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-20t, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Security Manager, 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 ............................................................................................................................... ix
  Organization ......................................................................................................................... x
  NetScreen Publications ......................................................................................................... xi

Introduction ............................................................................................................................. 1

Migration and Installation Process ......................................................................................... 2
  Management System Install Process ..................................................................................... 2
  Data Export Process (Optional) ........................................................................................... 2
  User Interface Install Process .............................................................................................. 4
  Data Import Process (Optional) ........................................................................................... 4

Installation Package ............................................................................................................... 6

Minimum System Requirements ............................................................................................. 7
  System Requirements - Management System ........................................................................ 7
  System Requirements - User Interface .................................................................................. 8

Configuration Options ........................................................................................................... 9
  Typical Configuration ........................................................................................................... 9
  Extended Configuration ...................................................................................................... 10

Next Steps .............................................................................................................................. 11

Migrating and Installing From Global PRO Express ............................................................. 13

Migration and Installation Scenarios ..................................................................................... 14
  Installing Security Manager Using Existing Hardware ......................................................... 14
  Installing Security Manager Using New Hardware .............................................................. 15
  Installing Security Manager Using Both Existing and New Hardware ............................. 16
  Migration Scenarios Not Supported .................................................................................... 17
  Migration Path ..................................................................................................................... 17

Pre-Migration Steps ............................................................................................................... 18

Installing the Management System ....................................................................................... 19
  Defining System Parameters .............................................................................................. 19
  Prerequisite Steps ............................................................................................................. 20
  Other Recommended Actions ............................................................................................ 22
  Upgrading the RPM Package (For Linux Users Only) ......................................................... 22
  Installing Unix Client Utilities For Automatic Database Backup Tool (Optional) .......... 24

Installing the Management System Software ....................................................................... 25
  Validating Management System Status .............................................................................. 31
  Installing the Management System On Separate Servers ................................................. 32
  Viewing the Installation Log .............................................................................................. 32

Exporting Data From Global PRO Express ......................................................................... 33
  Transferring the Export Data Files ..................................................................................... 33
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the User Interface</td>
<td>34</td>
</tr>
<tr>
<td>Viewing the Installation Log</td>
<td>38</td>
</tr>
<tr>
<td>Running the User Interface</td>
<td>38</td>
</tr>
<tr>
<td>Validating the Installation</td>
<td>39</td>
</tr>
<tr>
<td>Running the UI in Demo Mode</td>
<td>41</td>
</tr>
<tr>
<td>Importing Data Into Security Manager</td>
<td>42</td>
</tr>
<tr>
<td>Import Process</td>
<td>42</td>
</tr>
<tr>
<td>Resolving Domain Name Conflicts</td>
<td>42</td>
</tr>
<tr>
<td>Importing Migration Data</td>
<td>43</td>
</tr>
<tr>
<td>Rolling Back a Failed Migration</td>
<td>45</td>
</tr>
<tr>
<td>Validating a Successful Migration</td>
<td>45</td>
</tr>
<tr>
<td>Post Migration Steps</td>
<td>46</td>
</tr>
<tr>
<td>Manually Configuring Protected Resources</td>
<td>46</td>
</tr>
<tr>
<td>Manually Configuring Authentication Servers</td>
<td>46</td>
</tr>
<tr>
<td>Manually Configuring VPNs</td>
<td>46</td>
</tr>
<tr>
<td>Transferring Certificate Files</td>
<td>46</td>
</tr>
<tr>
<td>Next Steps</td>
<td>47</td>
</tr>
<tr>
<td>Migrating and Installing From Global PRO</td>
<td>49</td>
</tr>
<tr>
<td>Migration and Installation Scenarios</td>
<td>50</td>
</tr>
<tr>
<td>Installing Management System Using New Hardware</td>
<td>50</td>
</tr>
<tr>
<td>Installing Management System Using Existing Hardware</td>
<td>51</td>
</tr>
<tr>
<td>Considerations If You Are Running Multiple Arbitrators</td>
<td>53</td>
</tr>
<tr>
<td>Considerations If You Are Running Multiple Data Collectors</td>
<td>54</td>
</tr>
<tr>
<td>Maintaining Historical Reporting Functionality</td>
<td>54</td>
</tr>
<tr>
<td>Migration Scenarios Not Supported</td>
<td>55</td>
</tr>
<tr>
<td>Migration Path</td>
<td>55</td>
</tr>
<tr>
<td>Pre-Migration Steps</td>
<td>56</td>
</tr>
<tr>
<td>Installing the Management System</td>
<td>57</td>
</tr>
<tr>
<td>Defining System Parameters</td>
<td>57</td>
</tr>
<tr>
<td>Prerequisite Steps</td>
<td>58</td>
</tr>
<tr>
<td>Other Recommended Actions</td>
<td>60</td>
</tr>
<tr>
<td>Upgrading the RPM Package (For Linux Users Only)</td>
<td>60</td>
</tr>
<tr>
<td>Installing Unix Client Utilities For Automatic Database Backup Tool</td>
<td>62</td>
</tr>
<tr>
<td>Installing the Management System Software</td>
<td>63</td>
</tr>
<tr>
<td>Validating Management System Status</td>
<td>69</td>
</tr>
<tr>
<td>Installing the Management System On Separate Servers</td>
<td>69</td>
</tr>
<tr>
<td>Viewing the Installation Log</td>
<td>70</td>
</tr>
<tr>
<td>Exporting Data From Global PRO</td>
<td>71</td>
</tr>
<tr>
<td>Policy Manager Export Data</td>
<td>71</td>
</tr>
<tr>
<td>Report Manager Export Data</td>
<td>71</td>
</tr>
<tr>
<td>Transferring the Export Data Files</td>
<td>71</td>
</tr>
<tr>
<td>Installing the User Interface</td>
<td>72</td>
</tr>
<tr>
<td>Viewing the Installation Log</td>
<td>76</td>
</tr>
<tr>
<td>Running the User Interface</td>
<td>76</td>
</tr>
<tr>
<td>Validating the Installation</td>
<td>77</td>
</tr>
</tbody>
</table>
# Migration Details

<table>
<thead>
<tr>
<th>Category</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications</td>
<td>A-V</td>
</tr>
<tr>
<td>Domains</td>
<td>B-II</td>
</tr>
<tr>
<td>Domain Migration</td>
<td>B-II</td>
</tr>
<tr>
<td>Devices and Device Groups</td>
<td>B-III</td>
</tr>
<tr>
<td>Policy Manager Device Migration</td>
<td>B-III</td>
</tr>
<tr>
<td>Report Manager/Realtime Monitor Device Migration</td>
<td>B-IV</td>
</tr>
<tr>
<td>Users and User Groups</td>
<td>B-VI</td>
</tr>
<tr>
<td>Policy Manager User Migration</td>
<td>B-VI</td>
</tr>
<tr>
<td>Report Manager/Realtime Monitor User Migration</td>
<td>B-VII</td>
</tr>
<tr>
<td>Policy Manager User Group Migration</td>
<td>B-VII</td>
</tr>
</tbody>
</table>
| Report Manager/Realtime Monitor User Group Migration | B-VIII |}

<table>
<thead>
<tr>
<th>Category</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Objects</td>
<td>B-X</td>
</tr>
<tr>
<td>Address Book Migration</td>
<td>B-X</td>
</tr>
<tr>
<td>Schedule Objects</td>
<td>B-XII</td>
</tr>
<tr>
<td>Schedule Object Migration</td>
<td>B-XII</td>
</tr>
<tr>
<td>Service Objects</td>
<td>B-XIII</td>
</tr>
<tr>
<td>Service Object Migration</td>
<td>B-XIII</td>
</tr>
<tr>
<td>Shared and Protected Resources</td>
<td>B-XIV</td>
</tr>
<tr>
<td>Shared Resource Object Migration</td>
<td>B-XIV</td>
</tr>
<tr>
<td>Global Objects</td>
<td>B-XVI</td>
</tr>
<tr>
<td>Global Object Migration</td>
<td>B-XVI</td>
</tr>
<tr>
<td>Authentication Servers</td>
<td>B-XVII</td>
</tr>
<tr>
<td>Authentication Server Object Migration</td>
<td>B-XVII</td>
</tr>
<tr>
<td>Group Expressions</td>
<td>B-XIX</td>
</tr>
<tr>
<td>Group Expression Migration</td>
<td>B-XIX</td>
</tr>
<tr>
<td>Shared Configs</td>
<td>B-XX</td>
</tr>
<tr>
<td>Shared Config Object Migration</td>
<td>B-XX</td>
</tr>
<tr>
<td>Zone Profile</td>
<td>B-XXII</td>
</tr>
<tr>
<td>Zone Profile Object Migration</td>
<td>B-XXII</td>
</tr>
<tr>
<td>Policies</td>
<td>B-XXIII</td>
</tr>
<tr>
<td>Policy Migration</td>
<td>B-XXIII</td>
</tr>
<tr>
<td>VPNs</td>
<td>B-XXIV</td>
</tr>
<tr>
<td>VPN Migration</td>
<td>B-XXIV</td>
</tr>
<tr>
<td>P1 and P2 Proposals</td>
<td>B-XXV</td>
</tr>
<tr>
<td>P1 and P2 Proposal Object Migration</td>
<td>B-XXV</td>
</tr>
<tr>
<td>IP Pools</td>
<td>B-XXVI</td>
</tr>
<tr>
<td>IP Pool Migration</td>
<td>B-XXVI</td>
</tr>
</tbody>
</table>
Thank you for choosing NetScreen-Security Manager 2004 FP1, the integrated management software for all NetScreen FW/VPN devices and systems.

This NetScreen-Security Manager 2004 FP1 Migration Guide describes how to install and setup an initial working Security Manager system using either new or existing hardware. It also describes how you can migrate data from your existing NetScreen management system into Security Manager.

This Migration Guide is intended primarily for IT administrators and primary application administrators who are responsible for installing Security Manager, and migrating data from either NetScreen-Global PRO Express™ or NetScreen-Global PRO™ into Security Manager.

**Note:** If you have not previously used a version of NetScreen-Global PRO or NetScreen-Global PRO Express, and are installing NetScreen management software for the first time, refer to the NetScreen-Security Manager 2004 FP1 Installer’s Guide for more specific information on new installations of NetScreen-Security Manager.
Preface

Organization

The NetScreen-Security Manager 2004 FP1 Migration Guide contains the following four chapters and two appendices:

- **Chapter 1, “Introduction”** provides an introduction to the installation and migration process. It describes minimum system requirements to help you to identify the appropriate hardware and software that you need to install and run Security Manager. It also provides an overview of the tools that you will use to import data from your existing management software into Security Manager.

- **Chapter 2, “Migrating and Installing From Global PRO Express”** describes the migration and installation process specifically for those who have previously used NetScreen-Global PRO Express. It describes planning considerations for installing Security Manager using new or existing hardware. It also describes how to install Security Manager and migrate data from NetScreen-Global PRO Express into Security Manager.

- **Chapter 3, “Migrating and Installing From Global PRO”** describes the installation and migration process specifically for those who have previously used NetScreen-Global PRO. It describes planning considerations for installing Security Manager over existing hardware. It also describes how to install Security Manager and migrate data from Global PRO into Security Manager.

- **Chapter 4, “Administration”** describes how to maintain and uninstall the management system and UI.

- **Appendix A, “Technical Overview”** provides an overview of the NetScreen-Security Manager three-tiered architecture including the management system, User Interface, and the managed firewall/VPN devices in your network.

- **Appendix B, “Migration Details”** provides an overview of how features in NetScreen-Global PRO and NetScreen-Global PRO Express map to Security Manager.
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
NetScreen-Security Manager is software that enables you to integrate control and management of your network security environment including firewalls and VPNs. You can install Security Manager using new hardware or over your existing hardware configuration. If you are currently using a previous version of NetScreen management software (NetScreen-Global PRO or NetScreen-Global PRO Express), you can also migrate your existing configuration data into Security Manager.

This chapter provides an overview of the Security Manager migration and installation process, minimum hardware and software requirements and other migration planning considerations.
MIGRATION AND INSTALLATION PROCESS

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 and migrating configuration data from your previous NetScreen management software is as follows:

- “Management System Install Process” on page 2
- “Data Export Process (Optional)” on page 2
- “User Interface Install Process” on page 4
- “Data Import Process (Optional)” on page 4

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.

The management system installer is a shell archive script that you can run on any dedicated, secure and trusted Solaris 8 or 9, Red Hat Linux 8.0, 9.0, or Red Hat Enterprise Linux ES server that meets minimum system requirements. Refer to “Minimum System Requirements” on page 7 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.

Data Export Process (Optional)

Security Manager supports the migration of data from the following previous versions of NetScreen management software:

- Global PRO Express
- Global PRO

Note: Security Manager does not support the migration of data from NetScreen-IDP.

If you wish to migrate data from your previous version of NetScreen management software, you must install and run the Global PRO data export utility over your existing hardware configuration.
Global PRO Data Export Utility

The Global PRO data export utility is a shell archive script (the file is called “nsm04fp1_gpexport_sol_sparc.sh”) that you can install and run on any Solaris system. The Global PRO data export utility is also part of the management system installation package for Solaris. If you run the Security Manager installer for Solaris on your existing Global PRO Express appliance or Global PRO arbitrator, the installer automatically detects if you are running Global PRO or Global PRO Express on the system. If Global PRO or Global PRO Express is detected running on the system, the installer automatically installs and runs the utility.

The Global PRO data export utility performs all the functions necessary to export configuration data from your previous installation of Global PRO or Global PRO Express including device configuration data from the managed FW/VPN devices in your network. During the export process, you can specify whether you want to export data from all domains, a group of domains (i.e., you can do this by listing them separated by a comma), or a specific domain in Policy Manager.

The process by which the Global PRO data export utility extracts configuration data is as follows:

1. Initially, the Global PRO data export utility extracts configuration data from the local LDAP server on the Global PRO Express appliance or Global PRO arbitrator. For Report Manager, it extracts configuration data from the database on the Report Manager Master Controller.
2. It then attempts to contact each individual managed device for the latest device configuration data. If the utility is successful in connecting to the device, it retrieves the device configuration directly from the device.
3. If the utility is not successful in connecting to the device, it extracts the device configuration from the latest configuration summary generated for the device in Policy Manager.

When it has completed this process, the Global PRO data export utility saves export data from Policy Manager and your device configurations in the following location:

/usr/netscreen/migration/var/data/pmexport.tar

The Global PRO data export utility saves the export data from Realtime Monitor or Report Manager in the following location:

/usr/netscreen/migration/var/data/RMexport.out
Using the Global PRO Data Export Utility

The following table outlines instructions for migrating from Global PRO Express and Global PRO.

<table>
<thead>
<tr>
<th>Migrating From...</th>
<th>Install and run the...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScreen-Global PRO Express</td>
<td>Security Manager installer for Solaris on the Global PRO Express appliance.</td>
</tr>
<tr>
<td></td>
<td>The installer automatically detects your previous installation of Global PRO Express and installs and runs the Global PRO data export utility.</td>
</tr>
<tr>
<td>NetScreen-Global PRO</td>
<td>Global PRO data export utility on the servers where you are running your Global PRO arbitrator(s) for Policy Manager and device configuration data.</td>
</tr>
<tr>
<td></td>
<td>Global PRO data export utility on the server where you are currently running your Report Manager Master Controller for Report Manager data.</td>
</tr>
</tbody>
</table>

Once you have completed exporting your data from your previous NetScreen management software, you can then import the data into Security Manager using the Security Manager User Interface.

Transferring Export Files

Once you have exported your data from Global PRO and Global PRO Express, you must transfer the files to the following directory location on the server where you have installed your GUI Server:

```
/usr/netscreen/GuiSvr/var/migration/
```

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 7 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.

