



NetScreen-Security Manager and NSMXpress Release Notes

7/1/08

Release 2007.3r3

Contents

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Upgrade Considerations on page 5
- 4 Upgrading NSMXpress and NSMCM Appliances on page 5
- 5 NSMXpress Data Migration on page 15
- 6 User Privileges on NSMXpress on page 18
- 7 Addressed Issues on page 19
- 8 Known Issues on page 22
- 9 Getting Help on page 28

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-022670-01 Rev. 3

1 Version Summary

Juniper Networks NetScreen-Security Manager (NSM) is a comprehensive security management solution designed to manage device, network, and security configuration for integrated firewall, intrusion detection and prevention, and virtual private network (VPN) appliances, sensors, and systems. Juniper Networks NSMXpress is an appliance version of NSM.

The features in the following sections list the new features and enhancements in this NSM release and NSMXpress.

2 New Features

This section contains a list of new features and enhancements in this NSM release.

2.1 NSM Features

This section contains a list of new NSM features and enhancements in this NSM release.

- **Log out Admins**—The NSM super admin now has the ability to log out other admins.
- **Auto download of NSM client**—This feature allows auto download and upgrading of NSM Client from server side whenever there is a mismatch in NSM server and client version. This avoids the need to manually download the client from the support site.
- **NSM license enforcement**—NSM now requires a license to manage more than 25 devices. In order to manage more than 25 devices, a license key must be retrieved from the Juniper licensing server (LMS) and be installed onto the NSM server or Appliance.
- **Firmware upgrade in RMA state**—NSM allows to change the device firmware during the RMA-activate workflow.
- **Systems Management Web UI for NSMXpress**—System management Web interface for NSMXpress appliance.
- **Ability to delete jobs in Job Manager**—NSM allows users to delete all the jobs at once in the Job Manager.
- **Role Based Route Config Management**—NSM now gives you the ability to enable/disable the creation, modification, and deletion of routing configuration using NSM's role-based administration.
- **Same address in different zones do not create two objects**—If one address object is used for two zones, NSM will no longer push two objects to the device. For address objects in different zones, NSM will no longer append zone name when pushing the configuration to the device. When importing from device, NSM will combine address object of the same name and same content from different zones into single NSM object.

- **log-to-policy works immediately after Import**—It is no longer necessary to do a "Update device" for the log-to-policy feature to work.
- **PCAP retrieval from IDP standalone "On Demand"**—You can now choose to have PCAP retrieved from an IDP Standalone device running IDP 4.1r2 "on-demand" instead of the device sending NSM the PCAPs in log data.
- **Change to IDP Attack Group Table in NSM**—For performance reasons, the organization of the IDP attack group table in NSM is being changed to delete some "Response" policies.
- **Support IPSEC ESP-Null Encryption for IDP Inspection**—NSM enables/disables IPSEC packets with null encryption for ISG1000/2000 with IDP.

2.2 ScreenOS Features

This section contains a list of new ScreenOS features and enhancements in this NSM release.

- **DIP Pool Enhancements**—ScreenOS 6.0 has increased the size of DIP (Dynamic IP) per VSYS and per interface from 252 to 1020. NSM now supports this range.
- **Extend VSYS Name Length to 20 Characters**—VSYS name now extended to 20 characters.
- **L2V support for ISG1000**—NSM now supports Layer 2 VSYS features on ISG1000 running ScreenOS 6.0.
- **Permitted Management IP Extension**—The number of manager-IPs has been increased and made configurable based on platform. The number of manager-IPs will vary depending on the platform. The total number of manager-IPs will be 50 plus 1 times the number of VSYS.
- **Recommended Action for ISG-2000/1000 devices**—The IDP "Recommended Action" feature is now available for ISG-2000/1000 devices running ScreenOS 6.0.
- **AutoConnect VPN Support**—The Auto-Connect VPN (ACVPN) feature was introduced in ScreenOS 6.0 to provide a scalable VPN solution. In a large enterprise with many sites and branch offices, a Hub-n-spoke configuration is deployed, where each branch site (Spoke) is only connected to a central site (the Hub). All communications between Spoke sites must go through hub, which is not scalable as the number of spoke sites increase. The ACVPN feature specifies a solution wherein auto-connected security tunnels are setup dynamically among the spoke sites by leveraging the NHRP (Next Hop Resolution protocol).
- **VLAN Retagging Support**—VLAN retagging is used when you want to redirect network traffic. It must be used in conjunction with Layer 2 switch and only support in L2V mode.

