

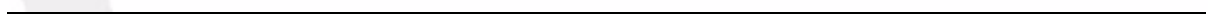
INSTALLER'S GUIDE

NetScreen-Security Manager 2004

Version 2004

P/N 093-0908-000

Rev. B



Copyright Notice

Copyright © 2004 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

This product includes software developed by SSHTools (<http://www.sshtools.com/>).

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in

which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contents

Preface	v
Organization	vi
NetScreen Publications	vii
Chapter 1 Introduction	1
Installation Process Overview	2
Management System Install Process	2
User Interface Install Process.....	2
Installation Package	3
Technical Overview	4
About the Management System.....	4
GUI Server	5
Device Server	5
About the Security Manager User Interface (UI).....	6
About Managed FW/VPN Devices	6
Communications	7
Communication Ports and Protocols	7
Configuration Options	10
Typical Configuration	10
Extended Configuration	11
Minimum System Requirements	12
System Requirements - Management System	12
System Requirements - User Interface.....	13
Sizing and Capacity Planning	14
Memory	14
Processor Requirements	14
Disk Storage.....	14
Network Bandwidth.....	15
Hardening Your System.....	15
Firewall Protection	15
Dedicating the System	15
Securing Communications	16
Installing Updates and Security Patches	16
Next Steps	17
Chapter 2 Typical Configuration	19
Installing the Management System, Typical Configuration	20
Defining System Parameters	21
Prerequisite Steps	22

- Upgrading the RPM Package (For Linux Users Only)22
- Installing the Management System Software 24
 - Validating Management System Status 28
 - Viewing the Installation Log 29
- Installing the User Interface 30
 - Viewing the Installation Log 32
 - Running the User Interface 32
 - Troubleshooting Tips 33
- Validating the Installation 34
 - Running the UI in Demo Mode..... 35
- Next Steps 36
- Chapter 3 Extended Configuration 37**
 - Installing the Management System, Extended Configuration 38
 - Defining System Parameters 39
 - Prerequisites 40
 - Installing the GUI Server 41
 - Viewing the Installation Log 44
 - Installing the User Interface 45
 - Adding the Device Server..... 45
 - Installing the Device Server 46
 - Transferring Certificate Files (optional) 50
 - Next Steps 51
- Chapter 4 Administration 53**
 - Controlling the Management System 54
 - Viewing Management System Commands 54
 - Starting the GUI Server 54
 - Starting the Device Server 55
 - Stopping the GUI Server..... 55
 - Stopping the Device Server 55
 - Maintaining the Management System 56
 - Changing the Management System IP Address 56
 - Changing the Device Server IP Address 56
 - Changing the GUI Server IP Address 57
 - Uninstalling the Management System 57
 - Installing a TFTP Server 58
 - Installing a TFTP Server on Linux 58
 - Installing a TFTP Server on Solaris 59
 - Uninstalling the User Interface 60
- Index..... ix**

Preface

Thank you for choosing NetScreen-Security Manager 2004, the integrated management software for all NetScreen FW/VPN devices and systems.

This *NetScreen-Security Manager 2004 Installer's Guide* describes how you can install an initial working Security Manager system. This Installer's Guide is intended primarily for IT administrators who are responsible for installing Security Manager for the first time.

Note: *If you are currently using a previous version of NetScreen management software (i.e., NetScreen-Global PRO or NetScreen-Global PRO Express) refer to the NetScreen-Security Manager 2004 Migration and Installer's Guide for more specific information.*

ORGANIZATION

This manual contains the following four chapters:

- [Chapter 1, “Introduction”](#) describes the concepts behind the two main software components that you need to install and run Security Manager—the management system and User Interface (UI). It discusses the installation process, minimum hardware and software requirements, and options for implementing components of the management system to provide for enhanced scalability and performance. This chapter also discusses considerations for hardware sizing and capacity planning. This information is provided to help you design and implement a management system that is appropriate for your network.
- [Chapter 2, “Typical Configuration”](#) describes specifically how to install the Security Manager management system for most typical cases—GUI Server and Device Server on the same server. It describes how to install and configure the required software for both management system components (GUI Server, Device Server) together on the same server. This chapter also describes procedures for manually controlling (starting and stopping) the management system.
- [Chapter 3, “Extended Configuration”](#) describes specifically how to install the Security Manager management system for enhanced scalability and performance—with the GUI Server and Device Server installed on separate servers.
- [Chapter 4, “Administration”](#) describes how to maintain and uninstall the management system and UI.

NETSCREEN PUBLICATIONS

To obtain technical documentation for any NetScreen product, visit:

www.netscreen.com/resources/manuals/.

To obtain the latest software version, visit: www.netscreen.com/services/download_soft. Select a category of software product from the dropdown list, then follow the displayed instructions. (You must be a registered user to download NetScreen software.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs@netscreen.com

Introduction

In This Chapter

- [Installation Process Overview](#)
- [Installation Package](#)
- [Technical Overview](#)
- [Configuration Options](#)
- [Minimum System Requirements](#)
- [Sizing and Capacity Planning](#)
- [Next Steps](#)

This chapter provides you with the information you need to plan how best to install Security Manager and integrate it into your network. It provides an overview of the Security Manager installation process. It introduces and describes the components of the Security Manager architecture—management system, user interface, and FW/VPN devices, as well as their roles in providing network management functionality.

This chapter also reviews options for configuring the management system to provide enhanced performance and scalability, minimum hardware and software requirements, and hardware sizing and capacity planning considerations.

INSTALLATION PROCESS OVERVIEW

NetScreen-Security Manager is software that enables you to integrate and centralize management of your NetScreen security environment.

There are two main software components that you need to install and run Security Manager: the Security Manager management system and the Security Manager User Interface (UI).

The overall process for installing Security Manager is as follows:

- [“Management System Install Process” on page 2](#)
- [“User Interface Install Process” on page 2](#)

Management System Install Process

The management system installer enables you to install all the software required to run each component of the Security Manager management system. Refer to [“Technical Overview” on page 4](#) for more information on the Security Manager management system.

The management system installer is a shell archive script that you can run on any dedicated, secure and trusted Red Hat Linux 8 or 9 or Solaris 8 or 9 server that meets minimum system requirements. Refer to [“Minimum System Requirements” on page 12](#) for more information on the minimum required hardware and software that you need to install the Security Manager management system.

There are separate installer scripts for both Linux and Solaris installations. When you launch the management system installer, the script guides you through all the steps required to install and configure each management system component.

User Interface Install Process

The Security Manager User Interface installer launches an InstallAnywhere wizard that you can run on any Windows-based computer that meets minimum system requirements. Refer to [“Minimum System Requirements” on page 12](#) for more information on the minimum required hardware and software that you need to install the Security Manager User Interface.

The InstallAnywhere wizard guides you through all the steps required to configure and install the User Interface. Once you install the User Interface, you can connect it to the management system.

INSTALLATION PACKAGE

All of the software files required to install Security Manager are located on the Security Manager installation CD or on the Internet at the NetScreen corporate support Web site. It is recommended that you download these files to the computers on which you plan to install Security Manager before beginning the installation process.

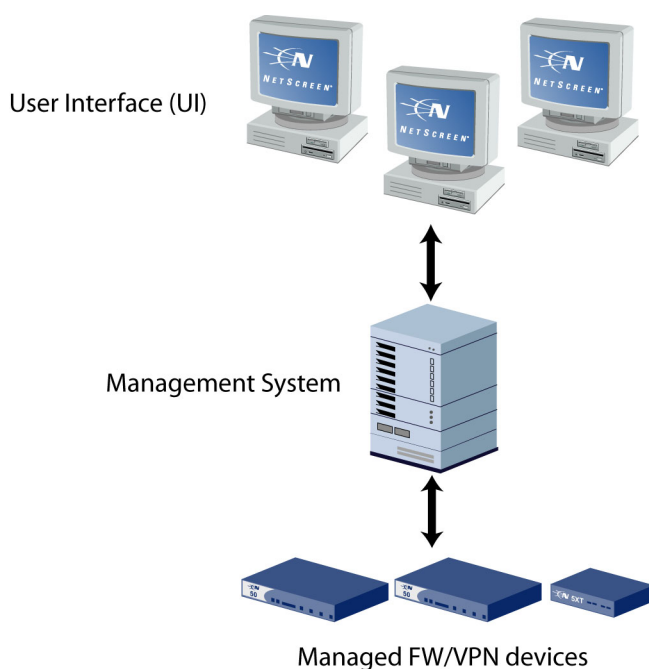
The following table describes the contents of the Security Manager installation CD.

File Name	Description
nsm2004_ui_win_x86.exe	Installer for the Security Manager UI.
nsm2004_servers_linux_x86.sh	Installer for the Security Manager management system for Linux
nsm2004_servers_sol_sparc.sh	Installer for the Security Manager management system for Solaris
nsm2004_gpexport_sol_sparc.sh	Installer for the Global PRO data export utility used to migrate data from Global PRO Express/Global PRO into Security Manager. You use this file only if you plan to migrate configuration data from Global PRO or Global PRO Express. If so, refer to the <i>NetScreen-Security Manager 2004 Migration and Installer's Guide</i> for more specific information.
system_update_linux_x86.tar	Linux system update utility. If you are installing on Linux, you use this file to update your RPM package for the version of Linux that you are using.

TECHNICAL OVERVIEW

The Security Manager management architecture is designed to provide optimum security, scalability, and flexibility for integrating with your specific network security environment. It includes the following key components:

- Management System
- User Interface (UI)
- Managed FW/VPN devices



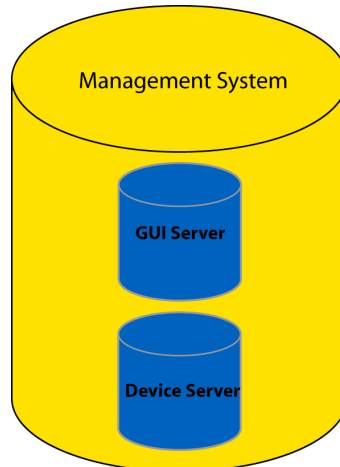
About the Management System

The management system used in Security Manager provides all the functionality required to integrate management of all the components in your network security environment. It enables you to centrally gather, store, configure, manage, monitor and generate reports on the FW/VPN devices you have deployed in your network.

The management system itself is composed of two distinct components:

- GUI Server
- Device Server

Both the GUI Server and Device Server working together are collectively referred to as the Security Manager “management system”.



You can install both components of the management system on the same physical server or on separate servers. By separating the two server components, you can improve system performance. Refer to “[Extended Configuration](#)” on page 11 later in this chapter for more information on configuring the management system on separate servers.

GUI Server

The GUI Server receives and responds to requests and commands from the Security Manager User Interface. It manages all the system resources and configuration data required to manage your network. It also contains a local data store where information about your managed FW/VPN devices, administrators, and configurations are centralized.

Note: The GUI Server can accommodate no more than 20 User Interfaces connected to it at any time. This is the maximum number of UI clients supported in this release of Security Manager.

Device Server

The Device Server acts as a collection point for all data generated by each FW/VPN device managed in your network. The Device Server stores this data, primarily traffic logs generated by the device, in a local data store.