Data Import Process (Optional)

Once you are connected to the Security Manager management system, you can import your exported data into Security Manager.
You can run the import process multiple times without corrupting the Security Manager database. The import of Policy Manager and Realtime Monitor/Report Manager data can be done at the same time or separately. If you are planning on importing data from both Policy Manager and Realtime Monitor/Report Manager, it is highly recommended that you perform the import of data from Policy Manager before or at the same time as you import your data from Realtime Monitor/Report Manager. This is because you want to establish your configuration data in Security Manager in the domains that applied in Policy Manager. This configuration data is inherent in Policy Manager. Data configured in Realtime Monitor/Report Manager is not domain-specific.

Refer to Chapter 2, “Migrating and Installing From Global PRO Express” for more information on migrating from Global PRO Express.

Refer to Chapter 3, “Migrating and Installing From Global PRO” for more information on migrating from Global PRO.
Chapter 1 Introduction

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.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsm04fp1_ui_win_x86.exe</td>
<td>Installer for the Security Manager UI (for Windows-based computers).</td>
</tr>
<tr>
<td>nsm04fp1_ui_linux_x86.bin</td>
<td>Installer for the Security Manager UI (for Linux-based computers).</td>
</tr>
<tr>
<td>nsm04fp1_servers_linux_x86.sh</td>
<td>Installer for the Security Manager management system for Linux.</td>
</tr>
<tr>
<td>nsm04fp1_servers_sol_sparc.sh</td>
<td>Installer for the Security Manager management system for Solaris.</td>
</tr>
<tr>
<td>nsm04fp1_gpexport_sol_sparc.sh</td>
<td>Installer for the Global PRO data export utility used to migrate data from Global PRO Express/Global PRO into Security Manager.</td>
</tr>
<tr>
<td>system_update_fp1.tar</td>
<td>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. If you are installing on Solaris, you use this file to install Unix client utilities required to run the automatic database backup option.</td>
</tr>
</tbody>
</table>
**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:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI Server and Device Server on the same server</td>
<td>Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES</td>
</tr>
<tr>
<td></td>
<td><strong>CPU:</strong></td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems UltraSPARC IIi 500MHz (or higher), OR Linux 1GHz processor (or higher)</td>
</tr>
<tr>
<td></td>
<td><strong>RAM:</strong> 1GB (or higher); 2GB+ (depending on the number of managed devices and configuration size)</td>
</tr>
<tr>
<td></td>
<td><strong>Swap Space:</strong> 4 GB for both GUI Server and Device Server</td>
</tr>
<tr>
<td></td>
<td><strong>Storage:</strong> IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)</td>
</tr>
<tr>
<td></td>
<td><strong>Network Connection:</strong> 100MBps NIC Ethernet adapter</td>
</tr>
<tr>
<td></td>
<td>Server must be dedicated to running Security Manager only.</td>
</tr>
</tbody>
</table>

| GUI Server and Device Server on separate servers | Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES  |
|                                                 | **CPU:**  |
|                                                 | Sun Microsystems UltraSPARC IIi 500MHz (or higher), OR Linux 1GHz processor (or higher) |
|                                                 | **RAM:** 512MB (or higher); 1GB (recommended) |
|                                                 | **Swap Space:** 2 GB for the GUI Server, 2 GB for the Device Server  |
|                                                 | **Storage:** IDE Hard Disk Drive with 10K rpm (minimum) - 15K rpm (recommended); 18 GB disk space (minimum) - 40 GB disk space (recommended) |
|                                                 | **Network Connection:** 100MBps NIC Ethernet adapter  |
|                                                 | **I/O:** Split backplane (recommended for Device Server)  |
|                                                 | Each server must be dedicated to running Security Manager only.  |

Note that you may extend system performance and data capacity by expanding on the minimum requirements specified for each component. Refer to Appendix C “Sizing and Capacity Planning” for more information.
System Requirements - User Interface

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
</table>
| User Interface - Software | - Microsoft Windows XP, OR  
- Microsoft Windows NT<sup>®</sup> Workstation/Server 4.0, Service Pack 6a or higher, OR  
- Microsoft Windows 2000 Server, Advanced Server, or Professional editions, OR  
- Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES US English versions only |
| User Interface - Hardware | - IBM<sup>®</sup> compatible PC  
- 400MHz Pentium<sup>®</sup> 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. |
**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 9
- “Extended Configuration” on page 10

**Note:** *NetScreen-Security Manager 2004 Feature Pack 1 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.
This chapter has provided you with the following:

- an overview of the migration and installation process
- minimum system requirements to help you identify the appropriate hardware and software to install and run Security Manager
- options for implementing components of the Security Manager management system to provide for enhanced performance and scalability

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 several installation and migration scenarios that exist depending upon the type of NetScreen management software that you have previously used:

- See Chapter 2, “Migrating and Installing From Global PRO Express” for specific information on how to install and migrate to Security Manager if you are currently using Global PRO Express.
- See Chapter 3, “Migrating and Installing From Global PRO” for specific information on how to install and migrate to Security Manager if you are currently using Global PRO.
- See Chapter 4, “Administration” for specific information describing how to maintain and uninstall the management system and UI.
Migrating and Installing From Global PRO Express

In This Chapter

- Migration and Installation Scenarios
- Pre-Migration Steps
- Installing the Management System
- Exporting Data From Global PRO Express
- Installing the User Interface
- Importing Data Into Security Manager
- Post Migration Steps
- Next Steps

This chapter describes the Security Manager migration and installation process for those who have previously used Global PRO Express. It describes scenarios and procedures for migrating your configuration data from Global PRO Express and installing Security Manager using new or existing hardware.
Migration and Installation Scenarios

If you are currently using Global PRO Express, migration and installation scenarios are as follows:

- “Installing Security Manager Using Existing Hardware” on page 14
- “Installing Security Manager Using New Hardware” on page 15
- “Installing Security Manager Using Both Existing and New Hardware” on page 16

Installing Security Manager Using Existing Hardware

The following table details the migration and installation process if you are using existing hardware. It also provides an estimate of the overall amount of time each step requires.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Copy the required software to install the Security Manager management system (for Solaris) on your existing Global PRO Express appliance. Copy the required software for the Security Manager user interface to the computer where you plan to install the UI.</td>
<td>20 min.</td>
</tr>
<tr>
<td>2</td>
<td>Run the Security Manager management system installer on your existing Global PRO Express appliance to install the management system. The installer automatically detects if you have Global PRO Express installed on the appliance. It then installs and runs the Global PRO data export utility automatically. The Global PRO data export utility exports your data from Global PRO Express and the managed FW/VPN devices in your network, and then saves the exported data in two files: • pmexport.tar for your Policy Manager and device configuration data • rmxexport.out for your Realtime Monitor data</td>
<td>2-8 hours</td>
</tr>
<tr>
<td>3</td>
<td>Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server.</td>
<td>10 min.</td>
</tr>
<tr>
<td>4</td>
<td>Install the User Interface.</td>
<td>5 min.</td>
</tr>
<tr>
<td>5</td>
<td>Launch the UI, and connect it to the management system.</td>
<td>5 min.</td>
</tr>
<tr>
<td>6</td>
<td>Import your configuration data into Security Manager. Validate the migration. (Optional)</td>
<td>2-4 hours (avg) - based on size of Express database</td>
</tr>
<tr>
<td>7</td>
<td>Perform any necessary post-migration steps. Remove your previous NetScreen management software version. (Optional)</td>
<td>45 minutes</td>
</tr>
</tbody>
</table>
Installing Security Manager Using New Hardware

It is possible to extend system performance by installing Security Manager onto new hardware that exceeds the prescribed minimum system requirements. The following table details the migration and installation process if you plan to install the Security Manager management system using new hardware. It also provides an estimate of the overall amount of time each step requires.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Time required</th>
</tr>
</thead>
</table>
| 1    | Copy the required software to install the Security Manager management system on the server(s) where you plan to install the Security Manager GUI Server and Device Server.  
Copy the Global PRO data export utility installer to your existing Global PRO Express appliance.  
Copy the Security Manager user interface installer to the computer where you plan to install the UI. | 20 min.       |
| 2    | Install the Security Manager management system.                                                                                               | 5 min.        |
| 3    | Install the Global PRO data export utility installer on your existing Global PRO Express appliance. Run the Global PRO data export utility to export your data from Global PRO Express and the managed FW/VPN devices in your network. The Global PRO data export utility saves the exported data in two files:  
• pmexport.tar for your Policy Manager and device configuration data  
• rmexport.out for your Realtime Monitor data | 2-8 hours     |
| 4    | Transfer both data files to the `/usr/netscreen/GuiSvr/var/migration` subdirectory on the server where you have installed the GUI Server.        | 10 min.       |
| 5    | Install the User Interface.                                                                                                                  | 5 min.        |
| 6    | Launch the UI, and connect it to the management system.                                                                                       | 5 min.        |
| 7    | Import your configuration data into Security Manager. Validate the migration. (Optional)                                                     | 2-4 hours (avg) - based on size of Express database |
| 8    | Perform any necessary post-migration steps. Remove your previous NetScreen management software version. (Optional)                              | 45 minutes    |
Installing Security Manager Using Both Existing and New Hardware

If you are installing the GUI Server and Device Server on separate servers, and you wish to use both your existing hardware and new hardware, install the GUI Server on your existing Global PRO Express appliance and the Device Server on new hardware.

The following table details the migration and installation process if you plan to install the GUI Server on your existing Global PRO Express appliance and the Device Server using new hardware. It also provides an estimate of the overall amount of time each step requires.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Copy the required software to install the Security Manager management system (for Solaris) on your existing Global PRO Express appliance. Copy the required software for the user interface to the Windows-based PC where you plan to install the UI.</td>
<td>20 min.</td>
</tr>
<tr>
<td>2</td>
<td>Run the management system installer (for Solaris) on your existing Global PRO Express appliance to install the GUI Server. The installer automatically detects if you have Global PRO Express installed on the appliance. It then installs and runs the Global PRO data export utility automatically. The Global PRO data export utility exports your data from Global PRO Express and the managed FW/VPN devices in your network, and then saves the exported data in two files: pmexport.tar for your Policy Manager and device configuration data; rmexport.out for your Realtime Monitor data.</td>
<td>10 min.</td>
</tr>
<tr>
<td>3</td>
<td>Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server.</td>
<td>10 min.</td>
</tr>
<tr>
<td>4</td>
<td>Run the management system installer (for Linux or Solaris) on a new server to install the Device Server.</td>
<td>10 min.</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface.</td>
<td>5 min.</td>
</tr>
<tr>
<td>6</td>
<td>Start the UI and connect it to the management system.</td>
<td>5 min.</td>
</tr>
<tr>
<td>7</td>
<td>Import your configuration data into Security Manager. Validate the migration. (Optional) 2-4 hours (avg) - based on size of Express database</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Perform any necessary post-migration steps. Remove your previous NetScreen management software version. (Optional)</td>
<td>45 minutes</td>
</tr>
</tbody>
</table>
Migration Scenarios Not Supported

Security Manager does not support the installation and migration over existing NetScreen-IDP devices.

Migration Path

To migrate data from your previous version of Global PRO Express, you must be running at least version 4.1.3. Customers running a previous version of Global PRO Express must upgrade to version 4.1.3 before migrating to Security Manager.

Supported Devices

The Global PRO data export utility does not support the migration of devices running a version of ScreenOS not supported by Security Manager. If you have devices in Global PRO Express that are not supported by Security Manager, you need to delete these devices from Global PRO Express before beginning the export process. Refer to Appendix A “Technical Overview” for a description of all the FW/VPN devices and versions of ScreenOS supported by Security Manager.

If the Global PRO data export utility detects a FW/VPN device configured in Global PRO Express, that is running a non-supported version of ScreenOS (i.e., ScreenOS 3.0.3), it reports the error and continues to export the next FW/VPN device.
Pre-Migration Steps

Before you begin the process of installing Security Manager, you need to perform several manual steps to ensure that your data in Global PRO Express is current.

To ensure that your devices are properly migrated, it is recommended that you:

- Perform an AutoDetect operation for all managed devices to verify they are all connected and online. This also verifies the Serial # and ScreenOS version information on the device.
- Perform a Delta Configuration Summary for all managed devices to verify that there are no discrepancies between the configuration information in Express and on the device.
- Verify that all virtual systems are connected during the export process.
- Verify all information for all "modeled" devices. These are devices that you may have configured in Global PRO Express, but are not currently managing. During the migration, configuration information for your "modeled" devices is derived from a Configuration Summary. Because this information is not validated, you may consider deleting these devices from Global PRO Express before you begin the migration process.
- Verify that there are no instances of cyclic containmentship in user, address and service objects in Policy Manager. Cyclic containmentship exists when objects are configured as members of themselves. For example, if you have three service objects, one named Service A, another named Service B, and another named Service C. If you have a scenario where Service A contains Service B, and Service B contains C, and C contains A, the migration fails.
INSTALLING THE MANAGEMENT SYSTEM

The management system installer provides several options allowing you to install, configure and run the following:

- Global PRO data export utility
- GUI Server and Device Server
- GUI Server only
- Device Server only

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address and port of the GUI Server</td>
<td>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.</td>
</tr>
<tr>
<td>Initial &quot;super&quot; user password</td>
<td>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.</td>
</tr>
</tbody>
</table>
| GUI Server data directory                | 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:          

/var/netscreen/GuiSvr/  

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. |
| Device Server data directory             | Directory location where device data on the Device Server is stored. By default, the installer stores data on the Device Server in:  

/var/netscreen/DevSvr/  

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. |
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 -
   ```

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Database Backup Directory</td>
<td>Directory location where backup data on the server is stored. By default, the installer stores data in: /var/netscreen/dbbackup/</td>
</tr>
<tr>
<td>Tool Configuration Directory (Optional)</td>
<td>Directory location where configuration data for the automatic backup tool is stored. By default, the installer stores data in: /var/netscreen/iHaSvr/</td>
</tr>
<tr>
<td>Path to the rsync Utility Package</td>
<td>Directory location where the rsync utility package is stored. This utility is required by the automatic database backup tool. The package is typically stored in: /usr/bin/rsync/</td>
</tr>
<tr>
<td>Automatic Database Backup Time</td>
<td>Time of day that you wish the automatic database backup utility to begin the daily backup process. You must enter a 2 digit number representing the time of day in military time (00-23). For example, if you want the backup to begin at 4:00am, enter 04; if at 4:00pm, enter 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. By default, the utility begins the daily backup process at 2:00am every day. Refer to Automatic Database Backup Option in Chapter 5 for more information on the automatic database backup process.</td>
</tr>
<tr>
<td>Number of Automatic Database Backup Files Stored</td>
<td>Total number of database backup files that the automatic database backup utility stores. By default, the utility stores seven (7) backup files before it begins to overwrite the oldest file.</td>
</tr>
</tbody>
</table>
At the password prompt, enter the root password for the computer.

**Note:** The Security Manager management system runs as the root user. If you wish to run the management system in a more secure mode, refer to “Changing Permissions To a Normal User” on page 76.

3. Partition drives for sufficient disk space to accommodate your planned data requirements.

4. 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:

   ```bash
   rpm -qi rpm
   ```

   For **Red Hat 8.0**, verify that you are running **version 4.1.1, release 1.8x**.
   For **Red Hat 9.0**, verify that you are running **version 4.2, release 1**.
   For **Red Hat Enterprise ES 3.0**, you are required to upgrade the RPM package.

   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. Refer to “Upgrading the RPM Package (For Linux Users Only)” on page 22 for more information.

5. (Optional) If you want the management system to perform automatic database backups, you must verify that you have installed the required Unix client utilities (i.e., rsync and popt) for your version of Linux or Solaris. If these packages are not installed, you must install them first before running the Security Manager management system installer. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 24 for more information.
Other Recommended Actions

It is highly recommended that you disable X server on all the server machines that you plan to install Security Manager. Disabling X server will free up additional server resources for enhanced system performance.

To disable X server on Linux:
1. Navigate to the /etc subdirectory.
2. Open the initab file in any text editor.
3. Comment out the line that refers to /etc/X11/prefdm.
4. Run init q
5. Log out of the graphical console and make sure X does not re-appear.

To disable X server on Solaris, run the following commands:

```
/etc/rc2.d/S99dtlogin stop
mv /etc/rc2.d/S99dtlogin /etc/rc2.d/orig-S99dtlogin
```

Upgrading the RPM Package (For Linux Users Only)

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

To upgrade your version of RPM:
1. Save the system update utility (the file is called system_update_fp1.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 save the utility in the /usr subdirectory.

2. Untar the file. You can do so by running the following command:

   ```
tar xvf system_update_fp1.tar
   ```
A subdirectory called `/systemupdate` is created and all the files required to upgrade your rpm package are extracted into that directory.

3. Navigate to the `/systemupdate` subdirectory where the update script is stored. You can do so by running the following command:
   
   ```bash
   cd /usr/systemupdate
   ```

4. Execute the update script. You can do so by running the following command:
   
   ```bash
   ./update.sh
   ```
5. Press **Enter**. You can also press **Ctrl C** to stop the upgrade process. Let the script run to completion. This may take up to 20 minutes depending upon the number of packages that must be installed.

### Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)

If you want the management system to perform automatic database backups, you must have already installed the required Unix client utilities (i.e., rsync and popt) on your system. These packages are typically installed on Linux systems by default.

If you are installing Security Manager on a Solaris system, and you have not previously installed rsync or popt, you can use the system update utility (the same utility used to upgrade your Linux rpm package) to install the utilities on your system.

Follow the same procedures provided in the previous section to save, untar and run the system update utility.

*Note: After installing rsync, note that you do **not** need to configure the daemon (rsync server).*
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 website.

2. Navigate to the directory where you have saved the management system installer file. It is recommended that you save the management system installer in the \tmp subdirectory.

3. Run the management system installer.

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

\texttt{sh nsm04fp1_servers_linux_x86.sh}

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

\texttt{sh nsm04fp1_servers_sol_sparc.sh}

The installation begins automatically by performing a series of pre-installation checks. The installer ensures that:

\begin{itemize}
\item you are installing the correct software for your operating system
\item all the needed software binaries are present
\item you have correctly logged in as root
\item the system has sufficient disk space and RAM
\end{itemize}

The installer then stops any running servers.

\textit{Note: The management system installer indicates the results of its specific tasks and checks:}

\begin{itemize}
\item “Done” indicates that the installer successfully performed a task.
\item “ok” indicates that the installer performed a check, and verified that the condition was satisfied.
\item “FAILED” indicates that the installer performed a task or check, but it was not successful.
\end{itemize}

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

\textit{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 following graphic depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.

![Installer Running on Linux](image)

The script next prompts if you want the management system to perform an automatic backup of the database on a daily basis. **It is highly recommended that you install the automatic database backup option.**

5. Enter **y** and then press **ENTER** if you want the management system to perform an automatic backup of the database on a daily basis. The script then prompts you to configure options for the backup operation:

   a. Enter the path to the rsync package. The local database backup option requires that you have previously installed the rsync package. If you have not already installed the rsync package, exit the installer and install it. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 24 for more information.

   b. Enter a **two-digit number** (00-23) specifying the hour of day that you wish the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, enter 12; for midnight, enter 00. Press **ENTER** to accept the default setting of 02 or 2:00am.

   c. Enter a directory location where you want the management system to store the database backup locally. Press **ENTER** to accept the default directory location of `/var/netscreen/dbbackup`. 
d. Enter a number (up to 7) specifying how many database backup files the management system stores. Once the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press **ENTER** to accept the default setting of 7 backup files.

If you do not want to backup the database automatically, enter **n** and then press **ENTER**.

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

6. Configure the paths for the directories where you want to store the management system data files:

   a. 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.

   b. 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).
7. If you specified that you want the management system to perform automatic backups, the script also prompts you to enter a directory location where you want the management system to store the configuration settings you have set for the database backup tool. Press ENTER to accept the default setting of /var/netscreen/iHaSvr.

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

8. 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.

9. 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.
10. 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.

11. 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 any applicable migration tasks (disregard since this is a new installation)
- install the Device Server
- install the GUI Server
- install the Database Backup Tool (if applicable)
– 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.

The installer runs for several minutes, and then exits.

Validating Management System Status

If you did not specify the installer to start the server(s) when finished, you must manually start the management system processes.

To validate the management system is started and running properly, it is recommended that you view the status of all the running server processes (i.e., the HA Server, Device Server and GUI Server) to confirm that all services are up and running.

Refer to Chapter 4, Administration for more information on manual commands that you can send to the Device Server, GUI Server, and HA Server.
Installing the Management System On Separate Servers

The process for installing the management system on separate servers is as follows:

1. Perform the pre-requisites steps described as if installing the management system in a basic configuration.
2. 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. Enable and configure automatic database backups (optional).
3. Run the UI installer on a Windows client and install the UI.
4. Launch the UI and create the Device Server. Note the Device ID and one time password that you used when you added the Device Server in Security Manager. You need this information to install the Device Server.
5. Run the management system installer on the server where you want to install the Device Server:
   - Specify that you want to install the Device Server only.
   - Enter the Device ID and one time password that you used when you added the Device Server in Security Manager.
   - Enter the IP address and port number of the running GUI Server.
   - Enable and configure automatic database backups (optional).
6. Start the GUI Server.
7. Start the Device 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.*
**EXPORTING DATA FROM GLOBAL PRO EXPRESS**

If you are installing the management system over existing hardware (for example, if you are installing the management system using your existing Global PRO Express appliance), the management system installer detects if you are running Global PRO Express, and installs and runs the Global PRO data export utility automatically.

If you are installing the management system using new hardware, you must install and run the Global PRO data export utility (nsm04fp1_gpexport_sol_sparc.sh) separately on the Global PRO Express appliance.

For more information on the data export process, refer to Chapter 1, Introduction.

**Transferring the Export Data Files**

Once you have completed the export process, you must transfer these data files to the following subdirectory on the server on which you are installing the Security Manager GUI Server:

```
/usr/netscreen/GuiSvr/var/migration/
```

You need to give the user "nsm" permission to the file (the GUI Server runs as this user). You can do so by running the following command:

```
chmod -R 777 /usr/netscreen/GuiSvr/var/migration/
```

You can then install the User Interface and import the data into Security Manager.
INSTALLING THE USER INTERFACE

The Security Manager User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-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 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.

   If you are installing the UI on a Windows-based PC, you can double-click on the installer executable.

   If you are installing the UI on a Linux-based computer, you can launch it from a command line. From the command line, you can launch the UI installer using the following command:

   ```
   sh nsm04fp1_ui_linux_x86.bin
   ```

   Initially, the following messages appear in the Linux terminal.
An Introduction screen for the InstallAnywhere wizard appears.

Follow the wizard through all the steps required to configure and install the UI. Click **Next** to continue the installation. The License Agreement screen appears.

4. Review the License Agreement carefully. If you choose to accept the terms of the License Agreement, click the button next to the appropriate statement. Click **Next** to continue.

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

   **Note:** If you are installing on a Windows-based computer, the installer saves the UI software files in C:\Program Files\NetScreen-Security Manager by default. If you are installing on a Linux-based computer, the installer saves the UI software files in /root/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**.

   On Windows-based computers, the Choose Shortcut Folder screen appears.

   On Linux-based computers, the Choose Link Folder screen appears.
6. Select where you would like to create the Security Manager product icons. Or, if you are installing on a Linux-based computer, select where you would like to create links to the Security Manager UI program. Click **Next** to continue. The Pre-Installation Summary screen appears.

7. 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.

8. If you do not have a default web browser configured, the Select Browser screen appears. Use the **Choose** button to navigate to the subdirectory where your web browser software files are located. Click **Next** to continue.
When the installation is complete, a screen indicating “Install Complete” appears.

**Note:** If you do not select a default web browser, the UI will not be able to launch the Security Manager online help. If you still wish to use the online help, you can configure your web browser using the Preferences menu from the UI.

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

**Viewing the Installation Log**

The installer generates a log file with information describing the context of the installation process. For troubleshooting purposes, you may need to access it. The installation log is saved by default in the following directory locations:

For Windows-based computers:

C:\Documents and Settings\<user name>\.nsm\

For Linux-based computers:

/root/.nsm/

**Note:** The .nsm subdirectory is a hidden subdirectory on Linux systems.

The Installation log file is named:

_out.<date/time stamp>.dat

**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.

   If you are running the UI on a Windows-based PC, you can double-click on the NetScreen-Security Manager icon.
If you are running the UI on a Linux-based computer, you can either launch it by double-clicking on the NetScreen-Security Manager application icon (specify that you want to run the program) or you can launch it from a command line. From the command line, navigate to the subdirectory where you have installed the UI software files, and then run the UI application shell archive script. The Login window will appear.

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.

## 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 appears
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 select **Edit** to view all information available on the Device Server.

![Device Server Configuration](image)

4. Use the **General** tab to verify the following information:
   - **Mapped IP address** - the IP address that is manually defined in the UI.
   - **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.

   **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.

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. 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**.
IMPORTING DATA INTO SECURITY MANAGER

Once you have completed installing the User Interface, you can launch the UI and import configuration data previously exported from Global PRO Express into Security Manager.

Import Process

You can run the import process multiple times without corrupting the Security Manager database. The import of Policy Manager and Realtime Monitor data can be done at the same time or separately.

If you are planning on importing data from both Policy Manager and Realtime Monitor, it is highly recommended that you perform the import of data from Policy Manager before or at the same time as you import your data from Realtime Monitor. This is because you want to establish your configuration data in Security Manager in the domains that applied in Policy Manager. This configuration data is inherent in Policy Manager. Data configured in Realtime Monitor is not domain-specific.

If you are importing domains individually into Security Manager, it is also highly recommended that you backup your previous installation of Security Manager before running the import. This is to ensure that you can reverse the migration process in the event of an error.

Resolving Domain Name Conflicts

The import identifies all name conflicts before performing the import operation allowing you to determine how to resolve them. Once you have done this, the rest of the migration process can be executed automatically.

During the import, if a domain name already exists in Security Manager (i.e., from a previous domain import), the import utility does not merge the two domains with the same name. The import utility prompts the user to resolve the name conflict. You can resolve the domain name conflict by choosing one of the following options:

- Rename the Policy Manager domain
- Rename the existing domain in the Security Manager database
- Overwrite the existing domain with the Policy Manager domain
- Do not import the Policy Manager domain

The import resolves conflicts by not importing the new domain by default. Note that the import utility does not try to merge two domains with the same name.

Because there is no concept of domains in Realtime Monitor, users and user groups are imported to the global domain only. Access privileges associated with your Realtime Monitor users and user groups are not imported. After the migration is completed, you have to create new admin roles for these users and user groups.
Importing Migration Data

Before importing data from Global PRO Express, you must ensure that no other Admins are logged into the system. Any changes made to Security Manager system during the migration process will result in database corruption.

To import data from Global PRO Express:

1. From the Tools menu, select Import Global PRO. A window appears prompting you to specify the type of data (i.e., Policy Manager, Realtime Monitor data) that you wish to import and the directory locations where you saved the import files.

2. Click in the appropriate checkbox to select the type of data that you wish to import.

   ![Import Global PRO window](image)

   **Note:** It is recommended that you import your data from Policy Manager first before importing any other data type.

   Click **Next** to continue. The import process begins automatically.

3. Occasionally, name conflicts occur when an import object has the same name as an existing object. If the import tool experiences a name conflict, a window appears prompting you to resolve the name conflict.

   Click in the radio button provided to specify how you want to resolve any name conflicts. Click **Next** to continue. The Admin Role Options window appears next.
4. During the import of administrators from Policy Manager, the administrative permissions for administrators do not map entirely into Security Manager. You need to select whether to give your administrators more access rights or less access rights in Security Manager.

![NetScreen Migrate GlobalPRO](image)

*Note:* If you choose "less access rights", the administrators that you migrate from Global PRO may not have sufficient permissions to perform all the tasks in Security Manager that they were previously allowed to perform.

5. Click **Next** to continue. A window appears indicating the status of the import process.
If the UI performs the import process successfully, no errors are indicated.

If the UI encounters error(s) during the import process, it indicates the error count in the Error and Fatal Error fields provided. Click **Cancel** and the UI rolls back all changes and restores the Security Manager database to its pre-migration state.

6. Click **Finish** to exit the import dialog.

**Rolling Back a Failed Migration**

If you are migrating additional domain information after initially performing an import, and you encounter an error, you need to restore the previous Security Manager database from backup.

**Validating a Successful Migration**

To validate that the migration process completed successfully, you need to perform a delta configuration summary on all devices in the network, and verify that there are no deltas.
POST MIGRATION STEPS

Once you are satisfied that all your data has successfully migrated from Global PRO Express into Security Manager, it is recommended that you perform the following manual post-migration steps:

Manually Configuring Protected Resources

If you wish to configure the server/client parameter in the Security Manager Protected Resource as uni-directional, you need to manually reconfigure this after the migration.

Manually Configuring Authentication Servers

If you do not want an authentication server to be used for a specific purpose in Security Manager, you need to manually disable these purposes (i.e., FWauth, Xauth, L2TP, Policy Manager Auth) after the migration.

Manually Configuring VPNs

If you implemented Hub and Spoke VPNs in Policy Manager, it was possible to control the granularity of your VPN tunnels by defining each tunnel endpoint as a main or branch. In Security Manager, VPN tunnel endpoints are device-specific. Because of this, "branch" VPN tunnels in Security Manager may have greater access to other branch VPN endpoints than they did in Policy Manager. If this occurs, you need to manually configure a firewall policy to deny this traffic.

Transferring Certificate Files

If you plan to continue managing FW/VPN devices running ScreenOS 4.0.X using NACN, you must transfer and load the private key and certificate file packed in PKCS12 into your security database.

To transfer certificate files:

1. On the server where you have installed the Device Server, navigate to the /usr/Netscreen/DevSvr/utils subdirectory.
2. Run the nacnLoadPKCS12 utility. The script prompts you to enter the full path location to the PKCS12 file.
3. Enter the path to the PKCS12 file. The script next prompts you to enter the PKCS12 password.
4. Enter the password. The script next prompts you whether or not you want to set the migration flag on the file.
5. Enter y to set the migration flag, and press Enter to continue. The script runs to completion.
Congratulations! You have just completed migration and 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 FP1 Administrator’s Guide* for information describing how to plan and implement Security Manager for your network.
Migrating and Installing From Global PRO

In This Chapter

- Migration and Installation Scenarios
- Pre-Migration Steps
- Installing the Management System
- Exporting Data From Global PRO
- Installing the User Interface
- Importing Data Into Security Manager
- Post Migration Processes
- Next Steps

This chapter describes the Security Manager migration and installation process for those who have previously used Global PRO. It describes scenarios and procedures for migrating your configuration data from Global PRO and installing Security Manager using new or existing hardware. It also describes how features in Global PRO map to Security Manager, and other considerations to ensure that you have installed Security Manager and migrated data from Global PRO successfully.
Chapter 3 Migrating and Installing From Global PRO

**Migration and Installation Scenarios**

There are multiple options for installing Security Manager if you are currently using Global PRO:

- “Installing Management System Using New Hardware” on page 50
- “Installing Management System Using Existing Hardware” on page 51
- “Considerations If You Are Running Multiple Arbitrators” on page 53
- “Considerations If You Are Running Multiple Data Collectors” on page 54
- “Maintaining Historical Reporting Functionality” on page 54

**Installing Management System Using New Hardware**

It is possible to extend system performance by installing Security Manager onto new hardware that exceeds the prescribed minimum system requirements.

The following table details the migration and installation process if you are using new hardware. It also provides an estimate of the overall amount of time each step requires.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Copy the Security Manager management system installer to the server(s) where you plan to install the Security Manager GUI Server and Device Server. Copy the Security Manager user interface installer to the computer where you plan to install the UI. Copy the Global PRO data export utility installer onto your existing Policy Manager arbitrator and onto the server where you are currently running your Report Manager Master Controller.</td>
<td>20 min.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Security Manager management system.</td>
<td>5 min.</td>
</tr>
<tr>
<td>3</td>
<td>Run the Global PRO data export utility installer (nsm04fp1_gpexport_sol_sparc.sh) on your existing Policy Manager arbitrator. Run the Global PRO data export utility to export your configuration data. Run the Global PRO data export utility installer on your existing Report Manager Master Controller. Run the Global PRO data export utility to export your configuration data. The Global PRO data export utility exports your data from Global PRO and the managed FW/VPN devices in your network, and then saves the exported data in two files: * pmexport.tar for your Policy Manager and device configuration data * rmexport.out for your Realtime Monitor data</td>
<td>2-8 hours</td>
</tr>
</tbody>
</table>
If you wish to use your existing hardware, you can install the Security Manager management system over your existing Global PRO hardware infrastructure. It is recommended that you:

1. Install the Security Manager management system over your existing Policy Manager arbitrator.
2. Install the Security Manager User Interface over your existing Global PRO admin console.

If you plan to install the Security Manager management system on separate servers:

1. Install the Security Manager GUI Server over your existing Global PRO arbitrator.
2. Install the Security Manager Device Server over any one of your other existing Global PRO servers (i.e., master controller, data collector).
3. Install the Security Manager User Interface over your existing Global PRO admin console.

### Installing Management System Using Existing Hardware

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Transfer both data files to the <code>/usr/netscreen/GuiSvr/var/migration</code> subdirectory on the server where you have installed the GUI Server.</td>
<td>10 min.</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface.</td>
<td>5 min.</td>
</tr>
<tr>
<td>6</td>
<td>Start the UI and connect it to the management system.</td>
<td>5 min.</td>
</tr>
<tr>
<td>7</td>
<td>Import your configuration data into Security Manager. Validate the migration. (Optional)</td>
<td>2-4 hours (avg) - based on size of database</td>
</tr>
<tr>
<td>8</td>
<td>Perform any necessary post-migration steps. Remove your previous NetScreen management software version. (Optional)</td>
<td>45 minutes</td>
</tr>
</tbody>
</table>
Chapter 3 Migrating and Installing From Global PRO

The following table details the migration and installation process if you are using existing hardware. It also provides an estimate of the overall amount of time each step requires.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Copy the management system installer (for Solaris) and the Global PRO data export utility installer to your existing Global PRO arbitrator. Copy the Global PRO data export utility installer (nsm04fp1_gpexport_sol_sparc.sh) also to the server where you are currently running your Report Manager Master Controller. Copy the required software for the user interface to the computer where you are currently running the Global PRO admin console.</td>
<td>20 min.</td>
</tr>
<tr>
<td>2</td>
<td>Run the management system installer on your existing Global PRO arbitrator to install the management system. After performing the server install, the installer automatically detects if you are running Global PRO on the arbitrator. If so, it then installs and runs the Global PRO data export utility automatically. The Global PRO data export utility installer exports data configured in Policy Manager and saves your exported data in a file called pmexport.tar. * If you are installing the GUI Server and Device Server on separate servers, run the management system installer to install the GUI Server only. You also need to run the management system installer on another server of your choice to install the Device Server.</td>
<td>2-8 hours</td>
</tr>
<tr>
<td>3</td>
<td>Install the Global PRO data export utility on the server where you are currently running your Report Manager Master Controller. Run the Global PRO data export utility. The Global PRO data export utility exports data configured in Report Manager and saves your exported data in a file called rmexport.out.</td>
<td>2-8 hours</td>
</tr>
<tr>
<td>4</td>
<td>Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server.</td>
<td>10 min.</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface.</td>
<td>5 min.</td>
</tr>
<tr>
<td>6</td>
<td>Start the UI and connect it to the management system.</td>
<td>5 min.</td>
</tr>
<tr>
<td>7</td>
<td>Import your configuration data into Security Manager. Validate the migration. (Optional)</td>
<td>2-4 hours (avg) - based on size of database</td>
</tr>
<tr>
<td>8</td>
<td>Perform any necessary post-migration steps. Remove your previous NetScreen management software version. (Optional)</td>
<td>45 minutes</td>
</tr>
</tbody>
</table>
Considerations If You Are Running Multiple Arbitrators

If you are running multiple arbitrators in Global PRO, you can use any one of the servers that they are running on to install the Security Manager GUI Server.

If you wish to migrate configuration data from Policy Manager, you need to install and run the Global PRO data export utility on one arbitrator, move the export data file to the GUI Server migration directory, and then run the import for that specific data file. You need to follow this process for each arbitrator individually.

The following table details the migration and installation process if you are using existing hardware with multiple arbitrators. It also provides an estimate of the overall amount of time each step requires.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Copy the Security Manager management system installer (for Solaris) and the Global PRO data export utility installer to one of your existing Global PRO arbitrators. Copy the Global PRO data export utility installer also to the other servers running your arbitrators, and to the server where you are currently running your Report Manager Master Controller. Copy the required software for the Security Manager user interface to the computer where you are currently running the Global PRO admin console.</td>
<td>20 min.</td>
</tr>
<tr>
<td>2</td>
<td>Run the management system installer on your existing Global PRO arbitrator to install the management system. After performing the Security Manager server install, the installer automatically detects if you are running Global PRO on the arbitrator. If so, it then installs and runs the Global PRO data export utility automatically. The Global PRO data export utility exports data configured in Policy Manager and saves your exported data in a file called pmexport.tar. * If you are installing the GUI Server and Device Server on separate servers, run the management system installer to install the GUI Server only. You also need to run the management system installer on another server of your choice to install the Device Server.</td>
<td>2-8 hours</td>
</tr>
<tr>
<td>3</td>
<td>Install the Global PRO data export utility on the server where you are currently running your Report Manager Master Controller. Run the Global PRO data export utility. The Global PRO data export utility exports data configured in Report Manager and saves your exported data in a file called rmergeport.out.</td>
<td>2-8 hours</td>
</tr>
<tr>
<td>4</td>
<td>Transfer the rmexport.out file to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server.</td>
<td>10 min.</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface.</td>
<td>5 min.</td>
</tr>
<tr>
<td>6</td>
<td>Start the UI and connect it to the management system.</td>
<td>5 min.</td>
</tr>
</tbody>
</table>
If you have deployed multiple data collectors in Global PRO, you can use any one of the servers that they are running on to install the Security Manager Device Server.

Security Manager does not provide historical reporting functionality. If you have previously used historical reports in Report Manager, you can continue to use it with Security Manager.

To continue using historical reports with Security Manager, you need to continue to maintain the historical reports server, database, and Report Manager Admin Console previously implemented for Report Manager.

The recommended installation process is as follows:

1. Install the GUI Server over your existing Global PRO arbitrator.
2. Install the Device Server over any one of your existing data collectors.

### Considerations If You Are Running Multiple Data Collectors

If you have deployed multiple data collectors in Global PRO, you can use any one of the servers that they are running on to install the Security Manager Device Server.

### Maintaining Historical Reporting Functionality

Security Manager does not provide historical reporting functionality. If you have previously used historical reports in Report Manager, you can continue to use it with Security Manager.

To continue using historical reports with Security Manager, you need to continue to maintain the historical reports server, database, and Report Manager Admin Console previously implemented for Report Manager.

The recommended installation process is as follows:

1. Install the GUI Server over your existing Global PRO arbitrator.
2. Install the Device Server over any one of your existing data collectors.
Migration and Installation Scenarios

You can continue to use the HRS server and database for your historical report data. You will also continue to use the Global PRO Report Manager Admin console to add new devices and admins to the database. You can use any web browser to access historical reports. Refer to the NetScreen-Global PRO Report Manager 4.0 documentation set for more information on using historical reporting.

Migration Scenarios Not Supported

Security Manager does not support the installation and migration over existing IDP devices nor over existing PRO deployments where devices exist behind a port NAT.

Migration Path

To migrate data from your previous version of Global PRO, you must be running at least version 4.1.3. Customers running a previous version of Global PRO must upgrade to version 4.1.3, before migrating to Security Manager.

Supported Devices

The Global PRO data export utility does not support the migration of devices running a version of ScreenOS not supported by Security Manager. If you have devices in Global PRO that are not supported by Security Manager, you need to delete these devices from Global PRO before beginning the export process. Refer to Appendix A “Technical Overview” for a description of all the FW/VPN devices and versions of ScreenOS supported by Security Manager.

If the Global PRO data export utility detects a FW/VPN device configured in Global PRO, that is running a non-supported version of ScreenOS (i.e., ScreenOS 3.0.3), it reports the error and continues to export the next FW/VPN device.
Before you begin the process of installing Security Manager, you need to perform several manual steps to ensure that your data in Global PRO Express is current.

To ensure that your devices are properly migrated, it is recommended that you:

- Perform an **AutoDetect** operation for all managed devices to verify they are all connected and online. This also verifies the Serial # and ScreenOS version information on the device.

- Perform a **Delta Configuration Summary** for all managed devices to verify that there are no discrepancies between the configuration information in Express and on the device.

- Verify that all virtual systems are connected during the export process.

- Verify all information for all "modeled" devices. These are devices that you may have configured in Global PRO Express, but are not currently managing. During the migration, configuration information for your "modeled" devices is derived from a Configuration Summary. Because this information is not validated, you may consider deleting these devices from Global PRO Express before you begin the migration process.

- Verify that there are no instances of cyclic containment in user, address and service objects in Policy Manager. Cyclic containment exists when objects are configured as members of themselves. For example, if you have three service objects, one named Service A, another named Service B, and another named Service C. If you have a scenario where Service A contains Service B, and Service B contains C, and C contains A, the migration fails.
INSTALLING THE MANAGEMENT SYSTEM

The management system installer provides several options allowing you to install and configure each management system component.

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.

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address and port of the GUI Server</td>
<td>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.</td>
</tr>
<tr>
<td>Initial &quot;super&quot; user password</td>
<td>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.</td>
</tr>
</tbody>
</table>
| GUI Server data directory                      | 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:  

/var/netscreen/GuiSvr/  

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. |
| Device Server data directory                   | Directory location where device data on the Device Server is stored. By default, the installer stores data on the Device Server in:  

/var/netscreen/DevSvr/  

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. |
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:

   \texttt{su -}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Database Backup Directory (Optional)</td>
<td>Directory location where backup data on the server is stored. By default, the installer stores data in: [ /var/netscreen/dbbackup/ ]</td>
</tr>
<tr>
<td>Automatic Database Backup Tool Configuration Directory (Optional)</td>
<td>Directory location where configuration data for the automatic backup tool is stored. By default, the installer stores data in: [ /var/netscreen/iHaSvr/ ]</td>
</tr>
<tr>
<td>Path to the rsync Utility Package</td>
<td>Directory location where the rsync utility package is stored. This utility is required by the automatic database backup tool. The package is typically stored in: [ /usr/bin/rsync/ ]</td>
</tr>
<tr>
<td>Automatic Database Backup Time</td>
<td>Time of day that you wish the automatic database backup utility to begin the daily backup process. You must enter a 2 digit number representing the time of day in military time (00-23). For example, if you want the backup to begin at 4:00am, enter 04; if at 4:00pm, enter 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. By default, the utility begins the daily backup process at 2:00am every day. Refer to Automatic Database Backup Option in Chapter 5 for more information on the automatic database backup process.</td>
</tr>
<tr>
<td>Number of Automatic Database Backup Files Stored</td>
<td>Total number of database backup files that the automatic database backup utility stores. By default, the utility stores seven (7) backup files before it begins to overwrite the oldest file.</td>
</tr>
</tbody>
</table>
At the password prompt, enter the root password for the computer.

**Note:** The Security Manager management system runs as the root user. If you wish to run the management system in a more secure mode, refer to “Changing Permissions To a Normal User” on page 76.

3. Partition drives for sufficient disk space to accommodate your planned data requirements.

4. 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 **Red Hat 8.0**, verify that you are running version **4.1.1, release 1.8x**.
   For **Red Hat 9.0**, verify that you are running version **4.2, release 1**.
   For **Red Hat Enterprise ES 3.0**, you are required to upgrade the RPM package.

   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. Refer to “Upgrading the RPM Package (For Linux Users Only)” on page 60 for more information.

5. (Optional) If you want the management system to perform automatic database backups, you must verify that you have installed the required Unix client utilities (i.e., rsync and popt) for your version of Linux or Solaris. If these packages are not installed, you must install them first before running the Security Manager management system installer. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 62 for more information.
Other Recommended Actions

It is highly recommended that you disable X server on all the server machines that you plan to install Security Manager. Disabling X server will free up additional server resources for enhanced system performance.

To disable X server on Linux:

1. Navigate to the /etc subdirectory.
2. Open the initab file in any text editor.
3. Comment out the line that refers to /etc/X11/prefdm.
4. Run init q
5. Log out of the graphical console and make sure X does not re-appear.

To disable X server on Solaris, run the following commands:

```
/etc/rc2.d/S99dtlogin stop

mv /etc/rc2.d/S99dtlogin /etc/rc2.d/orig-S99dtlogin
```

Upgrading the RPM Package (For Linux Users Only)

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

To upgrade your version of RPM:

1. Save the system update utility (the file is called system_update_fp1.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 save the utility in the /usr subdirectory.

2. Untar the file. You can do so by running the following command:

   `tar xvf system_update_fp1.tar`
A subdirectory called /systemupdate is created and all the files required to upgrade your rpm package are extracted into that directory.

3. Navigate to the /systemupdate subdirectory, where the update script is stored. You can do so by running the following command:
   ```bash
cd /usr/systemupdate
   ```

4. Execute the update script. You can do so by running the following command:
   ```bash
./update.sh
   ```
The script prompts you to press **Enter** to continue.

5. Press **Enter**. You can also press **Ctrl C** to stop the upgrade process. Let the script run to completion. This may take up to 20 minutes depending upon the number of packages that must be installed.

### Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)

If you want the management system to perform automatic database backups, you must have already installed the required Unix client utilities (i.e., rsync and popt) on your system. These packages are typically installed on Linux systems by default.

If you are installing Security Manager on a Solaris system, and you have not previously installed rsync or popt, you can use the system update utility (the same utility used to upgrade your Linux rpm package) to install the utilities on your system.

Follow the same procedures provided in the previous section to save, untar and run the system update utility.

*Note: After installing rsync, note that you do **not** need to configure the daemon (rsync server).*
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 website.

2. Navigate to the directory where you have saved the management system installer file. It is recommended that you save the management system installer in the /tmp subdirectory.

3. Run the management system installer.

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

   sh nsm04fp1_servers_linux_x86.sh

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

   sh nsm04fp1_servers_sol_sparc.sh

   The installation begins automatically by performing a series of pre-installation checks. The installer ensures 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 following graphic depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.

![Installer running on Linux](image)

The script next prompts if you want the management system to perform an automatic backup of the database on a daily basis. It is highly recommended that you install the automatic database backup option.

5. Enter y and then press ENTER if you want the management system to perform an automatic backup of the database on a daily basis. The script then prompts you to configure options for the backup operation:

   a. Enter the path to the rsync package. The local database backup option requires that you have previously installed the rsync package. If you have not already installed the rsync package, exit the installer and install it. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 62 for more information.

   b. Enter a two-digit number (00-23) specifying the hour of day that you wish the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, enter 12; for midnight, enter 00. Press ENTER to accept the default setting of 02 or 2:00am.

   c. Enter a directory location where you want the management system to store the database backup locally. Press ENTER to accept the default directory location of /var/netscreen/dbbackup.
d. Enter a number (up to 7) specifying how many database backup files the management system stores. Once the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press ENTER to accept the default setting of 7 backup files.

If you do not want to backup the database automatically, enter n and then press ENTER.

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

6. Configure the paths for the directories where you want to store the management system data files:
   a. 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.
   b. 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).
7. If you specified that you want the management system to perform automatic backups, the script also prompts you to enter a directory location where you want the management system to store the configuration settings you have set for the database backup tool. Press **ENTER** to accept the default setting of `/var/netscreen/iHaSvr`.

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

8. 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.

9. 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.
10. 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.

11. 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 any applicable migration tasks (disregard since this is a new installation)
- install the Device Server
- install the GUI Server
- install the Database Backup Tool (if applicable)
– 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.

<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>View</th>
<th>Terminal</th>
<th>Go</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extracting payloads</td>
<td>Extracting payload</td>
<td>Decompressing payload</td>
<td>gzip: payload.tgz: unexpected end of file</td>
<td>ok</td>
<td>ok</td>
</tr>
</tbody>
</table>

########## PERFORMING MIGRATION 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
Creating /var/netscreen/dbbackup | ok
Putting NSROOT into start scripts | ok
Filling in config file(s) | ok
Restarting xinetd service | ok
Installation of Device Server complete.

----- INSTALLING GUI Server -----
Looking for existing RPM package | ok
Removing GUI files from default location | ok
Installing GUI Server RPM | ok
Installing JRE | ok
Creating var directory | ok
Clearing contents of /var/netscreen/dbbackup | ok
Putting NSROOT into start scripts | ok
Filling in config file(s) | ok
Setting permissions for GUI Server | ok
Running generateWPK utility | ok
Running fingerprintWPK utility | ok
Installation of GUI Server complete.
Several messages display to confirm the installation progress.

The installer runs for several minutes, and then exits.

**Validating Management System Status**

If you did not specify the installer to start the server(s) when finished, you must manually start the management system processes.

To validate the management system is started and running properly, it is recommended that you view the status of all the running server processes (i.e., the HA Server, Device Server and GUI Server) to confirm that all services are up and running.

Refer to Chapter 4, Administration for more information on manual commands that you can send to the Device Server, GUI Server, and HA Server.

**Installing the Management System On Separate Servers**

The process for installing the management system on separate servers is as follows:
1. Perform the pre-requisites steps described as if installing the management system in a basic configuration.

2. 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. Enable and configure automatic database backups (optional).

3. Run the UI installer on a Windows client and install the UI.

4. Launch the UI and create the Device Server. Note the Device ID and one time password that you used when you added the Device Server in Security Manager. You need this information to install the Device Server.

5. Run the management system installer on the server where you want to install the Device Server:
   - Specify that you want to install the Device Server only.
   - Enter the Device ID and one time password that you used when you added the Device Server in Security Manager.
   - Enter the IP address and port number of the running GUI Server.
   - Enable and configure automatic database backups (optional).

6. Start the GUI Server.

7. Start the Device 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.
**EXPORTING DATA FROM GLOBAL PRO**

If you are installing the management system over existing hardware (for example, if you are installing the management system using your existing Global PRO arbitrator), the management system installer detects if you are running Global PRO, and installs and runs the Global PRO data export utility automatically.

If you are installing the management system using new hardware, you must install and run the Global PRO data export utility (`nsm04fp1_gpexport_sol_sparc.sh`) separately on the Global PRO arbitrator and Report Manager Master Controller.

**Policy Manager Export Data**

Recall that for Policy Manager, you run the Global PRO data export utility on your existing Policy Manager arbitrator. The utility proceeds as follows:

- extracts configuration data from the local LDAP server
- attempts to contact each individual managed device for the latest device configuration data. If utility is successful in connecting to the device, it downloads the device configuration directly from the device. If the utility is not successful in connecting to the device, it extracts the device configuration from the latest configuration summary generated for the device in Policy Manager.

When it has completed this process, the Global PRO data export utility saves the export data in the following location:

```
/usr/netscreen/var/migration/pmexport.tar
```

**Report Manager Export Data**

Recall that for Report Manager, you run the Global PRO data export utility on your existing Report Manager master controller. The utility extracts configuration data from the Report Manager database and saves it in the following location:

```
/usr/netscreen/var/migration/RMexport.out
```

**Transferring the Export Data Files**

Once you have completed the export process, you must transfer these data files to the following subdirectory on the server on which you are installing the Security Manager GUI Server:

```
/usr/netscreen/GuiSvr/var/migration/
```

You need to give the user "nsm" permission to the file (the GUI Server runs as this user). You can do so by running the following command:

```
chmod -R 777 /usr/netscreen/GuiSvr/var/migration/
```

You can then install the User Interface and import the data into Security Manager.
INSTALLING THE USER INTERFACE

The Security Manager User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-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 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.

   If you are installing the UI on a Windows-based PC, you can double-click on the installer executable.

   If you are installing the UI on a Linux-based computer, you can launch it from a command line. From the command line, you can launch the UI installer using the following command:

   sh nsm04fp1_ui_linux_x86.bin

Initially, the following messages appear in the Linux terminal.
An Introduction screen for the InstallAnywhere wizard appears.

Follow the wizard through all the steps required to configure and install the UI. Click **Next** to continue the installation. The License Agreement screen appears.

4. Review the License Agreement carefully. If you choose to accept the terms of the License Agreement, click the button next to the appropriate statement. Click **Next** to continue.

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

   **Note:** If you are installing on a Windows-based computer, the installer saves the UI software files in C:\Program Files\NetScreen-Security Manager by default. If you are installing on a Linux-based computer, the installer saves the UI software files in /root/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**.

   On Windows-based computers, the Choose Shortcut Folder screen appears. On Linux-based computers, the Choose Link Folder screen appears.
6. Select where you would like to create the Security Manager product icons. Or, if you are installing on a Linux-based computer, select where you would like to create links to the Security Manager UI program. Click Next to continue. The Pre-Installation Summary screen appears.

7. 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.

8. If you do not have a default web browser configured, the Select Browser screen appears. Use the Choose button to navigate to the subdirectory where your web browser software files are located. Click Next to continue.
When the installation is complete, a screen indicating “Install Complete” appears.

**Note:** If you do not select a default web browser, the UI will not be able to launch the Security Manager online help. If you still wish to use the online help, you can configure your web browser using the Preferences menu from the UI.

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

### Viewing the Installation Log

The installer generates a log file with information describing the context of the installation process. For troubleshooting purposes, you may need to access it. The installation log is saved by default in the following directory locations:

For Windows-based computers:

C:\Documents and Settings\<user name>\.nsm\n
For Linux-based computers:

/root/.nsm/

**Note:** The .nsm subdirectory is a hidden subdirectory on Linux systems.

The Installation log file is named:

_out.<date/time stamp>.dat

### 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.

   If you are running the UI on a Windows-based PC, you can double-click on the NetScreen-Security Manager icon.
If you are running the UI on a Linux-based computer, you can either launch it by double-clicking on the NetScreen-Security Manager application icon (specify that you want to run the program) or you can launch it from a command line. From the command line, navigate to the subdirectory where you have installed the UI software files, and then run the UI application shell archive script. The Login window will appear.

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.

**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 appears

2. Select the Servers node. The Servers view displays Device Server and GUI Server information.
3. Select the Device Server and click the **Edit** icon or right-click the Device Server and select **Edit** to view all information available on the Device Server.

4. Use the **General** tab to verify the following information:
   - **Mapped IP address** - the IP address that is manually defined in the UI.

   **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. 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.
**IMPORTING DATA INTO SECURITY MANAGER**

Once you have completed installing the Security Manager User Interface, you can use launch the UI and import configuration data previously exported from Global PRO into Security Manager.

**Import Process**

Note that you can run the import process multiple times without corrupting the Security Manager database. The import of Policy Manager and Report Manager data can be done at the same time or separately. It is highly recommended that you perform the import of Policy Manager data before or at the same time as the import of Report Manager data. This is because you want to establish your configuration data in Security Manager in the domains that applied in Policy Manager. This configuration data is inherent in Policy Manager. Data configured in Report Manager is not domain-specific.

If you are importing domains individually into Security Manager, it is also highly recommended that you backup your previous installation of Security Manager before running the import. This is to ensure that you can reverse the migration process in the event of an error.

**Resolving Domain Name Conflicts**

The import identifies all name conflicts before performing the import operation allowing you to determine how to resolve them. Once you have done this, the rest of the migration process can be executed automatically.

During the import, if a domain name already exists in Security Manager (i.e., from a previous domain import), the import utility does not try to merge the two domains with the same name. The import utility prompts the user to resolve the name conflict. You can resolve the domain name conflict by choosing one of the following options:

- Rename the Policy Manager domain
- Rename the existing domain in the Security Manager database
- Overwrite the existing domain with the Policy Manager domain
- Do not import the Policy Manager domain

The import resolves conflicts by not importing the new domain by default. Note that the import utility does not try to merge two domains with the same name.

Because there is no concept of domains in Report Manager, users and user groups are imported to the global domain only. Access privileges associated with your Report Manager users and user groups are not imported. After the migration is completed, you have to create new admin roles for these users and user groups.

**Import Migration Data**

Before importing data from Global PRO, you must ensure that no other Admins are logged into the system. Any changes made to Security Manager system during the migration process will result in database corruption.
To import data from Global PRO:

1. From the **Tools** menu, select **Import Global PRO**. A window appears prompting you to specify the type of data (i.e., Policy Manager, Realtime Monitor data) that you wish to import.

![Import Global PRO Window](image)

2. Click in the appropriate checkbox to select the type of data that you wish to import.

   **Note:** It is recommended that you import your data from **Policy Manager** first before importing any other data type.

   Click **Next** to continue. The import process begins automatically.

3. Occasionally, name conflicts occur when an import object has the same name as an existing object. If the import tool experiences a name conflict, a window appears prompting you to resolve the name conflict.

   Click **Next** to continue. The Admin Role Options window appears next.
4. During the import of administrators from Policy Manager, the administrative permissions for administrators do not map entirely into Security Manager. You need to select whether to give your administrators more access rights or less access rights in Security Manager.

![NetScreen Migrate GlobalPRO](image)

**Note:** If you choose "less access rights", the administrators that you migrate from Global PRO may not have sufficient permissions to perform all the tasks in Security Manager that they were previously allowed to perform.

5. Click **Next** to continue. A window appears indicating the status of the import process.

![NetScreen Migrate GlobalPRO](image)
If the UI performs the import process successfully, no errors are indicated.

If the UI encounters error(s) during the import process, it indicates the error count in the Error and Fatal Error fields provided. Click Cancel and the UI rolls back all changes and restores the Security Manager database to its pre-migration state.

6. Click Finish to exit the import dialog.

Rolling Back a Failed Migration

If you are migrating additional domain information after initially performing an import, and you encounter an error, you need to restore the previous Security Manager database from backup.

Validating a Successful Migration

To validate that the migration process completed successfully, you need to perform a delta configuration summary on all devices in the network, and verify that there are no deltas.
**POST MIGRATION PROCESSES**

Once you are satisfied that all your data has successfully migrated from Global PRO into Security Manager, it is recommended that you perform the following manual post-migration steps:

**Historical Reporting**

If you plan to continue to use Historical Reports with Security Manager, it is very important that you restart the GUI Server after performing the Global PRO import. The restart enables the forwarding of device statistics to the HRS database.

**Manually Configuring Protected Resources**

If you wish to configure the server/client parameter in the Security Manager Protected Resource as uni-directional, you need to manually reconfigure this after the migration.

**Manually Configuring Authentication Servers**

If you do not want an authentication server to be used for a specific purpose in Security Manager, you need to manually disable these purposes (i.e., FWauth, Xauth, L2TP, Policy Manager Auth) after the migration.

**Manually Configuring VPNs**

If you implemented Hub and Spoke VPNs in Policy Manager, it was possible to control the granularity of your VPN tunnels by defining each tunnel endpoint as a main or branch. In Security Manager, VPN tunnel endpoints are device-specific. Because of this, "branch" VPN tunnels in Security Manager may have greater access to other branch VPN endpoints than they did in Policy Manager. If this occurs, you need to manually configure a firewall policy to deny this traffic.

**Transferring Certificate Files**

If you plan to continue managing FW/VPN devices running ScreenOS 4.0.X using NACN, you must transfer and load the private key and certificate file used in your previous NetScreen management deployment. During the migration process, these files are stored in a file called PKCS12 in your security database. To transfer and load these files for use in Security Manager, you must manually run the nacnLoadPKCS12 utility.

To transfer your previous private key and certificate files:

1. Login to the computer where you are running the Device Server.
2. Navigate to the /usr/Netscreen/DevSvr/utils subdirectory.
3. Run the nacnLoadPKCS12 utility. The script prompts you to enter the full path location to the PKCS12 file.
4. Enter the path to the PKCS12 file. The script next prompts you to enter a password allowing you to access the PKCS12 file.

\textbf{Note}: \textit{The default password for the PKCS12 file is “production”}.

5. Enter the password. The script next prompts you whether or not you want to set the migration flag on the file. When set to “y”, the migration flag enables FW/VPN devices using NACN to properly load your old private key and certificate file.

6. Enter \texttt{y} to set the migration flag, and press \texttt{Enter} to continue. The script runs to completion.

\textbf{Note}: \textit{If you do not set the migration flag to “y”, FW/VPN devices using NACN will use the newly created private key and certificate file generated during the Security Manager installation.}

### Disabling the Realtime Monitor Console

If you are planning on using historical reports, you will need to maintain the Realtime Admin Console to add new devices and users. You do not however, need to continue to use the Monitor Console. It is recommended that you disable the Monitor Console.

To disable the Realtime Monitor Console:

1. Open the \texttt{pro.admin.init} file in any text editor. The \texttt{pro.admin.init} file is located in the Report Manager console installation directory (e.g., \texttt{C:\Program Files\NetScreen\Report Manager\Console\}).
2. Edit the value that appears for the “pro.admin.monitoring.enable” parameter to “false”.
3. Save the file.

### Disabling Historical Reporting

If you do not plan to use historical reporting with Security Manager, it is recommended that you disable forwarding of information from the Master Controller to the Report Manager database.

To disable MC forwarding:

1. Open the Report Manager export data file in any text editor - before performing the import.
2. Delete the line containing the “db_ip_address” parameter.
3. Save the file.
Congratulations! You have just completed migration and 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 FP1 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
- Archiving and Restoring Logs and Configuration Data
- Automatic Database Backup Option
- 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, GUI Server, or HA Server, and issuing a manual command.

The management system supports the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>sends a hangup signal to the management system process, then instructs the process to reload its configuration and start again.</td>
</tr>
<tr>
<td>restart</td>
<td>stops the management system process for 2 seconds, then restarts the process.</td>
</tr>
<tr>
<td>start</td>
<td>starts the management system process</td>
</tr>
<tr>
<td>stop</td>
<td>stops the management system process</td>
</tr>
<tr>
<td>status</td>
<td>provides a status of the management system process</td>
</tr>
<tr>
<td>version</td>
<td>lists the current version of the management system</td>
</tr>
</tbody>
</table>

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
   ```

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

1. Navigate to the HA Server bin subdirectory (i.e., /usr/netscreen/iHaSvr/bin).
2. Run the following command:
   ```
   ./iHaSvr.sh
   ```
**Starting Server Processes**

You can manually start each server process as follows.