- **IM AV Support**—This feature extends embedded Anti-Virus feature to scan popular public Instant Messengers (IM) namely AIM, ICQ, MSN Messenger and Yahoo Messenger. In addition, error handling has been extended to provide more granular control of passing/dropping the traffic when AV scan-engine cannot give a clean/infected scan result at Root/Vsys level.
- **TACACS Server support**—NSM now supports Screen OS TACACS authentication server type. (Terminal Access Controller Access Control System).
- **Admin Authentication Policy**—NSM now supports the ScreenOS 6.0 feature where you are allowed to specify the sequence for authentication and fallback policies.
- **NSRP Active Passive (Support for route-sync)**—NSM now supports DRP route synchronization in ScreenOS 6.0 devices. Support includes changes in the "RTO Mirror" view under NSRP section of edit-device-cluster. n in the screen shot.
- **DST Enhancement**—NSM now supports the ScreenOS 6.0 improvements that allow customers to set Daylight Savings Time rules according to their country's standard.
- **tcp-syn-bit-check**—Before ScreenOS 6.0 the "tcp-syn-check" option does TCP syn bit checking and TCP 3 way handshake checking. In ScreenOS 6.0 a new option "tcp-syn-bit-check" is added for syn bit checking.

Enabling the original option of "tcp-syn-check" performs syn bit checking and TCP 3 way handshake. The value of "tcp-syn-bit-check" is not used in this case. To have just the syn bit checking the original option should be disabled and new option should be enabled.

- **High CPU Protection Support**—In ScreenOS 6.0 the packet dropping feature has been moved to the ASIC in order to prevent high CPU utilization during DOS attacks. In addition users can configure blacklists for the ASIC to drop the packets from and also configure CPU throttling threshold. NSM now supports these features.
- **New hardware support**
 - 1 ADSL 2 + PIC support for SSG500 and SSG140 product line running ScreenOS 6.0.
 - 16 Port Copper Gigabit PIM for SSG500 and SSG140 product line running ScreenOS 6.0.
 - 8 port Copper Gigabit PIM for SSG500 and SSG140 product line running ScreenOS 6.0.
 - 6x SFP PIM support for SSG500 and SSG140 product line running ScreenOS 6.0.
 - 1x SFP Mini-PIM support on SSG20 running ScreenOS 6.0
 - 1xSerial Mini-PIM support on SSG20 running ScreenOS 6.0.
 - Jumbo Frame Support on ISG1000 devices running ScreenOS 6.0

- Support for SSG 320 and 350 devices.
- E3 card support-SSG520, SSG550, SSG120, SSG140 devices support WAN I/O cards like T1/E1/DS3. ScreenOS 6.0 and now NSM supports an E3 card.
- Support for SHDSL PIC support in SSG500, SSG140-NSM now supports SHDSL PICs for SSG 500 and 140 devices
- Switch PIM Support-NSM now support three new switch PIMs for SSG140 and SSG500 devices. These new PIMs are:
 - 8 x 10/100/1000: 8-port 10/100/1000 tri-mode Ethernet switch with RJ45 copper interface.
 - N x SFP: N-port gigabit Ethernet switch with small form factor fiber interface. N is the number of ports; currently it is limited at 6, by the width and height of a PIM.
 - 16 x 10/100/1000: 16-port 10/100/1000 tri-mode Ethernet switch with RJ45 copper interface.

3 Upgrade Considerations

If you are upgrading to NSM 2007.3r3 or NSM 2007.3r2 from 2006.1rX or earlier, or upgrading to NSM 2007.3r1 from 2007.1rX or earlier, you must perform the following two step process: First install NSM 2007.2r2 and then proceed with the upgrade.

4 Upgrading NSMXpress and NSMCM Appliances

This section provides upgrade information for NSMXpress and NSMCM appliances.

4.1 Upgrading to NSM 2007.3 release on NSMXpress Appliance

Use the following procedure to upgrade to upgrade to NSM 2007.3 on the NSMXpress appliance.



NOTE: NSM 2007.3 release requires a License File if you are managing more than 25 devices. You must have the License file available before performing the upgrade to NSM 2007.3 release. NSM installer will not proceed without the License file.

For information on the procedure of generating the License file, refer to the *NetScreen-Security Manager 2007.3 Installer Guide*.

Use the following procedure to upgrade to NSM 2007.3 on an NSMXpress appliance.

1. From NSM Software Download page, click on the link **NSMXpress Server**.
2. Download the file nsm2007.3r3_servers_upgrade_rs.zip.
3. FTP or SCP this file onto your NSMXpress appliance.

4. Log in as the admin user, and enter **n** when prompted to run the setup wizard.
5. Execute **sudo su -** and enter the admin password to gain root access.
6. Confirm the unzip utility is present on the NSMXpress appliance by executing the following command:

```
which unzip
```

This gives you the location of the file if it is available. If it is not available, use the following procedure to install this utility.

```
yum install unzip
```

7. Navigate to the directory where you saved the management system installer file (typically the `/tmp/` subdirectory).
8. Execute the following command to unzip and save the two files (`nsm2007.3r3_servers_linux_x86.sh`, `upgrade-os.sh`) and a directory (`apps-rpms`) on the NSMXpress system:

```
unzip nsm2007.3r3_servers_upgrade_rs.zip
```

9. Run the following command to automatically start the installation.

```
sh upgrade-os.sh nsm2007.3r3_servers_linux_x86.sh
```

The installer begins a series of pre-installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.
- You have installed a version of NetScreen-Security Manager preceding the current version you are installing.
- The system has sufficient disk space and RAM.