Note: The Device Server can accommodate no more than 1000 FW/VPN devices connected to it at any time. This is the maximum number of FW/VPN devices supported in this release of Security Manager.

About the Security Manager User Interface (UI)

The Security Manager User Interface (UI) is a java-based software application that you use to access and configure data about your network on the management system. Once you have installed the UI, you can launch it and connect it to the management system. From the UI, you can view, configure, and manage your network from a single, central administrative location. Refer to the *NetScreen-Security Manager 2004 Administrator's Guide* or the *Online Help* included in the UI for more information about the Security Manager UI.

About Managed FW/VPN Devices

The managed FW/VPN devices that you have implemented in your network are the lowest tier of the Security Manager management architecture. All of the information about your network security environment originates from the devices that you have installed in your network.

The following table details the FW/VPN devices and versions of ScreenOS supported by Security Manager.

FW/VPN Device	ScreenOS Versions Supported
NS5XP	4.0.0, 4.0.1, 4.0.3, 5.0
NS5XT	4.0.0, 4.0.0-DIAL2, 4.0.1, 4.0.3, 5.0
NS5GT	4.0.0-DIAL2, 5.0 only
NS25	4.0.0, 4.0.1, 4.0.3, 5.0
NS50	4.0.0, 4.0.1, 4.0.3, 5.0
NS100	4.0.0, 4.0.1, 4.0.3, 5.0
NS204	4.0.0, 4.0.1, 4.0.3, 5.0
NS208	4.0.0, 4.0.1, 4.0.3, 5.0
NS500	4.0.0, 4.0.1, 4.0.3, 5.0
NS5200/8	4.0.0, 4.0.1, 4.0.3, 5.0
NS5200/24	4.0.1-SBR, 5.0
NS5400	4.0.1-SBR, 5.0
NS-HSC	5.0 only

You need to enable each FW/VPN device to communicate and work with Security Manager. Refer to the *ScreenOS 5.0 Concepts and Examples Guide* for more information describing how to enable management on your FW/VPN devices.

Once enabled, each FW/VPN device communicates and sends information to the Security Manager management system. From Security Manager, you can centralize all configuration data, and manage the network from a single, central, administrative location. You can then implement your security policies by “pushing” or sending configuration updates back to your devices.

Based on the configuration policies you define in Security Manager, the managed NetScreen FW/VPN devices provide the firewall and VPN services required to secure your network environment.

Communications

As you plan your installation, it helps to understand how Security Manager establishes communication between the User Interface, Management System, and FW/VPN devices.

Communication Ports and Protocols

For optimum security, the number of total ports on the GUI Server and Device Server is kept to a minimum:

- There is only one open port on the GUI Server—an inbound TCP port that listens for incoming connection requests from the UI(s) and Device Server (if installed on a separate system than the GUI Server).

***Note:** If both the GUI Server and Device Server are installed on the same system, both server components communicate directly with one another via inter-process communication.*

- There are six ports on the Device Server: four inbound TCP ports supporting connection requests from existing FW/VPN devices; and two outbound TCP ports used to establish communication with FW/VPN devices running ScreenOS 4.0.X.

***Note:** FW/VPN devices running ScreenOS 4.x and earlier utilize the same communication protocols for communicating the NSM management system that were supported with NetScreen-Global PRO.*

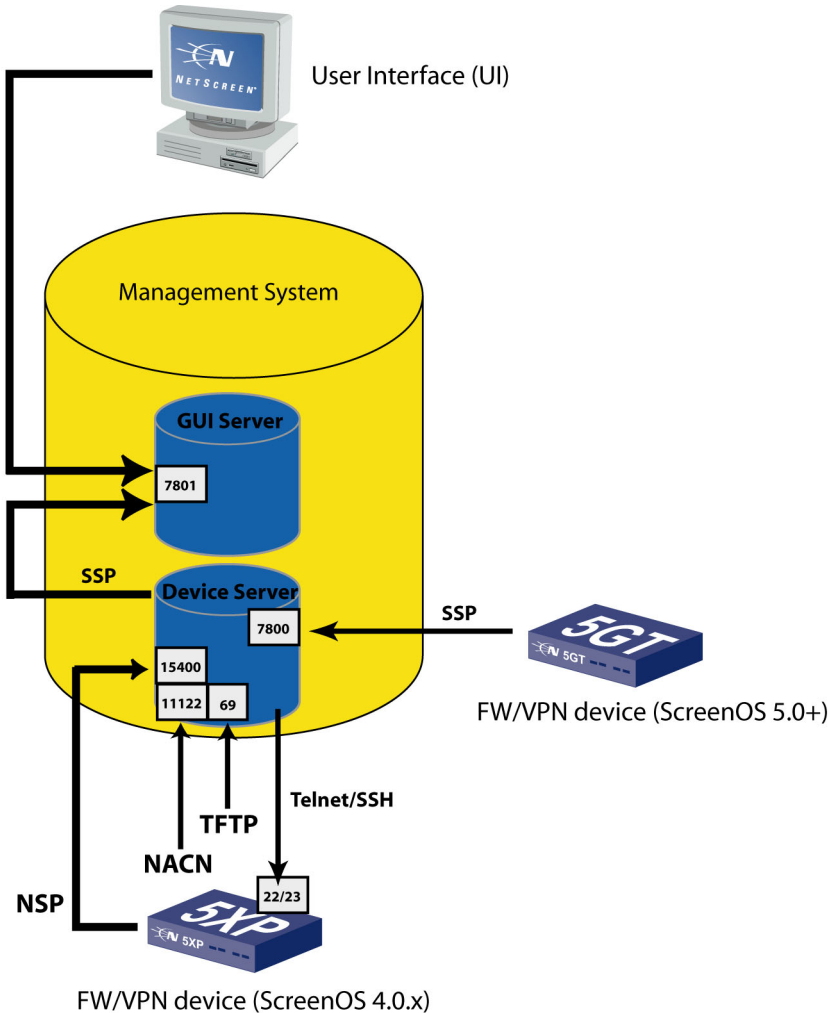
The following table summarizes the port that is open on the GUI Server.

Port	Protocol	Direction	Description
7801	TCP	INBOUND	<p>listens for incoming connection requests from the Security Manager UI(s) and Device Server. Used to establish communication session with Device Server and/or Security Manager UI(s).</p> <p>This communication session uses an encrypted form of TCP called Secure Server Protocol (SSP). SSP offers strong encryption and authentication mechanisms utilizing RSA public key cryptography, AES symmetric encryption, and HMAC-SHA-1 hashing, so management traffic is protected and kept confidential.</p> <p>This is also a duplexed connection enabling the UI and GUI Server to communicate back and forth to each other after the connection is established.</p>

The following table summarizes the ports that are open on the Device Server.

Port	Protocol	Direction	Description
7800	TCP	INBOUND	listens for incoming connection requests from FW/VPN device(s) running ScreenOS version 5.0+. Used to establish encrypted communication sessions with the GUI Server and FW/VPN devices (running ScreenOS v5.0+) . This communication session also uses SSP.
15400	TCP	INBOUND	listens for incoming NetScreen Server Protocol (NSP) connection requests from FW/VPN device(s) using ScreenOS 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS v4.0.x .
11122	TCP	INBOUND	listens for incoming NACN connection requests from FW/VPN device(s) using ScreenOS v4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS v4.0.x .
69	TCP	INBOUND	listens for incoming TFTP connection requests from FW/VPN device(s) using ScreenOS v4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS v4.0.x .
22/23	TCP	OUTBOUND	sends outbound Telnet/SSH connection requests to FW/VPN device(s) using ScreenOS v4.0.x. Used to establish communication sessions with FW/VPN devices running ScreenOS v4.0.x .

Since some of these protocols (i.e., TCP port 15400 and TFTP) are not encrypted or authenticated, an IPSEC tunnel between the management system and FW/VPN devices running ScreenOS 4.x and earlier is strongly recommended to secure the data transfer.



CONFIGURATION OPTIONS

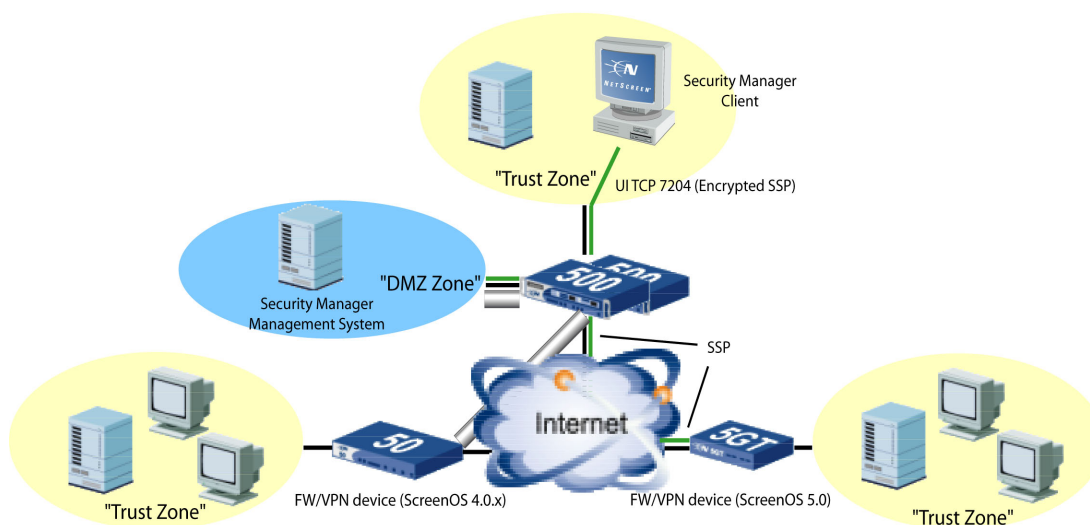
You can design and implement Security Manager to scale to small, medium, and large enterprises, as well as service provider deployments. There are two main options for configuring Security Manager:

- “Typical Configuration” on page 10
- “Extended Configuration” on page 11

Note: *NetScreen-Security Manager 2004 provides support for only one GUI Server and one Device Server. In future releases of Security Manager, you will be able to install and deploy multiple Device Servers in your network to provide greater scalability and performance. You will also be able to configure the management system for high availability.*

Typical Configuration

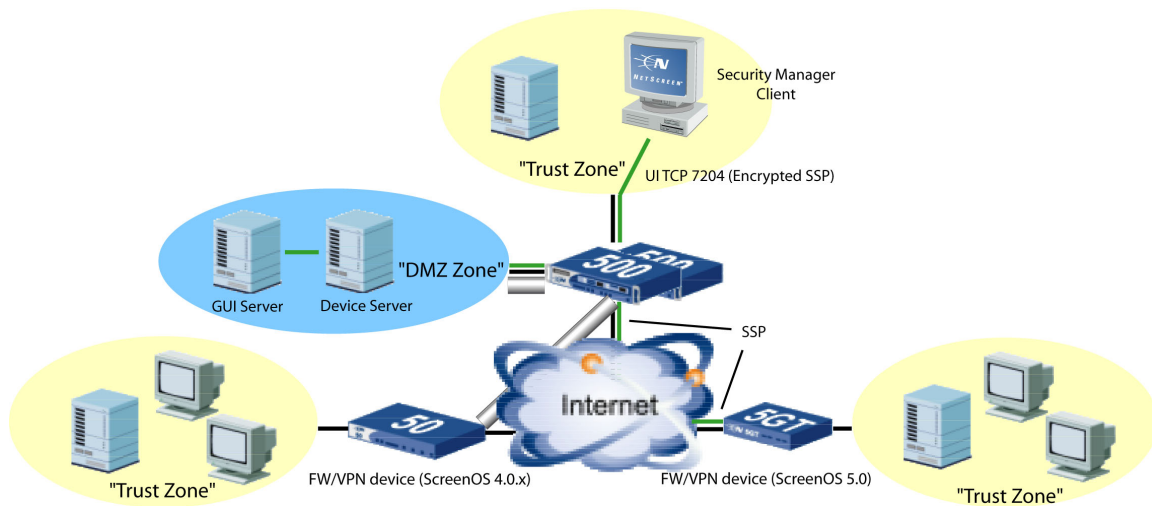
The most straightforward implementation of the Security Manager management system is to install both components of the management system (GUI Server and Device Server) on the same server. This configuration is appropriate for most typical small to medium-sized enterprises.



