2 GB
Free Disk Space	10 GB	10 GB	10 GB
Network Interface	100BaseT (100 Mbps) or faster	100BaseT (100 Mbps) or faster	100BaseT (100 Mbps) or faster

Security Manager Tuning

Security Manager includes several parameters that you can modify to tune the application performance.



Caution

You should only modify the parameters described in this chapter with consultation from Cisco TAC or the Security Manager product team.

Information is provided for tuning the following parameters:

- [Java Virtual Machine Heap Size, page 14](#)
- [Thread Counts, page 15](#)

Java Virtual Machine Heap Size

The Security Manager server-side Java Virtual Machines (JVMs) maximum heap size is set to 1 GB by default. You can increase the maximum heap size by modifying the `startbe.pl` file located in the `$NMSROOT\MDC\be\bin` directory. In the file, the maximum heap size is specified by the `Xmxvalue` argument. We recommend that you make a copy of the existing file before modifying it. After modifying the file you need to restart the daemon manager for the new maximum heap size to take effect.

The maximum heap size depends on the maximum address space per process, which is 2 GB for Windows 32-bit operating systems. Maximum heap space is always smaller than maximum address space per process, because the process also needs space for stack, libraries, and so on. You may need to experiment to find the maximum heap size your server permits. If you exceed the limit you will get an error message as follows:

```
Error occurred during initialization of VM
Could not reserve enough space for object heap
Could not create the Java virtual machine
```

The following shows the contents of the `startbe.pl` file modified to increase the maximum heap size to 1.5 GB (`Xmx1536m`).

```
use CRM;
use lib "$ENV{NMSROOT}/lib/perl/install";
use InstallUtility;
require "$ENV{NMSROOT}/MDC/be/bin/be-env.pl";

sub startBe {
    print "    startBe() Starts\n" if ($debug);

    my $ARGS="--server -Xmx1536m -Xnoclassgc -cw:verbose -cw:jre $BE_JRE -cp:p $BE_CP -wd
$BE_WD com.cisco.nm.vms.be.BEMain";

    # my $cmd= "$PDREG -r VmsBackendServer -e $BE_JAVA -d \"Tomcat,CmfDbEngine,ESS\"";
    # my $cmd= "$PDREG -r VmsBackendServer -e $BE_CW_JAVA -d \"Tomcat,CmfDbEngine,ESS\"";
    my $cmd= "$BE_CW_JAVA ".$ARGS."";

    print "cmdline => $cmd " if (debug);
    my $rc = system($cmd);
    if ($rc != 0) {
        $errMsg = "Failed to start BE Server.";
        print "$errMsg \n";
    }
    print "    startBe() Ends\n" if ($debug);
}
}
```

```

$debug=0;

initParams();
startBe();

print "\n   LogFile is $logfile\n" if ($debug);

```

Thread Counts

A number of Security Manager backend processes perform multiple tasks in parallel (that is, are multithreaded). You can tune two specific thread count parameters to control the number of these tasks performed in parallel:

- `DistributionFramework.Worker.Max.ThreadCount.JobGroup`
This parameter controls the maximum number of devices that Security Manager deploys to in parallel for non-signature related updates. The default value is 20.
- `DistributionFramework.Max.ThreadCount.SpecialThreadPool.SigUpdate`
This parameter controls the maximum number of devices that Security Manager deploys to in parallel for signature related updates. The default value is 60.

You can modify these parameters in the `taskmgr.prop` file located in the `$NMSROOT\MDC\athena\config` directory.

Increasing these values can reduce the amount of time it takes to complete deployment to a larger number of devices. However, increasing the value too much can result in an out-of-memory condition.

Some other default values for Security Manager are the following:

- Default concurrent number of devices to discover (20)
- Default current FWSM security contexts to deploy if via the system context (5)
- Heap size of the Tomcat process (128M min, 1024M max)
- Heap size of the backend process (128M min, 1024M max).

Summary of Security Manager Scalability

[Table 3](#) summarizes the basic aspects of Security Manager scalability based on tested configurations. Security Manager does not have any hard-coded scalability limitations.

Table 3 **Summary of Security Manager Scalability**

Attribute	Maximum Value
Devices in Inventory	6,400
Devices in a single Deployment Job	1,250
Host/network Policy Objects	5,000
Service Objects	500
Access-list Rules Total	3,000,000
Access-list Rules on a Single Device	400,000

Attribute	Maximum Value
Nodes in a Single VPN Topology	1250
Simultaneous Users	20 read/write + 10 read-only