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:
   
   ```bash
   ./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.*

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:
   
   ```bash
   ./devSvr.sh start
   ```

To start the HA Server process manually:
1. Navigate to the HA Server bin subdirectory (i.e., `/usr/netscreen/iHaSvr/bin`).
2. Run the following command:
   
   ```bash
   ./iHaSvr.sh start
   ```

*Note: If you start the HA Server process, it automatically starts the GUI Server and Device Server processes.*

**Stopping Server Processes**

You can manually stop each server process as follows.

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:
   
   ```bash
   ./guiSvr.sh stop
   ```

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

1. Navigate to the HA Server bin subdirectory (i.e., `/usr/netscreen/iHaSvr/bin`).
2. Run the following command:
   ```
   ./iHaSvr.sh stop
   ```
MAINTAINING THE MANAGEMENT SYSTEM

The following procedures are provided for your reference:

- “Changing the Management System IP Address” on page 91
- “Changing the Device Server IP Address” on page 91
- “Changing the GUI Server IP Address” on page 92
- “Changing Permissions To a Normal User” on page 92
- “Uninstalling the User Interface” on page 101

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.
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 the IP Address 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.
4. Login to the server where you are running the GUI Server as root.
6. Open the server_table.nml file in any text editor.
7. Edit the values for the IP Address 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.
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. Save the file.
5. Login to the server where you are running the GUI Server as root.
7. Open the server_table.nml file in any text editor.
8. Edit the values for the IP Address in the GUI Server section only. Save the file.
9. Restart the GUI Server, then restart the Device Server.

**Changing Permissions To a Normal User**

The Security Manager management system runs by default as the root user. If you want change this default behavior to a more secure setup, you can create a normal user (i.e., called “nsm”), and change permissions to that user. For your convenience, a script called “setperms.sh” is included for both the Device Server and GUI Server that will automatically change the setuid.user value in case they want to switch to the more secure setup.

*Note: You cannot change permissions and run the HA Server as any user other than root. You must run the HA Server as root.*

To create a normal user and change permissions:

1. Stop the Device Server. For example, you can do this by running the following command:
   ```bash
cd /usr/netscreen/DevSvr/bin
./devSvr.sh stop
   ```
2. Stop the GUI Server. For example, you can do this by running the following command:
   ```bash
cd /usr/netscreen/GuiSvr/bin
./guiSvr.sh stop
   ```
3. Create a normal user called “nsm”. Create a group called “nsm”, with the user nsm as the only member.

You can do this by typing the following commands:

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

4. Run the change permissions script on the Device Server. For example, you would run the following command:

```
/usr/netscreen/DevSvr/utils/setperms.sh DevSvr
```

5. Run the change permission script on the GUI Server. For example, you would run the following command:

```
/usr/netscreen/GuiSvr/utils/setperms.sh GuiSvr
```

6. Start the GUI Server.
7. Start the Device Server
8. Verify that the permissions you set are working correctly. One way to check is to verify that the NSM servers can write to disk. You can do this by adding a new device and seeing if it appears in the device table file.

---

**Uninstalling the Management System**

To uninstall previous management system installations:

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

```
cd /usr/netscreen/DevSvr/bin
./devSvr.sh stop
```

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

```
cd /usr/netscreen/GuiSvr/bin
./guiSvr.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
```
Archiving and Restoring Logs and Configuration Data

You can archive and retrieve log and configuration data in Security Manager using standard Unix commands. Logs reside on the Device Server. All other configuration information, including device configuration data, administrators, policies, audit logs and job information resides on the GUI Server.

Before you begin archiving, it is important that you first stop the processes running on both servers. After you have stopped both servers, use the “ls -al” command to identify the actual paths of the GUI Server and Device Server data directories. You should issue this command on the following directory locations:

- For all information on the GUI Server: /usr/netscreen/GuiSvr/var
- For all information on the Device Server: /usr/netscreen/DevSvr/var

These directories are links representing paths that are entered at the time you installed the server.

After you have completed archiving, restart both server processes.

Archiving Logs and Configuration Data

To archive log and configuration data:

1. Stop the Device Server.
2. Stop the GUI Server.
3. Use the "ls -al" command to discover the actual paths of the GUI Server and Device Server data directories. These are the directories that you need to back up. For example:
   ```
   ls -al /usr/netscreen/GuiSvr/var
   lrwxrwxrwx 1 root root 21 Feb 25 16:04 /usr/netscreen/GuiSvr var -> /var/netscreen/GuiSvr
   ```
   The output in the example indicates that the actual location of the GUI Server data is in /var/netscreen/GuiSvr. Verify on your own system where your data is stored and which directories should be backed up. Follow the same procedure to determine the location of your data on the Device Server.

4. Run the appropriate backup command on your Solaris or Linux platform to backup the GUI Server data. For example:
   ```
   tar -cvf /netscreen_backup/db-date.tar /var/netscreen/GuiSvr
   ```

5. Run the appropriate backup command on your Solaris or Linux platform to backup the Device Server data. Using tar may not be appropriate for log data in the Device Server which may be very large. It is recommended that you use either Secure Copy or FTP to backup the Device Server data.

   For example using scp:
   ```
   scp -r <local directory> usr@host:<remote-directory>
   ```
Archiving and Restoring Logs and Configuration Data

For example, using ftp:

```
ftp <host name>
bis
hash
lcd <local directory>
prompt
mput
```

7. Start the Device Server.

Restoring Logs and Configuration Data

To restore log and configuration data:

1. Stop the Device Server.
2. Stop the GUI Server.
3. Use the mv command to transfer data from the "var" directories to a safe location.
4. Untar or otherwise place your backups into both of the locations described above.
5. Start GUI Server.

**Note:** These instructions apply only to systems where the "var" links point to a true location outside the prescribed locations (e.g., /usr/netscreen/GuiSvr or /usr/netscreen/DevSvr). It is not recommend that you have these links point to locations that are inside /usr/netscreen/GuiSvr or /usr/netscreen/DevSvr. This will complicate any upgrade of Security Manager and will require special precautions during backup and restore.
If you installed and configured the option to perform automatic database backups, the utility performs the following actions on a daily basis:

- waits for all processes on the server to complete
- stops the running server process. During this time all UI clients currently connected to the management system are disconnected.
- backs up all relevant data in a file called `backupN` where `N` is the number day of the week (i.e., backup1 is the backup file saved on Monday, backup7 is the backup file saved on Sunday). The file is saved in the database directory location specified at installation.
- restarts the running server process

During this time, users will not be able to perform any changes to the management system until the system is restarted.

Note: If you have installed the management system on separate servers (in the extended configuration), and you wish to perform automatic database backups, you must install and configure the option on both the GUI Server and Device Server.

### Configuring the Automatic Database Backup Option

You can manually configure the behavior of the automatic database backup option by manually editing a configuration file (called `iHaSvr.cfg`) in the automatic database backup configuration directory.

To configure the automatic database backup tool:

1. Stop the running server process.
2. Navigate to the automatic database backup configuration directory (this is `var/netscreen/iHaSvr` by default).
3. Open the automatic database backup option configuration file (`iHaSvr.cfg`) in any text editor.
4. Configure the file as needed:
   a. To change the automatic database backup directory, edit the value for the `iHighAvail_pathDbBackup` variable.
   b. To change the time of day that the automatic database backup begins, edit the value for the `iHighAvail_backupTimeHour` variable.
   c. To change the number of backup files that the tool saves, edit the value for the `iHighAvail_numofBackup` variable.
   d. To change the path to the rsync package, edit the value for the `iHighAvail_rsyncLocation` variable.

For example, if you wanted to change the time of day that the automatic database backup begins to 4:00am, and you wanted to reduce the number of backup files to 3, the configuration file would appear as follows:
5. Save the file.
6. Restart the running server process.

**Restoring the Database**

If for any reason you are required to restore the database, you can do so by invoking a shell archive script.

To restore the database:

1. Install NetScreen-Security Manager 2004 FP1 on a new server machine. The new server machine is required to use:
   - the same IP Address as the previous server that you ran the GUI Server
   - the same operating system that you ran on the previous server

   During the installation, you must also install and configure the automatic database backup option on both the GUI Server and Device Server.

2. Save your remote copy of the database backup file(s) for the appropriate day of the week to the automatic database backup data directory on your new management system server.

3. Navigate to the HA Server utilities subdirectory (/usr/netscreen/iHaSvr/ utils by default).

4. Run the database restore shell archive script and specify the number day of the week for the backup file that you wish to restore from (i.e, \( N = \) backup day of the week). You can do so by running the following command:
   
   ```sh
   sh restoreDbFromBackup.sh N
   ```
   
   For example, if you wanted to restore the backup file from Friday, you would run the following command:
   
   ```sh
   sh restoreDbFromBackup.sh 5
   ```
The restore script runs automatically. It first prompts you to confirm stopping the running server process(es). It then proceeds to verify that you have properly logged in as the root user. It then verifies that the backup file specified exists. If so, the script proceeds to stop all running server processes. It then uses rsync to copy the backup file to the appropriate server directories. Once it has completed restoring the files, it restarts all server processes.

Validating the Database Recovery Process

If you are using the automatic database backup option on a network where the GUI Server and Device Server are installed on separate systems, it is possible that you may experience issues with devices reconnecting to the management system after you have restored the database. This is likely to occur if you did not install the automatic database backup option properly on both the GUI Server and Device Server. In this event, contact technical support for assistance.
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
}
```
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: If you are uninstalling the UI on a Windows-based computer, 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. On a Windows-based computer, use the **Start** menu, and select **NetScreen-Security Manager>Uninstall Security Manager**.

   On a Linux-based computer, you can either double-click on the Uninstall_NetScreen_Security Manager icon, or you can launch the UI uninstaller from a command line. From the command line, you can run the following command:

   ```sh
   sh Uninstall_Netscreen-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.
This appendix describes the Security Manager three-tiered architecture. This includes a description of the management system, User Interface (UI), and the FW/VPN devices managed in your network.
**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.

**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 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.*
HA Server

There is an additional server process called the HA Server that continuously monitors the GUI Server and Device Server processes. If the HA Server process detects that either the GUI Server or Device Server is down, it automatically restarts the process.

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 FP1 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.

<table>
<thead>
<tr>
<th>FW/VPN Device</th>
<th>ScreenOS Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS5XP</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS5XT</td>
<td>4.0.0, 4.0.0-DIAL2, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS25</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS50</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS100</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS204</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS208</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS500</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS5200/8</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS5200/24</td>
<td>4.0.1-SBR, 4.0.1-SIBR, 5.0</td>
</tr>
<tr>
<td>NS5400</td>
<td>4.0.1-SBR, 4.0.1-SIBR, 5.0</td>
</tr>
<tr>
<td>NS5GT</td>
<td>4.0.0-DIAL2, 5.0 only</td>
</tr>
<tr>
<td>NS-HSC</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS-ISG-2000</td>
<td>5.0 only</td>
</tr>
</tbody>
</table>
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 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.
- there are six ports on the Device Server: 4 inbound TCP ports supporting connection requests from existing FW/VPN devices; and 2 outbound TCP ports used to establish communication with FW/VPN devices running ScreenOS 4.0.X.

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7801</td>
<td>TCP</td>
<td>INBOUND</td>
<td>listens for incoming connection requests from the Security Manager UI(s) and Device Server. Used to establish communication session with <strong>Device Server</strong> and/or <strong>Security Manager UI(s)</strong>. This communication session uses an <em>encrypted</em> form of TCP called Secure Server Protocol (SSP). It is also a duplexed connection enabling the UI and GUI Server to communicate back and forth to each other after the connection is established.</td>
</tr>
</tbody>
</table>
The following table summarizes the ports that are open on the Device Server.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7800</td>
<td>TCP</td>
<td>INBOUND</td>
<td>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+).</td>
</tr>
<tr>
<td>15400</td>
<td>TCP</td>
<td>INBOUND</td>
<td>listens for incoming Report Manager NetScreen 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. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>11122</td>
<td>TCP</td>
<td>INBOUND</td>
<td>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. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>69</td>
<td>UDP</td>
<td>INBOUND</td>
<td>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. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>22/23</td>
<td>TCP</td>
<td>OUTBOUND</td>
<td>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. While SSH sessions are encrypted, Telnet sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
</tbody>
</table>
Using the Secure Server Protocol (SSP)

Security Manager uses the Secure Server Protocol (SSP) to provide secure communication between each management system component (i.e., GUI Server, Device Server, and User Interface), as well as between the Device Server and the FW/VPN devices managed in your network. SSP offers strong encryption and authentication mechanisms, so management traffic is protected and kept confidential. SSP utilizes RSA public key cryptography, AES symmetric encryption, and HMAC-SHA-1 hashing.

Communications With Devices Running ScreenOS 5.0+

If you are deploying Security Manager in a network with FW/VPN devices running ScreenOS 5.0 and higher, note that SSP uses two TCP ports for communication:
- TCP port 7800 for the Device Server
- TCP port 7801 for the GUI Server

You must therefore, allow TCP port 7800 on firewalls deployed between the Security Manager management system and the FW/VPN devices managed in your network. You must also configure firewalls between the GUI Server and UI clients to allow TCP port 7801.

The following table lists and describes the ports used specifically in communications between Security Manager and ScreenOS 5.0 devices.

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 7800</td>
<td>Accepts incoming ScreenOS 5.0 device connections</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 7801</td>
<td>On a separated install, used to communicate with GUI server</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to import initial configs of 5.0 devices.</td>
</tr>
<tr>
<td>GUI Server</td>
<td>Inbound TCP: 7801</td>
<td>Accepts communication from Device Server and Client GUI</td>
</tr>
</tbody>
</table>

**Note:** The Device Server may use port 22 (SSH) to import the configuration of existing FW/VPN devices running ScreenOS 5.0. After device import, all communication goes over SSP port 7800. FW/VPN devices running ScreenOS 5.0 also support SSH v2.

**Communicating With Devices Running Screen 4.x and Earlier**

FW/VPN devices running ScreenOS 4.x and earlier utilize the same communication protocols for communicating with Security Manager that were supported with NetScreen-Global PRO:

- Device configuration is performed via telnet or SSH1.
- Logging information is sent over the NetScreen Server Protocol (TCP port 15400).
- TFTP (UDP port 69) is used for sending firmware updates.
- NetScreen Address Change Notification (NACN), supported in ScreenOS 4.x devices, uses TCP port 11122.

Since some of these protocols (i.e., TCP port 15400, Telnet port 23, TFTP) are not encrypted or authenticated, an IPSEC tunnel between the management server and the FW/VPN devices running 4.x and earlier is strongly recommended.
The following table lists and describes the ports used specifically in communications between Security Manager and ScreenOS 4.x and earlier devices.

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to manage FW/VPN devices running ScreenOS 4.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 15400</td>
<td>Management for FW/VPN devices running ScreenOS 4.x</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound UDP: 69</td>
<td>TFTP server for updating FW/VPN devices running ScreenOS 4.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 11122</td>
<td>Accepts incoming NACN requests for FW/VPN devices running ScreenOS 4.x.</td>
</tr>
</tbody>
</table>

Creating a Separate Management Network

It is recommended you isolated the Security Manager management system from the rest of your network traffic. You should send management traffic on a separate management network, and you should deploy a firewall to enforce access policies on the management network.

If you are deploying Security Manager in a network with FW/VPN devices running ScreenOS 5.0 and ScreenOS 4.x, you must configure the firewall protecting the management network to allow:

- TCP ports 7800 and 11122 to the Device Server
- TCP port 15400 and UDP port 69 to the Device Server over VPN tunnels
- TCP port 22 outbound from the Device Server

You do not need to allow traffic to or from the GUI Server if you deploy your UI clients inside the management network. If you must deploy UI clients outside the management network, you must allow TCP port 7801 access to the GUI Server in the firewall protecting the management network.

For management of ScreenOS 5.0 devices, it is recommended that you use SSP on the untrust interface, as this configuration reduces the possibility of losing access to the device due to an invalid configuration update.

For management of ScreenOS 4.x and earlier devices, it is recommended that you use SSH to the untrust interface. In addition, you should configure a VPN tunnel to send logs/events via TCP port 15400 and firmware updates via TFTP.
This Appendix provides details on how data is migrated from NetScreen-Global PRO Express and NetScreen-Global PRO into NetScreen-Security Manager 2004.
### Domains

The use of domains in Policy Manager enabled you to group and manage separate components of your network. Security Manager extends domain functionality by enabling you to organize them hierarchically.

In Security Manager, a global domain maintains a parent-child relationship with all other sub-domains. In Policy Manager, there is no concept of domain hierarchy.

### Domain Migration

For every domain configured in Policy Manager, a sub-domain is created in Security Manager. All sub-domains created in Security Manager have a child relationship to the global domain.

Sub-domain names are unique in Security Manager. If you attempt to import a domain whose name matches a domain name that already exists in Security Manager, the import process identifies the conflict, and prompts you to resolve the name conflict before proceeding with the import.

Configuration data in Policy Manager migrates to Security Manager as part of the same domain that the data resides in Policy Manager (though, these domains may be renamed in the event of name conflicts).

As there is no concept of domains in Report Manager/Realtime Monitor, configuration data in Report Manager/Realtime Monitor migrates to the global domain in Security Manager.

Configuration data in Policy Manager migrates to Security Manager on a per domain basis. During both the export and import processes, you can specify whether or not you want to migrate individual domains, or all domains at the same time. Refer to Chapter 1, “Introduction” for more information on exporting and importing domains.

### Example

For example, if you configured 2 domains in Policy Manager - one called “sub0” and another called “sub1”, during the migration both domains and all the configuration data in them are created in Security Manager. Both sub-domains have a child-relationship to the global domain.
DEVICES AND DEVICE GROUPS

Security Manager enables you to manage devices and device groups in much the same manner that you were accustomed in Global PRO. During the migration, you may however notice subtle differences in the way that your device types are abstracted in Security Manager.

There are five main device types in Security Manager:

- FW/VPN Device
- Vsys device
- Extranet device
- Cluster
- Group

Policy Manager Device Migration

For every device configured in Policy Manager (except those mentioned below), a FW/VPN device object is created in Security Manager.

Exceptions:

- For every Vsys device configured in Policy Manager, a “Vsys device” is created in Security Manager.

  Note: Security Manager does not support the migration of virtual systems that are offline at the time of export. This is due to the fact that Policy Manager does not store information on the virtual system if offline as required. If you intend to migrate a domain that has virtual systems, you need to verify that the Vsys root device is online during the export.

- For every extranet device type configured in Policy Manager, an Extranet device is created in Security Manager.

- For every "configuration-related" Shared Config object in Policy Manager, a template in the Device Manager is created in Security Manager.

- For every device where HA is enabled (i.e., where "Active/Passive", "Active/Active" is enabled in the HA screen), a cluster device is created in Security Manager. In addition, for every cluster member configured in the HA device, a cluster member device is created in Security Manager within the cluster device.

All data that is configured for each device in Policy Manager (i.e., device name, device type, device ScreenOS version, serial #, admin name/password, contact IP address (management IP Address), SCS use and information, NACN information, and OSPF information) migrates to the configuration of the FW/VPN device object.
Report Manager/Realtime Monitor Device Migration

Devices configured in Report Manager/Realtime Monitor migrate to Security Manager as follows:

- For every device configured in Report Manager/Realtime Monitor where the serial # configured in Report Manager/Realtime Monitor matches the serial # of any FW/VPN device object already existing in Security Manager (i.e., imported from Policy Manager), the configuration data related to that device in Report Manager/Realtime Monitor is merged with the FW/VPN device object (not Vsys device) already created in that sub-domain. This means that any additional data in Report Manager/Realtime Monitor is added to the FW/VPN device configuration. Note that no data from the existing FW/VPN device object is overwritten by data from Report Manager/Realtime Monitor.

- For every device configured in Report Manager/Realtime Monitor where the serial # configured in Report Manager/Realtime Monitor does not match the serial # of any FW/VPN device object already existing in Security Manager, a new FW/VPN device object is created in Security Manager and placed in the global domain.

For every device group in Policy Manager, a device group is created in Security Manager. In addition, all the devices that are members of that device group are listed as members of the device group in Security Manager.

Device groups in Report Manager/Realtime Monitor are not migrated.

Example: Migrating Devices

For example, let’s say you configured four devices in Policy Manager:

- NS-500 with HA enabled called “NS-500”
- Vsys device called “VS1”
- Extranet device called “Extranet Device 1”
During the migration, the same devices and all the configuration data in them are created in Security Manager. In addition, a cluster device is also created.
Users and User Groups

In Global PRO, you could define and configure one type of user only. You could also assign users of Global PRO specific administrative privileges to access objects in the management system.

Security Manager enables you to specifically manage users of the management system and users in your network. There are two main types of users in Security Manager:

- **Admins.** Users of the Security Manager system with specific roles and privileges. Admins are allowed to log into a domain and perform specific activities such as configure and manage devices in the network.

- **Users.** User objects in Security Manager represent users of the devices you manage with Security Manager. User objects can be remote members of a VPN or those referenced in security policies.

During the migration, all users configured in Policy Manager migrate to Security Manager as local user objects. Those users associated with administrative roles in Global PRO also migrate to Security Manager as Admins.

Due to differences inherent in how Global PRO and Security Manager deal with administrative privileges, there is not an exact 1-1 mapping of privileges. Admins as they are configured in Global PRO may have more or less privileges in Security Manager. During the import process, the import utility prompts you to specify a general guideline to apply to all these cases.

You can group “users” in Security Manager. You cannot however group “Admins” in this release of Security Manager.

Policy Manager User Migration

Users configured in Policy Manager migrate to Security Manager as follows:

- For every user created in Policy Manager, a local user object is created in Security Manager.

- For every user configured in a firewall policy under the "restricted usage" screen using an external authentication server (i.e., Radius, LDAP, SecurID) in Policy Manager, an external user object is created in Security Manager.

  **Note:** If the user is authenticated locally (using local DB), a local user object is created in Security Manager only.

- For every user configured as part of a manual key VPN, a manual key user object is created in Security Manager.

- For every user configured with administrative roles in Policy Manager, an Admin user object is created in Security Manager.
  - If the Policy Manager user has privileges in a specific domain in Policy Manager, they are created in Security Manager in that specific domain.
  - If the Policy Manager user has privileges in multiple domains in Policy Manager, they are created in Security Manager in the global domain.
Since there is no concept of domains in Report Manager/Realtime Monitor, all users from Report Manager/Realtime Monitor are imported into the global domain.

All data configured in the user object in Policy Manager migrates to Security Manager.

**Report Manager/Realtime Monitor User Migration**

Users configured in Report Manager/Realtime Monitor migrate to Security Manager as follows:

- For every user configured in Report Manager/Realtime Monitor, an Admin user object is created and placed in the global domain in Security Manager. Administrative privileges configured in Report Manager/Realtime Monitor are not however migrated.

**Note:** Admin users created from Report Manager data have no administrative privileges associated with them. They are effectively useless until you assign them privileges in Security Manager.

- If the user name configured in Report Manager/Realtime Monitor matches the name of any Admin object already existing in Security Manager (i.e., already imported from Policy Manager), then the import utility prompts you to resolve the conflict. You can resolve the conflict by renaming the existing Admin object in the Security Manager database; overwriting the existing Admin object; or you can choose not to import the Report Manager/Realtime Monitor user.

**Policy Manager User Group Migration**

User groups configured in Policy Manager migrate to Security Manager as follows:

- For every user group created in Policy Manager that includes users without administrative privileges, a local user group object is created in Security Manager.

- If a user is part of a user group in Policy Manager that has administrative privileges, or in other words, that user has "inherited permissions", then an Admin user object is created for that user in Security Manager.

- If a user has administrative privileges in Policy Manager and is part of a local user group (no permissions), then the local user object associated with the user is created in the local user group.

**Note:** Importing Policy Manager domains separately may impact where your users are created in Security Manager. For example, if you have a user in Policy Manager with privileges in subdomain1 and subdomain2, and you import subdomain1 only, the export process does not know that the user has privileges in subdomain2. During the migration, a user object is created only in subdomain1. This is different than if you imported both domains together. In this case, the same user object is created in the global domain (but with privileges to subdomain1 and subdomain2).
Report Manager/Realtime Monitor User Group Migration

If a user in Report Manager/Realtime Monitor is part of a user group, that association is still maintained in Security Manager.

**Note:** Users and user groups could share the same name in Policy Manager. In Security Manager, they cannot share the same name. During the migration process, a text string ("i_") is prepended to the user group name in the event that a user and user group share the same name. For example, if you have both a user and user group called "California", the user group is renamed "i_California".

If you want to maintain the administrative privileges configured for your Admin users and Admin groups in Report Manager/Realtime Monitor, you need to manually re-create the new admin roles in Security Manager.
Example: Migrating Users

For example, if you configured a user in Policy Manager named “Shingo Katayama” with administrative roles, during the migration, both a local user object with the same name and an Admin is created in Security Manager.
ADDRESS OBJECTS

Both Security Manager and Policy Manager support the creation of security policies and VPNs by referencing shared objects. Objects such as addresses, services, or schedules represent elements of a network or network configuration that you can share across multiple devices.

In Policy Manager, you create and configure address objects in an Address Book. You could also define and associate multiple address members and network mask pairs in a single address book entry.

In a similar manner, Security Manager enables you to configure address objects in the Object Manager module under Address Objects.

In Security Manager, however, you cannot associate multiple addresses within a single address object as you could with address members or network mask pairs in Policy Manager. Each address entry is managed as a separate object entity in Security Manager. During the migration process, each address member and network mask pair in a Policy Manager address book entry is created as an individual address object in Security Manager. Because of this, you may notice after the migration that you now have more address objects in Security Manager than you previously configured in Policy Manager.

Security Manager also introduces the concept of address network objects and address groups.

Address Book Migration

Address objects configured in Policy Manager migrate to Security Manager as follows:

- For every individual address entry configured in Policy Manager, an address object is created in Security Manager. This includes individual address entries configured as a network mask pair as well as those configured as an address member in every address object Policy Manager.

- Address entries with a less than 32 bit mask configured in Policy Manager are created as an address network object in Security Manager. Address entries with a 32 bit mask in Policy Manager are created as an address host object in Security Manager.

- For every address book entry configured in Policy Manager with multiple address entries, an address group is created in Security Manager. The address group is named with the same name as in Policy Manager. Host address entries in the group are however renamed with the IP Address appended to it (i.e., "_10.1.1.1"). Network address entries in the group are renamed with the IP Address/NetMask appended to it (i.e., 10.1.1.0/16).

All data configured in the address object in Policy Manager migrates to Security Manager.
Example: Migrating Address Book Objects

For example, if you configured several address objects in Policy Manager, the same address objects and all the configuration data in them are created in Security Manager during the migration. The West Region Address Book with several address members associated with it becomes an address group in Security Manager. Note also that the Site A address object becomes an address network object in Security Manager.
**Schedule Objects**

Like addresses in Policy Manager, you could also define and configure schedule objects in a Schedule Book. In a similar manner, Security Manager enables you to configure schedule objects in the Object Manager module under Schedule Objects.

**Schedule Object Migration**

For every individual schedule object configured in Policy Manager, a schedule object is created in Security Manager. Any text string configured as a description in Policy Manager migrates as a comment in Security Manager.

All data configured in the Schedule object in Policy Manager migrates to Security Manager.

**Example: Migrating Schedule Objects**

For example, if you configured two schedule objects in Policy Manager - one named “Operating Hours” and another named “After-Hours”, both schedule objects are created in Security Manager during the migration.
**SERVICE OBJECTS**

In Policy Manager, you create and configure service objects in a Service Book. You could also define and associate multiple services in a single service book entry.

In a similar manner, Security Manager enables you to configure service objects in the Object Manager module under Service Objects. In Security Manager, however, you cannot associate multiple services within a single service object as you could with services in Policy Manager. Each service member is configured as a separate object entity in Security Manager. During the migration process, each service member in a Policy Manager service book is created as an individual service object in Security Manager. Because of this, you may notice after the migration that you now have more service objects in Security Manager than you previously configured in Policy Manager.

**Service Object Migration**

Service objects configured in Policy Manager migrate to Security Manager as follows:

- For every individual service object configured in Policy Manager, a service object is created in Security Manager.
- For every service member configured as part of a service object in Policy Manager, a service object is created in Security Manager.