Extended Configuration

For larger enterprises, specifically where you expect to generate and store an inordinate amount of traffic logs, it is recommended that you install the GUI Server and Device Server on separate servers.

Note: You must install and run both servers on the same platform. NetScreen-Security Manager 2004 does not support the GUI Server and Device Server running on different platforms. For example, you cannot install the GUI Server on a system running Solaris, and the Device Server on a system running Linux.



MINIMUM SYSTEM REQUIREMENTS

The following minimum hardware and software requirements must be met to properly install and run Security Manager.

System Requirements - Management System

The following table describes the minimum requirements that must be met for the GUI Server and Device Server:

Component	Minimum Requirements
GUI Server and Device Server on the same server	<p>Solaris 8 or 9 operating system, OR Linux Red Hat 8.0 or 9.0</p> <p>CPU: Sun Microsystems UltraSPARC III 500MHz (or higher), OR Linux 1GHz processor (or higher)</p> <p>RAM: 512 MB (or higher); 2GB+ (depending on the number of managed devices and config size)</p> <p>Swap Space: 4 GB for both GUI Server and Device Server</p> <p>Storage: IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)</p> <p>Network Connection: 10/100Mbps NIC Ethernet adapter</p> <p>Server must be dedicated to running Security Manager only.</p>
GUI Server and Device Server on separate servers	<p>Solaris 8 or 9 operating system, OR Linux RedHat 8 or 9</p> <p>NOTE: Both servers must be installed and run on the same platform. For example, you cannot install the GUI Server on a system running Solaris, and the Device Server on a system running Linux.</p> <p>CPU: Sun Microsystems UltraSPARC III 500MHz (or higher), OR Linux 1GHz processor (or higher)</p> <p>RAM: 512MB (or higher); 1GB (recommended)</p> <p>Swap Space: 2 GB for the GUI Server, 2 GB for the Device Server</p> <p>Storage: IDE Hard Disk Drive with 10K rpm (minimum) - 15K rpm (recommended); 18 GB disk space (minimum) - 40 GB disk space (recommended)</p> <p>Network Connection: 10/100Mbps NIC Ethernet adapter</p> <p>I/O: Split backplane (recommended for Device Server)</p> <p>Each server must be dedicated to running Security Manager only.</p>

Note that you may extend system performance and data capacity by expanding on the minimum requirements specified for each component. Refer to [“Sizing and Capacity Planning” on page 14](#) for more information.

System Requirements - User Interface

The following table describes the minimum system requirements that must be met for the User Interface:

Component	Minimum Requirements
User Interface - Software	Microsoft Windows XP, OR Microsoft Windows NT [®] Workstation/Server 4.0, Service Pack 6a or higher, OR Microsoft Windows 2000 Server, Advanced Server, or Professional editions US English versions only
User Interface - Hardware	IBM [®] compatible PC 400MHz Pentium [®] II or equivalent (minimum); 700 MHz Pentium II or equivalent (recommended) RAM: 256 MB (minimum); 512 MB or above (recommended) 384kbps (DSL) or LAN connection - minimum bandwidth required to connect to the Security Manager management system.

SIZING AND CAPACITY PLANNING

As you plan to implement Security Manager in your network, you will want to consider issues specific to your network (i.e., sizing, memory or capacity) that may influence the hardware you choose to install on. The following guidelines are provided to help you size your hardware to accommodate specific network requirements.

Key hardware components that are affected by specific usage requirements include:

- [“Memory” on page 14](#)
- [“Processor Requirements” on page 14](#)
- [“Disk Storage” on page 14](#)
- [“Network Bandwidth” on page 15](#)

Memory

Log viewing, querying and investigating, as well as importing device configurations are all activities that increase the overall memory requirements for your management system. The number of devices and the complexity of their configurations also contributes to overall memory requirements. If you anticipate keeping a large amount of data available (online), it is highly recommended that you add additional memory to your system.

Processor Requirements

Security Manager is a multi-process, multi-threaded environment. The more processing power provided the better.

Disk Storage

The requirement for disk storage on the management system is largely determined by the amount of traffic logs that you are expected to generate, as well as those that you are required to record on a daily basis.

Traffic logs are stored on the Device Server in separate files, each covering a 24 hour time period. Each log on average is typically **100 bytes or less** in size. Each daily log file varies in size depending on the total number of logs that you receive. The exact number of days you can store depends on the total size of these files.

You can store as many logs as you have chosen to provide disk space for. Once the disk space allocated for logs on the Device Server is used, the system begins deleting the oldest logs currently stored on the system.

Configuration data is stored on the GUI Server. This information is not expected to exceed minimum system requirements for disk storage.

Network Bandwidth

Security Manager employs a symmetric key encryption algorithm that does not impact the size of data transported over the network. In most cases, a 56K connection is the minimum connection required for the User Interface to communicate with the Security Manager management system; and a 10/100Mbps Ethernet connection for communications between the Security Manager management system and your managed FW/VPN devices.

Hardening Your System

Since Security Manager is a software-only product, it is highly recommended that you take all the necessary precautions to reduce any hardware security vulnerabilities.

Refer to documentation relevant to the platform on which you are installing Security Manager (e.g., Bastille Linux project, Sun BluePrints, the Linux Administrators' Security Guide, YASSP or [ww.openssh.com](http://www.openssh.com)) for more specific information describing how to harden your system.

The following guidelines are provided as general recommendations for improving your hardware security.

- [“Firewall Protection” on page 15](#)
- [“Dedicating the System” on page 15](#)
- [“Securing Communications” on page 16](#)
- [“Installing Updates and Security Patches” on page 16](#)

Firewall Protection

It is recommended that you implement a layered approach to system security.

The first layer of protection for your Security Manager system is the network firewall. As you plan to deploy Security Manager, it is highly recommended that you place the management system behind a network firewall.

If you are implementing Security Manager components behind a firewall, you must create a security rule permitting traffic through all management system communication ports. Refer to [“Communications” on page 7](#) for more information on the management system's communication ports.

Dedicating the System

The management system computer should run only those components required for Security Manager.

It is recommended that you remove all unnecessary components and services. For example, if you do not need e-mail on the management system, turn SMTP off. If you do not need DNS server functionality, you can turn DNS off. If not set, you can turn telnet off.

Securing Communications

The management system server should not listen on any ports except those used by Security Manager for management. It is also recommended that you create security policies governing the use of the management system server.

Installing Updates and Security Patches

It is highly recommended that you install all the latest manufacturer-supplied updates and security patches.

NEXT STEPS

This chapter has provided you with the following:

- An overview of the Security Manager installation process
- An overview of the Security Manager architecture
- The role of the Security Manager management system and User Interface in providing network management functionality
- Options for implementing components of the Security Manager management system to provide for enhanced performance and scalability
- Minimum system requirements to help you identify the appropriate hardware and software to install and run Security Manager
- Considerations for hardware sizing and capacity planning

You should use this information to plan how best to implement Security Manager and integrate it into your network. When you are ready to install Security Manager, there are two options for configuring the management system depending upon the size and requirements of your specific network:

- Refer to [Chapter 2, “Typical Configuration”](#) for specific information describing how to install and run the management system for most typical cases, that is, on the same server.
- Refer to [Chapter 3, “Extended Configuration”](#) for specific information describing how to install and run the GUI Server and Device Server on separate servers. This configuration option enables you to extend performance and scalability for large enterprises.

Refer to [Chapter 4, “Administration”](#) for specific information describing how to maintain and uninstall the management system and UI.

Typical Configuration

In This Chapter

- [Installing the Management System, Typical Configuration](#)
- [Defining System Parameters](#)
- [Prerequisite Steps](#)
- [Installing the Management System Software](#)
- [Installing the User Interface](#)
- [Validating the Installation](#)
- [Next Steps](#)

Once you have decided how you want to deploy Security Manager in your network, and you have identified and procured the appropriate hardware, you are ready to begin the installation process.

This chapter describes how to install the Security Manager management system for most typical cases—GUI Server and Device Server on the same system. This includes performing any prerequisite steps, running the management system installer, running the UI installer on your Windows client, and validating that you have installed the management system successfully.

INSTALLING THE MANAGEMENT SYSTEM, TYPICAL CONFIGURATION

The following table summarizes the process for installing Security Manager for most typical cases. It also provides an estimate of the overall amount of time that each step requires. The total expected time to complete the actual installation procedure is no longer than 30 minutes.

Step	Description	Estimated Time to Complete
1	Define system parameters that you need to provide during the installation process.	10 min.
2	Perform prerequisite steps. This includes creating the user that the Security Manager management service runs as, and optionally partitioning drives for the GUI Server and Device Server data directories.	10 min.
3	Download the management system and UI installer software from the Security Manager installation CD or the NetScreen corporate Web site.	10 min.
4	Run the management system installer on the system where you want to install the management system. Specify that you want to install both the GUI Server and Device Server. * If you are installing the GUI Server and Device Server on separate systems, refer to Chapter 3, "Extended Configuration" for more information.	5 min.
5	Install the User Interface.	2-3 min.
6	Launch the UI, and connect it to the management system.	2-3 min.
7	Validate that you have successfully installed the management system and UI.	2 min.

DEFINING SYSTEM PARAMETERS

During the installation process, you are required to configure common system parameters such as the location of the directories where you wish to store data for the GUI Server and Device Server. It is necessary that you define these system parameters before performing the management system installation.

The following table identifies the parameters that you need to identify:

Parameter	Description
Management IP address and port of the GUI Server	The IP address and port used by the running GUI Server are required to start the Device Server. The Device Server also needs this information enabling it to connect and communicate with the GUI Server.
GUI Server data directory	<p>Directory location where user data on the GUI Server is stored. By default, the installer stores data on the GUI Server in the following location:</p> <pre style="text-align: center;">/var/netscreen/GuiSvr/</pre> <p>Because the data on the GUI Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</p>
Device Server data directory	<p>Directory location where device data on the Device Server is stored. By default, the installer stores data on the Device Server in:</p> <pre style="text-align: center;">/var/netscreen/DevSvr/</pre> <p>Because the data on the Device Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</p>
Initial "super" user password	This is the password required to authenticate the initial user in the system. By default, the initial super user account receives all administrative privileges in the system.

PREREQUISITE STEPS

Before you install the management system, you need to perform the following prerequisite steps:

1. Ensure that the computer you install the management system on is connected to a serial console or monitor and keyboard.
2. Login to the computer as root. If you are already logged in as a user other than root, you may become root by typing the following command:

```
su -
```

At the password prompt, enter the root password for the computer.

3. Partition drives for sufficient disk space to accommodate your planned data requirements.
4. Create a normal user called “*nsm*”. Create a group called “*nsm*”, with the user *nsm* as the only member.

You can do this in Linux, by typing the following command:

```
useradd nsm
```

You can do this in Solaris, by typing the following commands:

```
groupadd nsm  
useradd -g nsm nsm
```

The GUI Server and Device Server processes run as this user by default. It is recommended that you restrict this user account, so that the servers run as a non-privileged user.

5. If you are installing the management system on Linux, verify that you are running the correct version of RPM for the version of Linux that you are using. You can verify that you are running the correct version of RPM by running the following command:

```
rpm -qi rpm
```

For **RedHat 8.0**, verify that you are running **version 4.1.1, release 1.8x**.

For **RedHat 9.0**, verify that you are running **version 4.2, release 1**.

If you are not running the correct version of RPM for the version of Linux that you are using, you must upgrade it before proceeding.

Upgrading the RPM Package (For Linux Users Only)

Use the Linux system update utility provided to upgrade to the correct version of RPM.

To upgrade your version of RPM:

1. Untar the Linux system update utility (the file is called `system_update_linux_x86.tar`) provided on the Security Manager Installation CD, or from the directory where it is saved, to a suitable directory on the server.

Note: *It is recommended that you untar the utility to the `/usr` subdirectory.*

You can do so by running the following command:

```
tar xvf /mnt/cdrom/system_update_linux-x86.tar /usr
```

2. Navigate to the resulting directory called “systemupdate”, where the update script is stored. You can do so by running the following command:

```
cd /usr/systemupdate
```

3. Execute the update script. You can do so by running the following command:

```
./update.sh
```

Let the script run to completion. This may take up to 20 minutes depending upon the number of packages that must be installed.

INSTALLING THE MANAGEMENT SYSTEM SOFTWARE

In most typical cases, you install both the GUI Server and Device Server on the same server. The management system installer is designed to guide you through all the steps to configure required system parameters, then run to completion.

To install the management system on a single system:

1. Load the management system installer software onto the server which you have decided to function as the Security Manager management system.

You can run the installer directly from the Security Manager installation CD. You can also copy the installer to a directory on the server, or you can download the installer from the NetScreen Customer Services Online Web site.

2. Navigate to the directory where you have saved the management system installer file.
3. Run the management system installer.

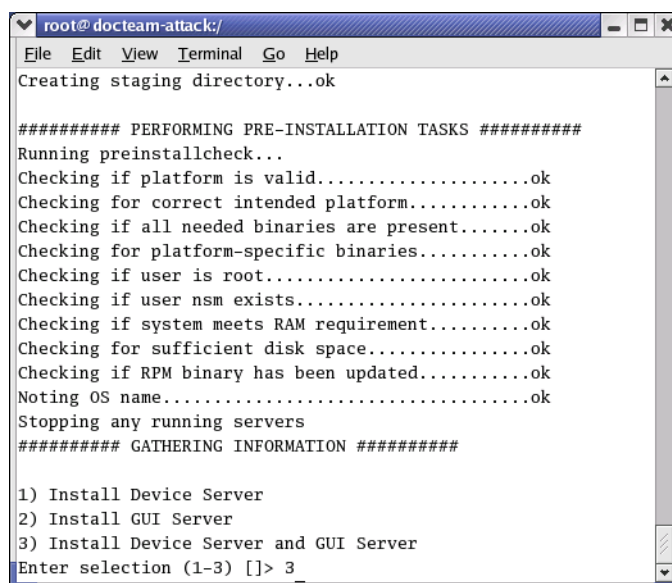
On Linux, you can run the management system installer using the following command:

```
sh nsm2004_servers_linux_x86.sh
```

On Solaris, you can run the management system installer using the following command:

```
sh nsm2004_servers_sol_sparc.sh
```

The installation begins automatically. The following graphic depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.



```
root@ docteam-attack:/
File Edit View Terminal Go Help
Creating staging directory...ok

##### PERFORMING PRE-INSTALLATION TASKS #####
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Checking if RPM binary has been updated.....ok
Noting OS name.....ok
Stopping any running servers
##### GATHERING INFORMATION #####

1) Install Device Server
2) Install GUI Server
3) Install Device Server and GUI Server
Enter selection (1-3) []> 3
```

It performs a series of pre-installation checks to ensure that:

- you are installing the correct software for your operating system
- all the needed software binaries are present
- you have correctly logged in as root
- the system has sufficient disk space and RAM

The installer then stops any running servers.

***Note:** The management system installer indicates the results of its specific tasks and checks:*

- **“Done”** indicates that the installer successfully performed a task.
- **“ok”** indicates that the installer performed a check, and verified that the condition was satisfied.
- **“FAILED”** indicates that the installer performed a task or check, but it was not successful.

The installer next prompts you to specify the components of the Security Manager management system that you wish to install.

***Note:** If you have installed a previous version of the management system, you may notice different menu options.*

4. Enter selection **3** to specify that you want to install the Device Server and GUI Server.

The script then prompts you to specify where you want to store the Device Server data files.

5. Enter the path for the directory that you want to store the data files for the Device Server or press **ENTER** to accept the default path (the default location is `/var/netscreen/DevSvr`).

***Note:** If you specify a new directory location, the installer creates it. The installer does not however, allow you to specify an existing directory location. This is to safeguard against over-writing any existing data. If you try to specify an existing directory, the installer indicates that an existing directory already exists, and prompt you to try again.*

The script prompts you to specify where you want to store the GUI Server data files.

6. Enter the path for the directory that you want to store the data files for the GUI Server, or press **ENTER** to accept the default path (the default location is `/var/netscreen/GuiSvr`).

The script next prompts you to specify the IP address of the Device Server.

7. Enter the management IP address for the server. This should be the same IP address of the server that you are installing on. The installer sets the IP address and port number on the GUI Server enabling the Device Server to connect. It attempts to connect to the GUI Server using port **7800** by default.

The script next prompts you to enter a password for the “super” user account. The initial administrator or “super” user account is the account that you use when you first login to Security Manager using the Security Manager UI.

This account is used to authenticate communication between the management system and the Security Manager UI. It possesses all administrative privileges by default.

8. Enter any text string for the password. Enter the password again for verification.


Note: Make a note of the password that you have set for the super user account. You need this when you first login to the UI.

The script next prompts you if you want to start both servers once it has completed installation.

9. Enter **y** and then press **ENTER** to start both servers once the installer has completed the installation process. Enter **n** and then press **ENTER**, if you do not want to start both servers.

Note: Whenever you restart your operating system, both the GUI Server and Device Server start automatically.

The script next prompts you to verify your installation configuration settings.



```
File Edit View Terminal Go Help
Enter the management IP address of this server [2.2.2.174]>

Setting GUI Server address and port to 2.2.2.174:7800 for Device Server

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Start server(s) when finished? (y/n) [n]> y

About to proceed with the following actions:
- Install Device Server
- Install GUI Server
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Use IP address 2.2.2.174 for management
- Connect to GUI Server at 2.2.2.174:7800
- Set password for 'super' user
- Start server(s) when finished: Yes

Are the above actions correct? (y/n)> y
```

10. Verify your settings, and if they are correct, enter **y** and then press **ENTER** to proceed. If you enter **n** and then press **ENTER**, the installer returns you to the original Selection prompt.

The installation proceeds automatically. The installer proceeds to perform the following actions:

- extract the software payloads
- perform migration tasks (disregard since this is a new installation)
- perform installation tasks such as installing the Device Server/GUI Server RPMs, creating the Device Server/GUI Server data directory, and setting correct permissions.

```
File Edit View Terminal Go Help
##### PERFORMING MIGRATION TASKS #####
##### PERFORMING INSTALLATION TASKS #####

----- INSTALLING Device Server -----
Looking for existing RPM package.....ok
Removing DevSvr files from default location.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in config file(s).....ok
Setting permissions for Device Server.....ok
Restarting xinetd service.....ok
Installation of Device Server complete.

----- INSTALLING GUI Server -----
Looking for existing RPM package.....ok
Removing GuiSvr files from default location.....ok
Installing GUI Server RPM.....ok
Installing JRE.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in config file(s).....ok
Setting permissions for GUI Server.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Installation of GUI Server complete.

----- SETTING START SCRIPTS -----
█
```

- perform post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server.

Several messages display to confirm the installation progress.

```
File Edit View Terminal Go Help
----- SETTING START SCRIPTS -----
Enabling Device Server start script.....ok
Enabling GUI Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
Running nacnCertGeneration.....ok
Removing staging directory.....ok
Starting GUI Server.....ok
Starting Device Server.....ok

NOTES:
- Installation log is stored in /tmp/netmgtInstallLog.20031202130108

- This is the GUI Server fingerprint:
  6E:E1:53:20:35:CC:41:D8:78:74:CE:C8:64:4C:0D:10:55:B4:01:BB
  You will need this for verification purposes when logging into the GUI
  Server. Please make a note of it.

[root@docteam-attack /]# █
```

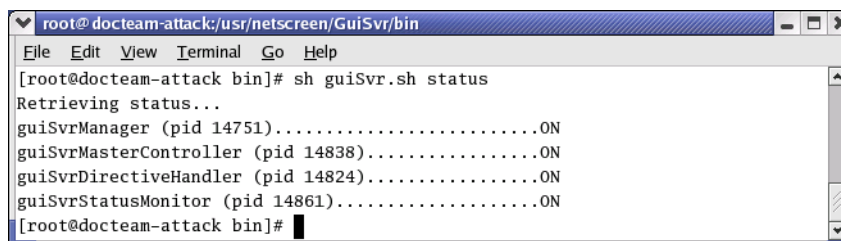
The installer runs for several minutes, and then exits.

Validating Management System Status

If you specified that you want the installer to start server(s) when finished, it is recommended that you view the status of the Device Server and GUI Server to confirm that all services are up and running.