- For every service object configured with multiple user-defined services in Policy Manager, a service group object is created in Security Manager. The service group is named with the same name as in Policy Manager. The service entry in the group is however, renamed using the name of the service group and a text string appended to it (currently this is "_svc"). For example, if the service group is called "service" in Policy Manager, the service entry is renamed "service_svc" in Security Manager.
- For the “AOL” pre-defined service object in Policy Manager, a service group and a service object called “AOL” is created in Security Manager. The “AOL” service object is then added as a member of the group.

All data configured in the Service object in Policy Manager migrates to Security Manager.

**Example: Migrating Service Objects**

For example, if you configured a service object in Policy Manager named “Service Book 1”, with two service members (i.e., Gopher and FTP), during the migration, individual service objects are created in Security Manager for Gopher and FTP, and a service group called “Service Book 1” that includes Gopher and FTP.
**Shared and Protected Resources**

In Policy Manager, you create and configure shared resource objects in a Shared Resource Book. You could further define Protected Resources for use in creating a VPN for a specific FW/VPN device. In a similar manner, Security Manager enables you to configure shared resource objects in the Object Manager module under Protected Resources.

Because both shared and protected resources defined in Policy Manager as a shared object and those specifically protected by a specific device are migrated as shared resource objects in Security Manager, you may notice more shared resource objects in Security Manager than you had in Global PRO.

**Shared Resource Object Migration**

Shared Resource objects configured in Policy Manager migrate to Security Manager as follows:

- For every Shared Resource object configured in Policy Manager, a Protected Resource object is created in Security Manager. This includes those “Protected Resources” defined for every device as well as those defined as a Shared resource (protected by multiple devices) in Policy Manager.
- All configuration data for the Shared Resource is collapsed into the Protected Resources object in Security Manager.
- Server/Client parameter in Security Manager is set to "Both" by default.
Example: Migrating Shared Resources

For example, if you defined a Protected Resource called “My Protected Resources” as part of a VPN for a FW/VPN device in Policy Manager, during the migration, the object is created as a Protected Resource object in the VPN Manager.
GLOBAL OBJECTS

In Policy Manager, you create and configure global objects under Global Objects. You could further define device-specific Dynamic IPs, Mapped IPs, and Virtual IPs under the NAT settings associated with a FW/VPN device.

In a similar manner, Security Manager enables you to configure global objects in the Object Manager module under NAT Objects. Note that you may notice more NAT objects in Security Manager than those configured as global objects in Policy Manager because device-specific global objects in Policy Manager are migrated as NAT objects in Security Manager.

Global Object Migration

For every Global object configured in Policy Manager, a NAT object is created in Security Manager.

For device-specific objects in Policy Manager:

- For every device-specific MIP objects in Policy Manager, a NAT object is created in Security Manager. If there are multiple device-specific MIP objects in Policy Manager with the same MIP IP Address/Mask, they all merge into one NAT object in Security Manager. The name of the object in Security Manager is "MIP(IP Address/Mask)".

- For every device-specific DIP object in Policy Manager, a NAT object is created in Security Manager. If there are multiple device-specific DIP objects in Policy Manager with the same DIP IP range, they all merge into one NAT object in Security Manager. The name of the object in Security Manager is "DIP id (start IP address-end IP address)".

- For every device-specific DIP group object in Policy Manager, a NAT object is created in Security Manager. If there are multiple device-specific DIP group objects in Policy Manager with the same DIP group id, they all merge into one NAT object in Security Manager. The name of the group object in Security Manager is "DIP group id(group)" for example ("5(group)).

All data configured in the Global object in Policy Manager migrates to Security Manager.

Example: Migrating Global Objects

For example, if you configured a Global object in Policy Manager, during the migration, the object and all its configuration data are created in Security Manager in the Object Manager module under NAT Objects.
Authentication Servers

Security Manager enables you to configure authentication server objects in the Object Manager module under Authentication Servers.

Authentication Server Object Migration

For every authentication server object configured in Policy Manager, an authentication server object is created in Security Manager. All data configured in the authentication server object in Policy Manager migrates to Security Manager. You could enable multiple purposes for authentication servers in Policy Manager. During the migration, all purposes are enabled in Security Manager.

*Note*: In Policy Manager, the default global authentication server object called “Local Database” does not migrate into Security Manager.
Example: Migrating Authentication Server Objects

For example, if you configured an authentication server object in Policy Manager named “Corporate Authentication Server”, during the migration, the object and all its configuration data are created in Security Manager in the Object Manager module under Authentication Servers.
**GROUP EXPRESSIONS**

Security Manager enables you to configure group expression objects in the Object Manager module under Group Expressions.

**Group Expression Migration**

For every Group Expression configured in Policy Manager, a Group Expression object is created in Security Manager. All data configured in the group expression object in Policy Manager migrates to Security Manager.

**Example: Migrating Group Expression Objects**

For example, if you configured two group expression objects in Policy Manager named “exp1” and “exp2”, during the migration, both objects and all their configuration data are created in Security Manager in the Object Manager module under Group Expressions.
Shared Configs

Shared Configs in Policy Manager enabled you to define and configure common settings that you could apply to multiple devices or other Global PRO components.

In Security Manager, the same functionality is achieved using templates. Templates in Security Manager enable you to configure a device or multiple devices with a set of predefined configuration settings.

Shared Config Object Migration

Shared config objects configured in Policy Manager migrate to Security Manager as follows:

- For every "configuration-related" Shared Config object in Policy Manager (e.g., Global Pro Monitoring, Packet Flow, AuthServer, Banner, NTP/Clock, DNS, SNMP, E-mail Alerts, Syslog, URL Filter, WebTrends), a template in the Device Manager is created in Security Manager. All data configured in the shared config object in Policy Manager migrates to Security Manager.
- "Action-related" Shared Configs in Policy Manager including CA Certs and CRL By File are not migrated.

Security Manager does not permit device templates and device objects to share the same name. During the migration process, the following text strings are prepended to the device template name in the event of a device template and device name conflict.

<table>
<thead>
<tr>
<th>Shared Config Type</th>
<th>Text String Prepended to Device Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Group</td>
<td>AdminGroup_</td>
</tr>
<tr>
<td>Auth Server</td>
<td>AuthServerTemplate_</td>
</tr>
<tr>
<td>Banner</td>
<td>BannerTemplate_</td>
</tr>
<tr>
<td>Email Alert</td>
<td>Email AlertTemplate_</td>
</tr>
<tr>
<td>Flow Shared</td>
<td>FlowTemplate_</td>
</tr>
<tr>
<td>GlobalPRO</td>
<td>GlobalPROTemplate_</td>
</tr>
<tr>
<td>NTP</td>
<td>NTPTemplate_</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMPTemplate_</td>
</tr>
<tr>
<td>Syslog</td>
<td>SyslogTemplate_</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>UrlFilteringTemplate_</td>
</tr>
<tr>
<td>WebTrend</td>
<td>WebTrendTemplate_</td>
</tr>
</tbody>
</table>

The export tool prints out a table at the end of the exporting process to list all the objects that are renamed due to name conflicts.
Example: Migrating Shared Config Objects

For example, if you configured a shared config object in Policy Manager called “No Dog Sites”, during the migration, the configuration data appears in Security Manager as a template in the Device Manager.
ZONE PROFILE

Similar to Shared Configs, Zone Profiles enabled you to define common zone settings that you could apply to multiple devices. In Security Manager, the same functionality is achieved using templates.

Zone Profile Object Migration

For every Zone Profile configured in Policy Manager, a template in the Device Manager is created in Security Manager. Data configured for each zone profile in Policy Manager migrates to the configuration of the template (Network > Zone) in Security Manager. This includes the zone name, interfaces, traffic filtering settings, VR settings etc.

Note: Configuration data for Zone profiles is migrated into Security Manager as part of the device configuration import process.

Example: Migrating Zone Profile Objects

For example, if you configured a zone profile object in Policy Manager called “Zone1”, during the migration, the configuration data appears in Security Manager as a template in the Device Manager.
POLICIES

Both Security Manager and Policy Manager support the definition and configuration of firewall policies enabling you to either deny or permit specific network traffic across your FW/VPN devices. In Policy Manager, you could apply multiple policies to a specific FW/VPN device in a priority list order.

Security Manager provides the same functionality, but without the concept of hierarchical policy lists. In Security Manager, the same functionality is achieved by installing 1 active policy with multiple rules on each FW/VPN device.

Policy Migration

During the migration, all policy lists or "groups" are merged into one active policy called “Migrated-GlobalPRO-Policy”. The priority of each policy determines the order in which the policy rules appear.

Example: Migrating Policies

For example, if you have 3 policies configured in Policy Manager, Policy A, Policy B, and Policy C. If each policy has 5 rules, during the migration, the 3 individual policies are merged and stacked according to priority and built into a single shared policy with 15 rules. Each policy in PRO becomes a rule in the shared policy in SM.
VPN Migration

VPNs configured in Policy Manager migrate to Security Manager as follows:

- For every IKE Autokey and Manual VPN configured in Policy Manager, an IPsec VPN is created in Security Manager. Policy-based members and route-based members that are configured in Policy Manager migrate to these VPNs as well. All relevant configuration data in Policy Manager migrates to the object in Security Manager.
- For every IKE Autokey VPN with users configured as policy-based members, an IPsec User VPN in Security Manager is created. All relevant configuration data in Policy Manager migrates to the object in Security Manager.
- For every L2TP VPN configured in Policy Manager, an L2TP VPN object is created in Security Manager. All relevant configuration data in Policy Manager migrates to the object in Security Manager.
- For every L2TP over IPsec VPN configured in Policy Manager, an L2TP over IPsec VPN object is created in Security Manager. All relevant configuration data in Policy Manager migrates to the object in Security Manager.
P1 AND P2 PROPOSALS

Security Manager enables you to manage P1 and P2 Proposals objects in the VPN Manager module.

P1 and P2 Proposal Object Migration

P1 and P2 Proposal objects configured in Policy Manager migrate to Security Manager as follows:

- For every P1 Proposal object configured in Policy Manager, a Custom IKE Phase1 Proposal object is created in Security Manager under the VPN Manager. These objects are renamed with the VPN name prepended to the name of the proposal (i.e., “VPN Name:P1 Proposal”).
- For every P2 Proposal object configured in Policy Manager, a Custom IKE Phase2 Proposal object is created in Security Manager under the VPN Manager. These objects are renamed with the VPN name prepended to the name of the proposal (i.e., “VPN Name:P2 Proposal”).

Example: Migrating P1 & P2 Proposal Objects

For example, if you configured a P1 Proposal object in Policy Manager named “P1”, during the migration, the object and all its configuration data are created in Security Manager in the VPN Manager module under IKE Phase 1 Proposals.
**IP POOLS**

Security Manager enables you to manage IP Pools in the VPN Manager module.

**IP Pool Migration**

For every IP Pool object configured in Policy Manager, an IP Pool object is created in Security Manager under the VPN Manager.

**Example: Migrating IP Pool Objects**

For example, if you configured an IP Pool in Policy Manager, during the migration, the object is created in Security Manager in the VPN Manager module under IP Pools with all the configuration data related to the IP Range.
**REMOTE SETTINGS**

Security Manager enables you to manage Remote Settings objects in the VPN Manager module.

**Remote Setting Object Migration**

For every IP Pool object configured in Policy Manager, an IP Pool object is created in Security Manager under the VPN Manager.

**Example: Migrating Remote Settings Objects**

For example, if you configured a remote setting in Policy Manager, during the migration, the object is created in Security Manager in the VPN Manager module with all the relevant return values configured.
EVENTS

Mapping tables configured in Realtime Monitor enabling events to appear in Security Manager as they did in Realtime Monitor - by group, type, and severity level, are migrated into Security Manager.
CERTIFICATES

Certificates used for communications with FW/VPN devices running ScreenOS 4.0.X using NACN are also migrated from Policy Manager into Security Manager. After the migration, you must copy the private certificate key using the NACN certificate transfer utility to the Device Server.
**DATA COLLECTOR PROPERTIES**

The polling attributes and intervals used by each data collector to collect data from each device configured in Report Manager/Realtime Monitor are migrated in Security Manager. Assuming that the Device Server in Security Manager is installed on the same server as the Report Manager/Realtime Monitor data collector, the configuration parameters enable Security Manager to connect to FW/VPN devices running ScreenOS 4.0.x. If the Device Server is installed on a server with a new IP address, you can still connect to legacy devices by changing the Global PRO IP addresses in all devices.

*Note: Server properties from your previous configuration in Global PRO override any existing data configured in Security Manager.*
MASTER CONTROLLER PROPERTIES

Master Controller properties enabling the MC to connect and forward data to the Report Manager database (i.e., database name, IP Address, protocol and port) are migrated in Security Manager. This is applicable only if you plan to continue using historical reports with Security Manager.

E-mail properties enabling Security Manager e-mail alerts to be sent to the Security Manager admin are also migrated.

**Note:** Server properties from your previous configuration in Global PRO override any existing data configured in Security Manager.
HISTORICAL REPORTS

You can continue to use historical reports in Report Manager with Security Manager. By maintaining your HRS infrastructure, you can still receive resource statistics, traffic, and service level agreement data from managed FW/VPN devices using ScreenOS versions 4.0.X.

Note: You can use the Security Manager UI to view realtime alarm and log data from managed FW/VPN devices using ScreenOS versions 5.0.X.
FEATURES NO LONGER SUPPORTED

Security Manager does not support the migration of logs from Global PRO.

Security Manager does not support the following features in Policy Manager:

- Hierarchical policy lists in PRO are no longer supported in Security Manager. In Security Manager, you can only have 1 active policy per device.
- Policy Queries
- NSRP - previously depicted in the HA tab in Device Objects, now appears as a cluster object (containing devices).
- Admin Groups
- Manual VPNs - are abstracted in a different manner in Security Manager.
- VSYS - manifested differently in Security Manager
- Templates - manifested differently in Security Manager

Security Manager does not support the migration of the following data configured in Report Manager:

- Admin privileges
- Device Groups

Security Manager does not support the following features in Report Manager:

- Global properties configured in Report Manager that controlled how data was integrated with other third party management systems, archived and purged are not migrated.
- Oracle, MS-SQL, or PGSQL database support.
- Report Manager/Realtime Monitor monitor and display filters. You need to manually create new filters in the Log Viewer.
- Report Manager/Realtime Monitor histograms. You can no longer view a histogram of your events.
Sizing and Capacity Planning

This appendix provides guidelines to help you size your hardware to accommodate specific network requirements.
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 II
- “Processor Requirements” on page II
- “Disk Storage” on page II
- “Network Bandwidth” on page III

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. As disk space allocated for logs on the Device Server is maxed out, 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 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 III
- “Dedicating the System” on page III
- “Securing Communications” on page IV
- “Installing Updates and Security Patches” on page IV

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 Appendix A “Technical Overview” 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.
ADDITIONAL INFORMATION

The detailed system requirements for each deployment of Security Manager can vary greatly from installation to installation, depending on the size and topology of the network. For additional information, it is recommended that you consult with your NetScreen Professional Services representative.
Index

A
address objects, migration details B-X
Admin groups, migration details B-XXXIII
authentication servers, migration details B-XVII

C
capacity planning, management system C-II–C-IV
certificates, migration details B-XXIX
changing
default user management system runs as 92
communication ports A-V–A-IX
communications A-V–A-IX
configuration options
installing management system on same server (typical) 9
installing management system on separate servers (extended) 10
configuring
Device Server data directory 27, 65
GUI Server data directory 27, 65
management system IP addresses 92
password for super user 28, 66
CPU
requirements on management system, same server 7
requirements on management system, separate servers 7

d
Device Server
communication ports, described A-VI
data directory, configuring 27, 65
described A-III
starting 89
stopping 89
devices
see FW/VPN devices
disabling
X Server 22, 60
disk storage
requirements on management system, same server 7
requirements on management system, separate servers 7
domains, migration details B-II

e
export data file
Policy Manager 71
Report Manager 71
export process 2–4
extended configuration option 10

f
FW/VPN devices
maximum number supported A-III
platforms supported A-IV

g
global objects, migration details B-XVI
Global PRO
migration 49–85
migration and installation scenarios 50–55
Global PRO data export utility 6
described 3
using 4, 14, 15
Global PRO Express
migration 13–46
migration and installation scenarios 14–17
group expressions, migration details B-XIX

data collector
multiple, migration considerations 54
properties, migration details B-XXX
data directory
for device-server, described 19, 57
for GUI-server, described 19, 57
database support, migration details B-XXXIII
defining system parameters 19, 57
Demo Mode 41, 79
device and device groups, migration details B-III–B-V
device groups, migration details B-XXXIII
GUI Server
  communication ports, described A-V
  data directory, configuring 27, 65
described A-III
  starting 89
  stopping 89

H
hardening your system C-III–C-IV
hardware
capacity planning C-II–C-III
  requirements for UI 8
historical reporting
  migration details B-XXXII
  using with Security Manager 54

I
IDP, migration details 17
import process 4–5
installation
  CD contents 6
  log file for UI 38, 76
  log, viewing 32, 70
package 6
installing
  configuration options 9
  management system 19–32, 57–70
  management system on same server 19–31, 57–69
prerequisite steps 20–24, 58–62
TFTP server on Linux 99
TFTP server on Solaris 100
UI 34–38, 72–76
IP pools, migration details B-XXVI

L
Linux RPM package
  requirements 21, 59
  verifying 21, 59
log file
  management system installation 32
  UI installation 38, 76
logging in to the UI 38, 76

M
management IP address for GUI-server 19, 57
management server
  see management system
management system
capacity planning C-II–C-IV
  changing default user 92
  commands 88
described A-II–A-III
  installing 19–32, 57–70
  installing on same server 19–31, 57–69
  restarting 88
  starting 88
  status 88
  stopping 88
  uninstalling 93
Master Controller properties, migration details B-XXXI
memory requirements
  capacity planning C-II
  for UI 8
  management system on same server 7
  management system on separate servers 7
migration
  address objects B-X–B-XI
  authentication servers B-XVII–B-XVIII
certificates B-XXIX
data collector properties B-XXX
devices and device groups B-III–B-V
domains B-II
events B-XXVIII
features not supported (Global PRO) B-XXXIII
global objects B-XVI
group expressions B-XIX
historical reports B-XXXII
IP pools B-XXVI
Master Controller properties B-XXXI
P1 and P2 proposals B-XXV
policies B-XXIII
remote settings B-XXVII
schedule objects B-XII
service objects B-XIII
shared and protected resources B-XIV–B-XV
shared configs B-XX–B-XXI
users and user groups B-VI–B-IX
VPNs B-XXIV
zone profile B-XXII
migration and installation process 2–5
migration and installation scenarios
  Global PRO 50–55
  Global PRO Express 14–16
migration path 17
migration scenarios
  not supported (Global PRO Express) 17
  not supported (Global PRO) 55
minimum system requirements
described 7–8
for UI 8
management system 7

N
network connection
  requirements for UI 8
  requirements on management system, same server 7
  requirements on management system, separate servers 7
NSRP, migration details B-XXXIII

O
operating system
  requirements for management system 7
  requirements for UI 8

P
P1 and P2 proposal objects, migration details B-XXV
password
  super user, configuring 28, 66
  super user, described 19, 57
pmexport.tar
  see Policy Manager data export file
policies, migration details B-XXIII
Policy Manager
  data migration B-II–B-XXXIII
  export data file 71
post migration steps 46
pre-migration steps
  Global PRO Express 18, 56
prerequisites before installing 20–24, 58–62
privileges, migration details B-XXXIII

R
remote settings, migration details B-XXVII
Report Manager
  data migration B-IV–B-XXXIII
  export data file 71
restarting
  management system manually 88
restarting management system 88
rmexport.out
  see Report Manager data export file
root user
  changing user that management system runs as 92
running
  UI 38, 76
  UI, in Demo Mode 41, 79

S
schedule objects, migration details B-XII
ScreenOS versions supported A-IV
securing Security Manager C-III–C-IV
Security Manager technical overview A-II–A-IX
server
  see management system
service objects, migration details B-XIII
shared configs, migration details B-XX
shared resources, migration details B-XIV
sizing
  see capacity planning
starting
  Device Server 89
  GUI Server 89
  management system manually 88
stopping
  Device Server 89
  GUI Server 89
  management system manually 88
super user
  password, configuring 28, 66
  password, described 19, 57
swap space
  requirements on management system, same
T

TFTP server
  installing 99–100
  installing on Linux 99
  installing on Solaris 100

transferring
  export data files (for Global PRO Express) 33
  export data files (for Global PRO) 71

typical configuration option 9

U

UI
  described A-IV
  hardware requirements 8
  installing 34–38, 72–76
  operating system requirements 8
  running 38, 76
  uninstalling 101

uninstalling
  management system 93
  UI 101
  upgrading RPM package (for Linux only) 22–24, 60–62
  user interface
    See UI
  users and user groups, migration details B-VI–B-IX

V

validating
  management system installation 39, 77
  management system status 31, 69
  verifying Linux RPM package 21, 59
  viewing management system commands 88
  virtual systems, migration details B-XXXIII
  VPN, migration details B-XXIV

X

X Server
  disabling 22, 60

Z

zone profiles, migration details B-XXII