To check the status of the GUI Server:

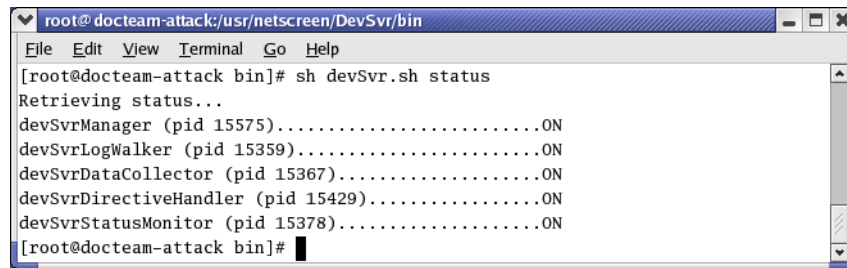
1. Navigate to the GUI Server bin subdirectory (i.e., /usr/netscreen/GuiSvr/bin).
2. Run the following command: `sh guiSvr.sh status`



```
root@ docteam-attack:/usr/netscreen/GuiSvr/bin
File Edit View Terminal Go Help
[root@docteam-attack bin]# sh guiSvr.sh status
Retrieving status...
guiSvrManager (pid 14751).....ON
guiSvrMasterController (pid 14838).....ON
guiSvrDirectiveHandler (pid 14824).....ON
guiSvrStatusMonitor (pid 14861).....ON
[root@docteam-attack bin]# █
```

To check the status of the Device Server:

1. Navigate to the Device Server bin subdirectory (i.e., `/usr/netscreen/DevSvr/bin`).
2. Run the following command: `sh devSvr.sh status`



```
root@docteam-attack:/usr/netscreen/DevSvr/bin
File Edit View Terminal Go Help
[root@docteam-attack bin]# sh devSvr.sh status
Retrieving status...
devSvrManager (pid 15575).....ON
devSvrLogWalker (pid 15359).....ON
devSvrDataCollector (pid 15367).....ON
devSvrDirectiveHandler (pid 15429).....ON
devSvrStatusMonitor (pid 15378).....ON
[root@docteam-attack bin]#
```

Refer to “[Controlling the Management System](#)” on page 54 for more information on manual commands that you can send to the Device Server and GUI Server.

Viewing the Installation Log

The installer generates a log file with the output of the installation commands for troubleshooting purposes. This file is saved by default in the `tmp` subdirectory.

The naming convention used for the installation log file is:
`netmgtInstallLog.<current date><current time>`

For example if you ran the installer on December 1, 2003 at 6:00pm, the installation log file would be named: `netmgtInstallLog.20031201180000`

Note: Once the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.

INSTALLING THE USER INTERFACE

The Security Manager User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows-based computer that meets minimum system requirements. Refer to [Chapter 1, “Introduction”](#) for more information on the minimum system requirements for the UI.

The InstallAnywhere wizard guides you through all the steps required to configure and install the Security Manager UI. Once you install the UI, you can connect it to the management system.

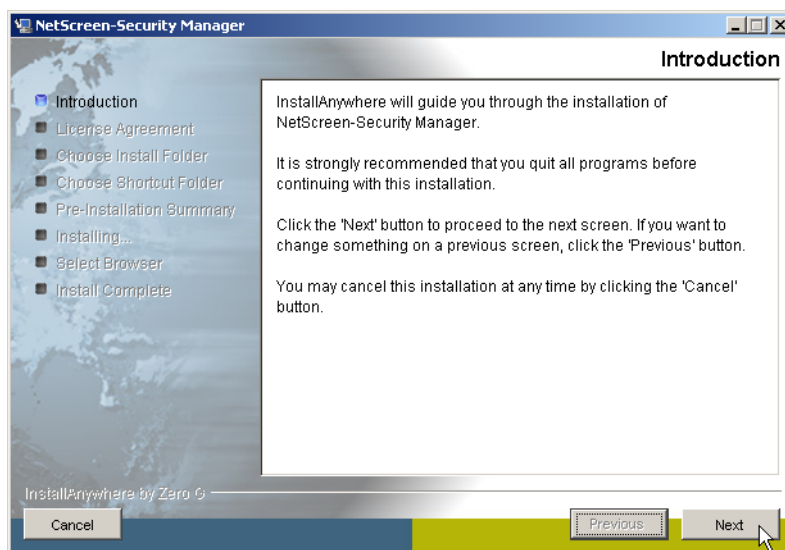
Note: *It is recommended that you quit all running applications before installing the UI.*

To install the Security Manager UI:

1. Login as an Administrator user on the computer where you are installing the UI.

Note: *For instructions on adding users to the Administrator group, please refer to your operating system manual.*

2. Download the UI installer (`nsm2004_ui_win_x86.exe`) from the Security Manager installation CD or the NetScreen corporate Web site to the computer where you are installing the UI.
3. Run the UI installer. An Introduction screen for the InstallAnywhere wizard appears.



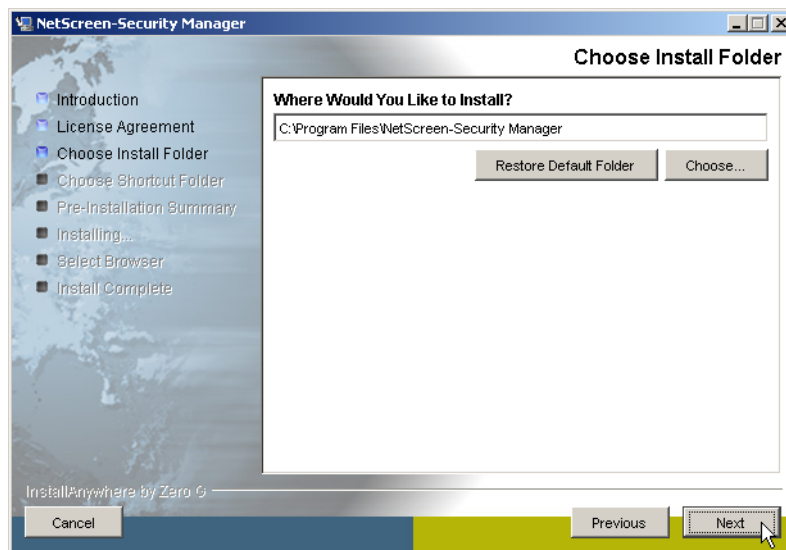
Follow the wizard through all the steps required to configure and install the UI.

4. Click **Next** to continue the installation. The License Agreement screen appears.

5. Review the License Agreement carefully. If you choose to accept the terms of the License Agreement, click the button next to the appropriate statement.

***Note:** If you choose to not accept the terms of the License Agreement, you will not be able to proceed with the installation.*

If you accepted the License Agreement, the Choose Install Folder screen appears.



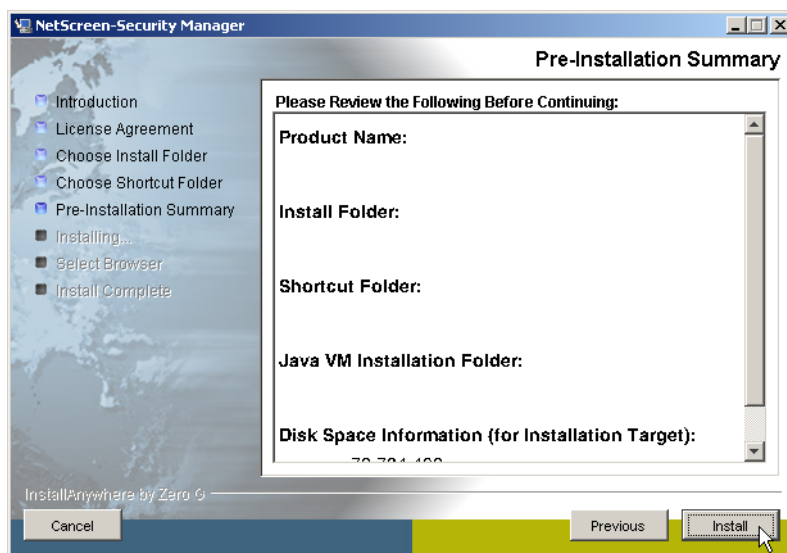
6. To accept the default install folder, click **Next**.

***Note:** The installer saves the UI software files in C:\Program Files\NetScreen-Security Manager by default.*

To specify a new or different folder location, click **Choose...** If you decide to accept the default install folder, you can click **Restore Default Folder**.

The Choose Shortcut Folder appears.

7. Select where you would like to create the Security Manager product icons. Click **Next** to continue. The Pre-Installation Summary screen appears.



8. Verify that the information is correct. To make a change to any of the previous configuration options, click **Previous**. When you are satisfied that the information is correct for this installation, click **Install**. The installer proceeds to install the software files for the UI.

When the installation is complete, a screen indicating “Install Complete” appears.

9. Click **Done** to exit the installation program.

Viewing the Installation Log

If for any reason, you cancelled the installation process, the installer generates a log file with information describing the context of the installation process. The installation log is saved by default in the following directory location:

```
C:\Documents and Settings\\Desktop
```

The Installation log file is named:

```
Security Manager_Prototype_InstallLog.xml
```

Running the User Interface

Once you have completed installing the UI, you can launch the application and verify that you can connect to the management system.

The first time you open the UI, you need to specify the host name (or IP address) of the management system that you want to connect to, a user name, and password. The default user name for new installations is “super”; the default password is the password you specified when configuring the management system. Passwords and user names are *case-sensitive*.

To log in to the UI for the first time:

1. Run the Security Manager UI (from the **Start** menu, select **NetScreen-Security Manager > NetScreen-Security Manager** or double-click the Security Manager icon on your desktop). The Login window appears.
2. Verify that the user name in the **Login** field provided is the initial admin user called “super”. If not, enter “super” in the Login field.
3. Enter the password that you specified when you installed the management system in the **Password** field provided.
4. Enter the IP address you assigned to the GUI Server in the **Server** field provided. If you have enabled DNS-lookup, you can enter the host name instead of the IP address.



5. Click **OK**.

The UI appears indicating that the installation was successful.

Troubleshooting Tips

The following are common reasons why you might be unsuccessful logging into the Security Manager management system from the User Interface:

- **Cannot Connect to the Security Manager Management System.** If you receive an error message indicating that the UI cannot connect to the Management System, try pinging the IP address of the management system to verify your network connection.
- **Password incorrect.** If you receive an error message indicating that you are using an invalid password, verify that the password that you are using, matches the password that was configured during installation.

VALIDATING THE INSTALLATION

Once you have installed the management system and UI, it is recommended that you validate basic information configured on the Device Server. You can use the Server Manager to view and edit your configuration on the management system.

To validate your configuration on the Device Server:

1. From the Security Manager UI, double-click the **Server Manager** module. The Server Manager module expands, and the Servers and Server Monitor appear.
2. Select the **Servers** node. The Servers view displays Device Server and GUI Server information.
3. Select the Device Server and click **Edit** or right-click the Device Server and click **Edit** to view all information available on the Device Server.

The screenshot shows the 'Device Server' configuration window. The 'Name' field is 'server_1' and the 'IP Address' is '2.2.2.174'. The 'Device Polling' tab is active, showing 'Device Server Manager Port' as 7800, a 'Set Password...' button for the GUI connection, and 'Device Server ID' as 1. A table under 'MIP' shows a mapping of 0.0.0.0 to port 7800. The 'General' tab is also visible but not active.

Mapped IP Address	Mapped Port
0.0.0.0	7800

4. Use the **General** tab to verify the following information:

- **Mapped IP address.** The IP address that is configured during installation.

***Note:** You can configure the Device Server to use a Mapped IP (MIP) address. A MIP maps the destination IP address in an IP packet header to another static IP address, enabling the FW/VPN device to receive incoming traffic at one IP address, and automatically forward that traffic to the mapped IP address. MIPs enable inbound traffic to reach private addresses in a zone that contains NAT mode interfaces.*

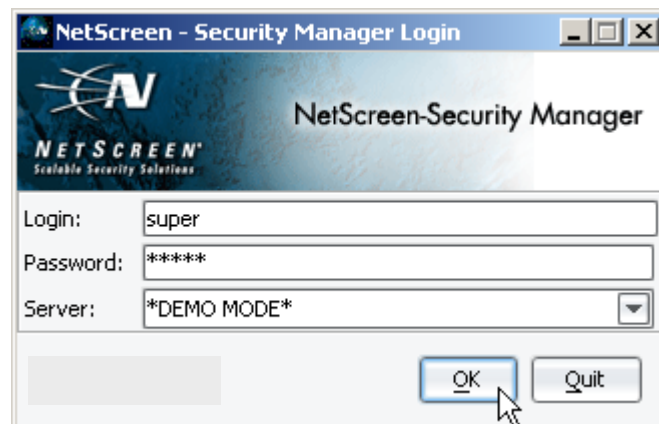
- **Device Server Manager Port.** The default port is 7800.
 - **Password for GUI Server Connection.** This password authenticates communication between the Device Server and GUI Server.
 - **Device Server ID.** The ID number identifies the Device Server; you cannot change the Device Server ID.
5. Click **OK** when you are done.

Running the UI in Demo Mode

Before you begin using Security Manager to configure and manage your network, it is recommended that you first run the UI in Demo mode. Demo mode is an option in the UI enabling you to run the UI disconnected from the management system.

To run the UI in Demo mode:

1. Run the Security Manager UI (from the **Start** menu, select **NetScreen-Security Manager > NetScreen-Security Manager** or double-click the Security Manager icon on your desktop). The Login window appears.
2. Enter any user name in the **Login** field provided.
3. Enter any password in the **Password** field provided.
4. Select ***DEMO MODE*** from the **Server** field pull-down menu.



5. Click **OK**.

NEXT STEPS

Congratulations! You have just completed installation of the Security Manager management system and User Interface. You can now begin to manage your network using Security Manager. Refer to the *NetScreen-Security Manager 2004 Administrator's Guide* for information describing how to plan and implement Security Manager for your network.

If you plan to install the GUI Server and Device Server on separate servers, refer to [Chapter 3, "Extended Configuration"](#) for more information.

Extended Configuration

In This Chapter

- [Installing the Management System, Extended Configuration](#)
- [Defining System Parameters](#)
- [Prerequisites](#)
- [Installing the GUI Server](#)
- [Installing the User Interface](#)
- [Installing the Device Server](#)
- [Transferring Certificate Files \(optional\)](#)
- [Next Steps](#)

For larger enterprises, specifically where you expect to generate an inordinate amount of traffic logs, it is recommended that you install the GUI Server and Device Server on separate servers.

This chapter describes how to install the Security Manager management system—GUI Server and Device Server on separate servers. This includes performing any prerequisite steps, running the management system installer, running the UI installer, and validating that you have installed the management system successfully.

INSTALLING THE MANAGEMENT SYSTEM, EXTENDED CONFIGURATION

Installing Security Manager in the extended configuration—where the GUI Server and Device Server are installed on separate servers is recommended in the following situations:

- You expect to generate or are required to store over (x) logs.
- You have geographically distributed sites and response time is important.

The following table summarizes the process for installing the management system on separate servers. It also provides an estimate of the overall amount of time that each step requires. The total time expected to complete the installation process is no longer than 30 minutes.

Step	Description	Estimated Time to Complete
1	Define system parameters that you need to provide during the installation process.	10 min.
2	Perform prerequisite steps. This includes creating the user that the Security Manager management system service runs as, and optionally partitioning drives for the GUI Server and Device Server data directories.	10 min.
3	Download the management system and UI installer software from the Security Manager installation CD or the NetScreen corporate Web site.	5 min.
4	Run the management system installer on the server where you want to install the GUI Server. Specify that you want to install the GUI Server only.	5 min.
5	Install the User Interface.	2-3 min.
6	Launch the UI, and connect it to the GUI Server. Add and configure the Device Server.	5 min.
7	Run the management system installer on the server where you want to install the Device Server only. Specify that you want to install the Device Server only.	5 min.
8	Transfer certificate files from the server that you are installing the Device Server to the server that you are installing the GUI Server.	5 min.

DEFINING SYSTEM PARAMETERS

During the installation process, you are required to configure common system parameters such as the location of the directories where you wish to store data for the GUI Server and Device Server. It is necessary that you define these system parameters before performing the management system installation.

The following table identifies the parameters that you need to identify:

Parameter	Description
Management IP address and port of the GUI Server	The IP address and port used by the running GUI Server are required to start the Device Server. The Device Server also needs this information enabling it to connect and communicate with the GUI Server.
GUI Server data directory	<p>Directory location where user data on the GUI Server is stored. By default, the installer stores data on the GUI Server in the following location:</p> <pre style="text-align: center;">/var/netscreen/GuiSvr/</pre> <p>Because the data on the GUI Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</p>
Device Server data directory	<p>Directory location where device data on the Device Server is stored. By default, the installer stores data on the Device Server in:</p> <pre style="text-align: center;">/var/netscreen/DevSvr/</pre> <p>Because the data on the Device Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</p>
Initial "super" user password	This is the password required to authenticate the initial user in the system. By default, the initial super user account receives all administrative privileges in the system.
Device Server ID	unique ID automatically assigned when you add the Device Server.
Password for GUI Server Connection	password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.

PREREQUISITES

Perform the prerequisite steps described as if you were installing the management system on the same server. Refer to [Chapter 2, “Typical Configuration”](#) for more information on installing the management system on the same server.

INSTALLING THE GUI SERVER

The management system installer guides you through all the steps required to configure system parameters, then runs to completion.

To install the GUI Server:

1. Navigate to the directory where you have saved the management system installer file.
2. Run the management system installer.

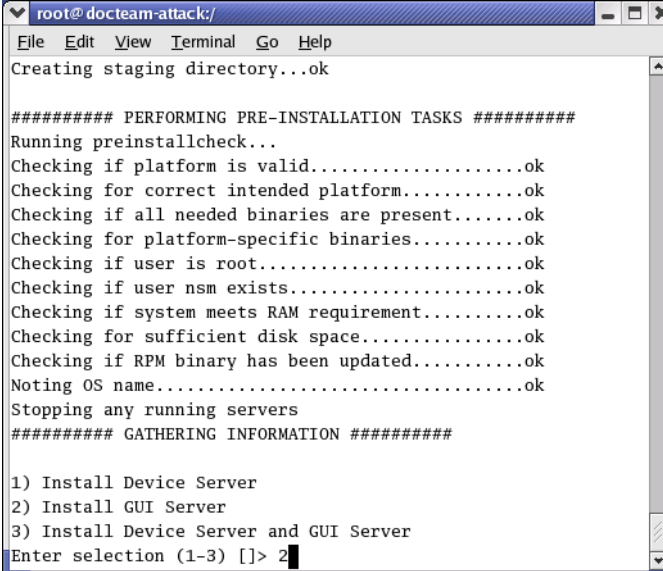
On Linux, you can run the management system installer using the following command:

```
sh nsm2004_servers_linux_x86.sh
```

On Solaris, you can run the management system installer using the following command:

```
sh nsm2004_servers_sol_sparc.sh
```

The installation begins automatically. The following depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.



```
root@docteam-attack:/
File Edit View Terminal Go Help
Creating staging directory...ok

##### PERFORMING PRE-INSTALLATION TASKS #####
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Checking if RPM binary has been updated.....ok
Noting OS name.....ok
Stopping any running servers
##### GATHERING INFORMATION #####

1) Install Device Server
2) Install GUI Server
3) Install Device Server and GUI Server
Enter selection (1-3) [ ]> 2
```

It performs a series of pre-installation checks to ensure that:

- you are installing the correct software for your operating system
- all the needed software binaries are present
- you have correctly logged in as root
- the system has sufficient disk space and RAM

The installer then stops any running servers.

Note: *The management system installer indicates the results of its specific tasks and checks:*

- **“Done”** indicates that the installer successfully performed a task.
- **“ok”** indicates that the installer performed a check, and verified that the condition was satisfied.
- **“FAILED”** indicates that the installer performed a task or check, but it was not successful.

The installer next prompts you to specify the components of the Security Manager management system that you wish to install.

Note: *If you have installed a previous version of the management system, you may notice different menu options.*

3. Enter selection **2** to specify that you want to install the GUI Server. The script then prompts you to specify where you want to store the GUI Server data files.
4. Enter the path for the directory that you want to store the data files for the GUI Server or press **ENTER** to accept the default path (the default location is `/var/netscreen/GuiSvr`).

Note: *If you specify a new directory location, the installer creates it. The installer does not however, allow you to specify an existing directory location. This is to safeguard against over-writing any existing data. If you try to specify an existing directory, the installer indicates that an existing directory already exists, and prompt you to try again.*

The script next prompts you to specify the management IP address of this server.

5. Enter the management IP address of this server. This should be the same IP address of the server that you are installing. The installer sets the IP address and port number on the GUI Server enabling the Device Server to start and connect. It attempts to connect to the GUI Server using port **7800** by default.

The script next prompts you to enter a password for the “super” user account. The initial administrator or “super” user account is the account that you use when you first log into Security Manager using the UI. This account is used to authenticate communication between the management system and the UI. It possesses all administrative privileges by default.

6. Enter any text string for the password. Enter the password again for verification.

Note: *Make a note of the password that you have set for the super user account. You need this when you first login to the system.*

The script next prompts you if you want to start the GUI Server once it has completed installation.

7. Enter **y** and then press **ENTER** to start the GUI Server once the installer has completed the installation process. Enter **n** and then press **ENTER**, if you do not want to start the GUI Server.

Note: Whenever you restart your server, the GUI Server starts automatically.

The script next prompts you to verify your installation configuration settings.

8. Verify your settings, and if they are correct, enter **y** and then press **ENTER** to proceed.

```
File Edit View Terminal Go Help
The GUI Server stores all of the user data under a single directory.
By default, this directory is /var/netScreen/GuiSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition. Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netScreen/GuiSvr]>

Enter the management IP address of this server [2.2.2.174]>

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Start server(s) when finished? (y/n) [n]> n

About to proceed with the following actions:
- Install GUI Server
- Store GUI Server data in /var/netScreen/GuiSvr
- Use IP address 2.2.2.174 for management
- Set password for 'super' user
- Start server(s) when finished: No

Are the above actions correct? (y/n)> y
```

If you enter **n** and then press **ENTER**, the installer returns you to the original Selection prompt.

The installation proceeds automatically. The installer proceeds to perform the following actions:

- extract the software payloads
- perform migration tasks (disregard since this is a new installation)
- perform installation tasks such as installing the GUI Server RPMs, creating the GUI Server data directory, and setting correct permissions.
- perform post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server.
- enabling the startup scripts for the GUI Server.

Several messages display to confirm the installation progress. The installer runs for several minutes, and then exits.

Viewing the Installation Log

The installer generates a log file with the output of the installation commands for troubleshooting purposes. This file is saved by default in the `tmp` subdirectory.

The naming convention used for the installation log file is:
`netmgtInstallLog.<current date><current time>`

For example if you ran the installer on December 1, 2003 at 6:00pm, the installation log file would be named: `netmgtInstallLog.20031201180000`

Note: *Once the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.*

INSTALLING THE USER INTERFACE

Install the Security Manager User Interface. Refer to [Chapter 2, “Typical Configuration”](#) for more information on installing the User Interface.

Adding the Device Server

Once you have installed the UI, you need to create the Device Server in Security Manager and configure the following:

- Device Server ID
- Password for GUI Server Connection

This information enables the Device Server to establish a connection with the GUI Server.

Note: Make a note of the Device Server ID and Password for GUI Server Connection. You will need this when you install the Device Server.

INSTALLING THE DEVICE SERVER

The management system installer guides you through all the steps required system parameters to configure, then runs to completion.

***Note:** Before installing the Device Server, verify that the GUI Server is up and running. After you install the Device Server, the installer starts the Device Server by default. If the GUI Server is not already up and running, the Device Server will fail to connect to it.*

To install the management system on a single server:

1. Navigate to the directory where you have saved the management system installer file.
2. Run the management system installer for the same platform that you used to install the GUI Server.

***Note:** You must install and run both servers on the same platform. NetScreen-Security Manager 2004 does not support the GUI Server and Device Server running on different platforms. For example, you cannot install the GUI Server on a system running Solaris, and the Device Server on a system running Linux.*

On Linux, you can run the management system installer using the following command:

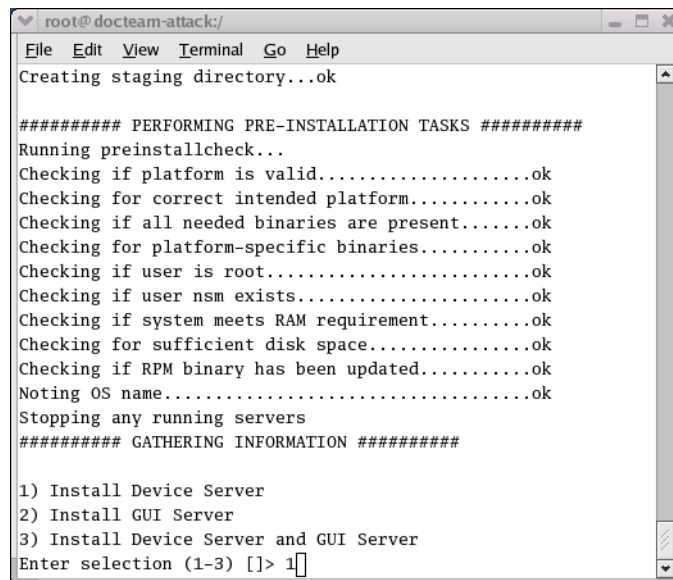
```
sh nsm2004_servers_linux_x86.sh
```

On Solaris, you can run the management system installer using the following command:

```
sh nsm2004_servers_sol_sparc.sh
```

The installation begins automatically. The following depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.

The installer next prompts you to specify the components of the Security Manager management system that you wish to install.



```
root@docteam-attack:/
File Edit View Terminal Go Help
Creating staging directory...ok

##### PERFORMING PRE-INSTALLATION TASKS #####
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Checking if RPM binary has been updated.....ok
Noting OS name.....ok
Stopping any running servers
##### GATHERING INFORMATION #####

1) Install Device Server
2) Install GUI Server
3) Install Device Server and GUI Server
Enter selection (1-3) []> 1
```

Note: If you have installed a previous version of the management system, you may notice different menu options.

3. Enter selection **1** to specify that you want to install the Device Server only. The script then prompts you to specify where you want to store the Device Server data files.
4. Enter the path for the directory that you want to store the data files for the Device Server or press **ENTER** to accept the default path (the default location is `/var/netscreen/DevSvr`).

The script next prompts you to specify the IP address of the Device Server.

5. Enter the management IP address of this server. This should be the same IP address of the server that you are installing on.

The script next prompts you to enter the ID assigned by the UI to this Device Server.

6. Enter the Device Server ID. The script next prompts you to enter the one time password for this Device Server.
7. Enter the Password for GUI Server connection.

The script next prompts you for the IP address and port number of the running GUI Server. This is required to enable the Device Server to start and communicate with the GUI Server.

8. Enter the IP address of the running GUI Server.

9. Enter the port number of the running GUI Server. The installer sets the IP address and port number on the GUI Server enabling the Device Server to connect. It attempts to connect to the GUI Server using port **7800** by default.

The script next prompts if you want to start the Device Server once it has completed installation.

***Note:** Do not specify that you want to start the Device Server service automatically unless you have already started the GUI Server.*

10. Enter **y** and then press **ENTER** to start the Device Server once the installer has completed the installation process. Enter **n** and then press **ENTER**, if you do not want to start the device server.

***Note:** When you restart your server, the Device Server starts automatically.*

The script next prompts you to verify your installation configuration settings.

11. Verify your settings, and if they are correct, enter **y** and then press **ENTER** to proceed.

```
File Edit View Terminal Go Help
The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition. Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

Enter the management IP address of this server [2.2.2.174]>

Enter the ID assigned by the GUI to this Device Server (1-65535) []> 1234

Enter the one-time password for this Device Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

To enable the Device Server to communicate with the GUI Server, you must
provide the IP address and the port of the running GUI Server
Enter the IP address of the running GUI Server []> 10.1.2.3
Enter the port number (1-65535) of the running GUI Server [7800]> 7800

NOTE: Do not start up the Device Server unless you have already added it to
the system from the UI.
Start server(s) when finished? (y/n) [y]> n

About to proceed with the following actions:
- Install Device Server
- Store Device Server data in /var/netscreen/DevSvr
- Use IP address 2.2.2.174 for management
- Connect to GUI Server at 10.1.2.3:7800
- Start server(s) when finished: No

Are the above actions correct? (y/n)> y
```

If you enter **n** and then press **ENTER**, the installer returns you to the original Selection prompt. The installation proceeds automatically. The installer proceeds to perform the following actions:

- checks if a tftp server is installed on the system. If the installer does not detect a tftp server, a message indicating that you must install a tftp server to enable firmware updates for FW/VPN devices running ScreenOS versions 4.0.x appears. Refer to [“Installing a TFTP Server” on page 58](#) for more information on installing a tftp server.
- extract the software payloads
- perform migration tasks (disregard since this is a new installation)
- perform installation tasks such as installing the Device Server RPMs, creating the Device Server data directory, and setting correct permissions.
- perform post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server.
- enabling the startup scripts for the Device Server.

Several messages display to confirm the installation progress. The installer runs for several minutes, and then exits.

TRANSFERRING CERTIFICATE FILES (OPTIONAL)

If you are using Security Manager to manage FW/VPN devices running ScreenOS 4.0.X, you must manually copy the certificate files generated by the installer from the server that you are installing the Device Server to the server that you are installing the GUI Server.

To transfer certificate files to the GUI Server:

1. Navigate to the `/DevSvr/var/certDB/config` subdirectory on the server where you have installed the Device Server.
2. Locate and copy the following files:
`cacertificate_table.nml`
`crl_table.nml`
`nacncertificate_table.nml`
3. Save these files in the `/GuiSvr/var` subdirectory on the server where you have installed the GUI Server.

NEXT STEPS

Congratulations! You have just completed installation of the Security Manager management system on separate servers. You are now ready to begin managing your network. Refer to the *NetScreen-Security Manager 2004 Administrator's Guide* for information describing how to plan and implement Security Manager for your network.

Administration

In This Chapter

- [Controlling the Management System](#)
- [Maintaining the Management System](#)
- [Installing a TFTP Server](#)
- [Uninstalling the User Interface](#)

This chapter describes basic procedures used to administer Security Manager. This includes instructions describing how to manually send commands to the management system such as start and stop, change the IP address of the GUI Server (in the event that you move the GUI Server to another server), install a TFTP server (required if you are managing FW/VPN devices running ScreenOS 4.0.x), and uninstall the management system and UI.

CONTROLLING THE MANAGEMENT SYSTEM

On occasion, it may become necessary to start or stop the management system processes manually. You can control the management system by navigating to the appropriate “bin” subdirectory for the Device Server or GUI Server, and issuing a manual command.

The management system supports the following commands.

Command	Action
reload	sends a hangup signal to the management system process, then instructs the process to reload its configuration and start again.
restart	stops the management system process for 2 seconds, then restarts the process.
start	starts the management system process
stop	stops the management system process
status	provides a status of the management system process
version	lists the current version of the management system

Viewing Management System Commands

To view all the manual commands that you can send to the GUI Server:

1. Navigate to the GUI Server bin subdirectory (i.e., `/usr/netscreen/GuiSvr/bin`).
2. Run the following command: `./guiSvr.sh`

To view all the manual commands that you can send to the Device Server:

1. Navigate to the Device Server bin subdirectory (i.e., `/usr/netscreen/DevSvr/bin`).
2. Run the following command: `./devSvr.sh`

Starting the GUI Server

To start the GUI Server manually:

1. Navigate to the GUI Server bin subdirectory (i.e., `/usr/netscreen/GuiSvr/bin`).
2. Run the following command: `./guiSvr.sh start`

Note: Always start the GUI Server before starting the Device Server. When started, the Device Server attempts to connect to the GUI Server. If the GUI Server is not already up and running, the Device Server will fail to connect to it.

Starting the Device Server

To start the Device Server manually:

1. Navigate to the Device Server bin subdirectory (i.e., `/usr/netscreen/DevSvr/bin`).
2. Run the following command: `./devSvr.sh start`

Stopping the GUI Server

To stop the GUI Server manually:

1. Navigate to the GUI Server bin subdirectory (i.e., `/usr/netscreen/GuiSvr/bin`).
2. Run the following command: `./guiSvr.sh stop`

Stopping the Device Server

To stop the GUI Server manually:

1. Navigate to the GUI Server bin subdirectory (i.e., `/usr/netscreen/GuiSvr/bin`).
2. Run the following command: `./guiSvr.sh stop`

MAINTAINING THE MANAGEMENT SYSTEM

The following procedures are provided for your reference:

- [“Changing the Management System IP Address” on page 56](#)
- [“Changing the Device Server IP Address” on page 56](#)
- [“Changing the GUI Server IP Address” on page 57](#)
- [“Uninstalling the Management System” on page 57](#)

Changing the Management System IP Address

If you have installed the Security Manager management system on a single server (i.e., in the basic configuration), and you move it later to a different server, you need to re-configure the management IP address and port enabling your managed FW/VPN devices to connect to it at its new location.

To change the management system IP address:

1. Update the Device Server IP on each FW/VPN device (or set the secondary management server IP to the new IP address).
2. Login to the server where you are running the Device Server as root.
3. Navigate to `usr/netscreen/DevSvr/var`.
4. Open the Device Server configuration file (`devSvr.cfg`) in any text editor.
5. Edit the values for the `guiSvr.addr` and `guiSvr.port` variables using the new IP address and port number.
6. Open the `server_table.nml` file in any text editor.
7. Edit the values for: `ip "<a.b.c.d>"` in both GUI and Device Server sections.
8. Restart the GUI Server, then restart the Device Server.

Changing the Device Server IP Address

If you have installed the Security Manager management system on separate servers (i.e., in the extended configuration), and you later move the Device Server to a different server, you need to re-configure the management IP address and port enabling your managed FW/VPN to connect to it at its new location.

To change the Device Server IP address:

1. Update the Device Server IP on each FW/VPN device (or set the secondary management server IP to the new IP address).
2. Login to the server where you are running the Device Server as root.
3. Navigate to `usr/netscreen/DevSvr/var`.
4. Login to the server where you are running the GUI Server as root.
5. Navigate to `usr/netscreen/DevSvr/var`.
6. Open the `server_table.nml` file in any text editor.
7. Edit the values for: `ip "<a.b.c.d>"` in the Device Server section only.

8. Restart the GUI Server.

Changing the GUI Server IP Address

If you have installed the Security Manager management system on separate servers (i.e., in the extended configuration), and you later move the GUI Server to a different server, you need to re-configure the management IP address and port enabling the Device Server to connect to it at its new location.

To change the GUI Server IP address:

1. Login to the server where you are running the Device Server as root.
2. Navigate to `usr/netscreen/DevSvr/var`.
3. Open the Device Server configuration file (`devSvr.cfg`) in any text editor.
4. Edit the values for the `guiSvr.addr` and `guiSvr.port` variables using the new IP address and port number.
5. Login to the server where you are running the GUI Server as root.
6. Navigate to `usr/netscreen/GuiSvr/var`.
7. Open the `server_table.nml` file in any text editor.
8. Edit the values for: `ip "<a.b.c.d>"` in the GUI Server section only.
9. Restart the GUI Server, then restart the Device Server.

Uninstalling the Management System

To uninstall previous management system installations:

1. Stop the GUI Server. For example, you can do this by running the following command:

```
cd /usr/netscreen/GuiSvr/bin
./guiSvr.sh stop
```
2. Stop the Device Server. For example, you can do this by running the following command:

```
cd /usr/netscreen/DevSvr/bin
./devSvr.sh stop
```
3. Navigate to the `var` subdirectory, and remove all files in the `netscreen` subdirectory. For example, you can do this by running the following commands:

```
rpm -e netscreen-DevSvr
rpm -e netscreen-GuiSvr
rm -rf netscreen
```

INSTALLING A TFTP SERVER

If you are using Security Manager to manage FW/VPN devices running ScreenOS 4.0.x, you must install and run a TFTP server on the system that you are running the GUI Server. The TFTP server is required to enable firmware updates for FW/VPN devices running ScreenOS versions 4.0.x.

Installing a TFTP Server on Linux

Before installing the TFTP server on your Red Hat Linux server, you should first check to see if it is already installed.

To verify if the TFTP server is already installed on your Linux server, run the following command:

```
rpm -q tftp-server
```

If the TFTP server is installed, the output indicates the following:

```
tftp-server-<version>-<revision>
```

For example, the output for an unpatched Red Hat 9.0 server is as follows:

```
tftp-server-0.32-4
```

If the TFTP server is not installed, download and install the package from the Red Hat Linux installation CD, or from the Internet at the Red Hat or Red Hat mirror site. Once the package is installed, you must enable and configure the TFTP server.

To configure and enable the TFTP server on Linux:

1. Open the `/etc/xinetd.d/tftp` file in any text editor.
2. Edit the parameter “`server_args =`” so that the value is “`-s /usr/netscreen/DevSvr/var/cache`”.
3. Edit the parameter “`disable`” so that the value is “`no`”. The file should now appear as follows:

```
service tftp
{
    socket_type = dgram
    protocol = udp
    wait = yes
    user = root
    server = /usr/sbin/in.tftpd
    server_args = -s /usr/netscreen/DevSvr/var/cache
    disable = no
    per_source = 11
    cps = 100 2
}
```

4. Restart the `xinetd` service. You can do so by running the following command:

```
service xinetd restart
```

Installing a TFTP Server on Solaris

By default, Solaris installs the TFTP service on your machine but leaves it disabled.

To configure and enable the TFTP service on Solaris:

1. Open the `/etc/inetd.conf` file in any text editor.
2. Uncomment the line that begins with the word “tftp” or “#tftp”.
3. Edit the same line by replacing the words “in.tftpd -s /tftpboot” at the end of the line with “in.tftpd -s /usr/netscreen/DevSvr/var/cache”. The line should now appear as follows:

```
tftp dgram udp wait root /usr/sbin/in.tftpd
in.tftpd -s /usr/netscreen/DevSvr/var/cache
```

4. Restart the inetd service. You can do so by running the following commands:

```
/etc/init.d/inetsvc stop
/etc/init.d/inetsvc start
```

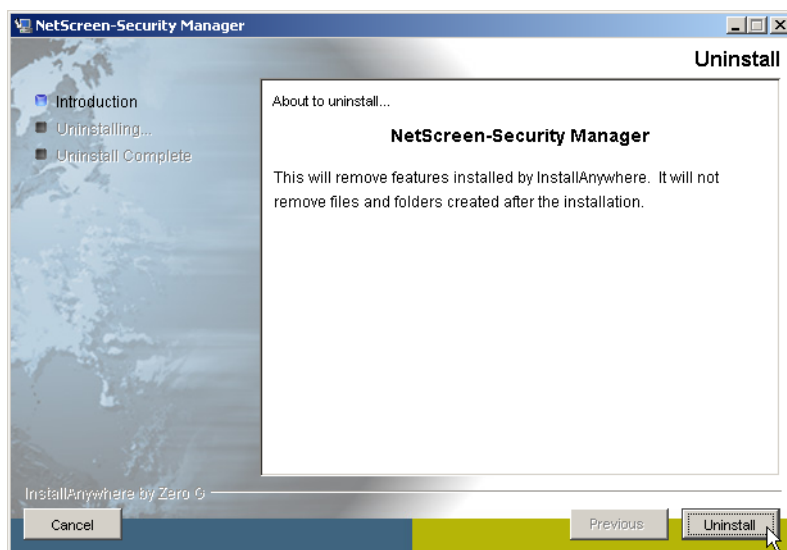
UNINSTALLING THE USER INTERFACE

If it is necessary to uninstall the Security Manager UI, run the Security Manager uninstall program.

***Note:** It is not recommended that you use the Add/Remove Programs utility to remove the Security Manager UI.*

To uninstall the Security Manager UI:

1. From the **Start** menu, select **NetScreen-Security Manager > Uninstall Security Manager**. The uninstaller launches.



2. Click the **Uninstall** button to uninstall the UI. The uninstaller proceeds to uninstall all the UI software files, shortcuts, folders and registry entries.
When the uninstaller has finished, a window appears indicating that all files were successfully uninstalled.
3. Click **Done** to exit the uninstaller.

Index

A

adding, Device Server [45](#)

C

capacity planning, management system [14–16](#)

certificates

files [50](#)

transferring [50](#)

communication ports [7–9](#)

communications [7–9](#)

configuration options

installing management system on same server
(typical) [10](#)

installing management system on separate
servers (extended) [11](#)

configuring

Device Server data directory [25](#)

Device Server ID [47](#)

GUI Server data directory [25](#)

management system IP addresses [57](#)

password for GUI Server connection [47](#)

password for super user [26](#)

CPU

requirements on management system, same
server [12](#)

requirements on management system, separate
servers [12](#)

D

data directory

for device-server, described [21, 39](#)

for GUI-server, described [21, 39](#)

defining system parameters [21, 39](#)

Demo Mode [35](#)

Device Server

adding [45](#)

communication ports, described [8](#)

data directory, configuring [25](#)

described [5](#)

installing [46–49](#)

starting [55](#)

stopping [55](#)

Device Server ID

configuring [47](#)

described [39](#)

devices

see FW/VPN devices

disk storage

requirements on management system, same
server [12](#)

requirements on management system, separate
servers [12](#)

E

extended configuration option [11](#)

F

FW/VPN devices

maximum number supported [5](#)

platforms supported [6](#)

G

Global PRO data export utility [3](#)

GUI Server

communication ports, described [7](#)

data directory, configuring [25](#)

described [5](#)

installing [41–43](#)

starting [54](#)

stopping [55](#)

H

hardening your system [15–16](#)

hardware

capacity planning [14–16](#)

requirements for UI [13](#)

I

installation

log file for management system [29, 44](#)

log file for UI [32](#)

installing

- configuration options 10
- Device Server 46–49
- GUI Server 41–43
- management system on same server 20–29
- management system on separate servers 38–50
- prerequisite steps 22–23
- TFTP server on Linux 58
- TFTP server on Solaris 59
- UI 30–32

L

Linux RPM package

- requirements 22
- verifying 22

Linux system update utility

- described 3
- running 23

log file

- management system install 29
- UI installation 32

logging in to the UI 33

M

management IP address

- for GUI-server, described 39

management IP address for GUI-server 21

management server

- see management system

management system

- capacity planning 14–16
- commands 54
- described 4–5
- installing on same server 20–29
- installing on separate servers 38–50
- restarting 54
- starting 54
- status 54
- stopping 54
- uninstalling 57

memory requirements

- capacity planning 14
- for UI 13
- management system on same server 12
- management system on separate servers 12

minimum system requirements

- described 12–13
- for UI 13
- management system 12

N

network connection

- requirements for UI 13
- requirements on management system, same server 12
- requirements on management system, separate servers 12

O

operating system

- requirements for management system 12
- requirements for UI 13

P

password

- super user, configuring 26
- super user, described 21

Password for GUI Server connection

- configuring 47
- described 39

prerequisites before installing 22–23

R

restarting

- management system manually 54
- restarting management system 54

running

- UI 32
- UI, in Demo Mode 35

S

ScreenOS versions supported 6

securing Security Manager 15–16

Security Manager technical overview 4–9

server

- see management system

sizing

- see capacity planning

starting

- Device Server [55](#)
- GUI Server [54](#)
- management system manually [54](#)
- stopping
 - Device Server [55](#)
 - GUI Server [55](#)
 - management system manually [54](#)
- super user
 - password, configuring [26](#)
 - password, described [21, 39](#)
- swap space
 - requirements on management system, same server [12](#)
 - requirements on management system, separate servers [12](#)
- system parameters [21, 39](#)

T

- TFTP server
 - installing [58–59](#)
 - installing on Linux [58](#)
 - installing on Solaris [59](#)
- typical configuration option [10](#)

U

- UI
 - described [6](#)
 - hardware requirements [13](#)
 - installing [30–32](#)
 - operating system requirements [13](#)
 - running [32](#)
 - uninstalling [60](#)
- uninstalling
 - management system [57](#)
 - UI [60](#)
- upgrading RPM package (for Linux only) [22–23](#)
- user interface
 - See UI

V

- validating
 - management system installation [34](#)
 - management system status [28](#)
- verifying Linux RPM package [22](#)
- viewing management system commands [54](#)