The installer then stops any running servers.

10. Type **2** to specify that you want to upgrade both device server and GUI server.

The installer next prompts you to configure additional options specific to your installation during the upgrade. This can include:

- Configuring High Availability
- Configuring interoperability with NetScreen-Statistical Report Server
- Configuring backup options
- Configuring https ports

If applicable, follow the installer prompts to configure these options.

The script next prompts if you want to restart the server(s) when finished.



NOTE: The management system installer indicates the results of its specific tasks and checks "Done" indicating 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.



NOTE: If you specify that you want to upgrade the device server and GUI server, all data previously configured in the system is restored. If you do not want to restore your previous configuration data, choose to have the installer perform a clean install of Central Manager.

11. Type **y** then press **Enter** to restart the server(s) when finished or type **n**, then press **Enter**, if you do not want to restart server processes.

The script prompts you to verify your upgrade configuration settings.

12. Verify your settings, and if they are correct, type **y** then press **Enter** to proceed or type **n**, then press **Enter**, for the installer to return you to the original selection prompt.

The upgrade proceeds automatically with the installer performing the following actions:

- Extracts and decompresses the software payloads.
- Upgrades the device server.
- Upgrades the GUI server.
- Installs the HA server.
- Sets start scripts.
- Performs post-installation tasks such as removing the staging directory and starting the server processes (if configured).

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

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting purposes. The installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/DevSvr/var/errorLog` subdirectory.

13. After the successful installation, copy the installer file `nsm2007.3r3_servers_rs.sh` to `/var/install` directory and run the following commands as follows:

```
rm -f NSM-RS
chmod 755 nsm2007.3r3_servers_linux_x86.sh
ln -s nsm2007.3r3_servers_linux_x86.sh NSM-RS
```

4.2 Upgrading to NSM 2007.3 release on NSM Central Manager Appliance



NOTE: NSM 2007.3 release for Central Manager does not require a License File. Enforcement is built into the product.

Use the following procedure to upgrade to NSM 2007.3 to NSMCM appliance.

1. From NSM Software Download page, click on the link **Central Manager Server**.
2. Download the file `nsm2007.3r3_servers_upgrade_cm.zip`.
3. FTP or SCP this file onto your NSMCM appliance.
4. Log in as the admin user, and answer "n" when prompted to run the setup wizard.
5. Execute **sudo su -** and enter the admin password to gain root access.
6. Confirm the unzip utility is present on the NSMCM appliance by executing the following command:

```
which unzip
```

This gives you the location of the file if it is available. If it is not available, use the following procedure to install this utility.

```
yum install unzip
```

7. Navigate to the directory where you saved the management system installer file (typically the `/tmp/` subdirectory).
8. Execute the following command to unzip and save the two files (`nsm2007.3r3_servers_cm.sh`, `upgrade-os.sh`) and a directory (`apps-rpms`) on the NSM Central Manager system:

```
unzip nsm2007.3r3_servers_upgrade_cm.zip
```

9. Run the following command to automatically start the installation.

```
sh upgrade-os.sh nsm2007.3r3_servers_cm.sh
```

The installer begins a series of pre-installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.

- You have installed a version of NetScreen-Security Manager preceding the current version you are installing.
- The system has sufficient disk space and RAM.

The installer then stops any running servers.

10. Type **1** to specify that you want to upgrade central manager server.

The installer next prompts you to configure additional options specific to your installation during the upgrade. This can include:

- Configuring High Availability
- Configuring backup options
- Configuring https ports

11. If applicable, follow the installer prompts to configure these options

12. The script next prompts if you want to restart the server(s) when finished.



NOTE: The management system installer indicates the results of its specific tasks and checks "Done" indicating 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.



NOTE: If you specify that you want to upgrade the Central Manger, all data previously configured in the system is restored. If you do not want to restore your previous configuration data, choose to have the installer perform a clean install of Central Manager.

13. Type **y** then press Enter to restart the server(s) when finished or type **n**, then press Enter, if you do not want to restart server processes.

The script prompts you to verify your upgrade configuration settings.

14. Verify your settings, and if they are correct, type **y** then press Enter to proceed or type **n**, then press Enter, for the installer to return you to the original selection prompt.

The upgrade proceeds automatically with the installer performing the following actions:

- Extracts and decompresses the software payloads.
- Upgrades central manager
- Installs the HA server.
- Sets start scripts.

- Performs post-installation tasks such as removing the staging directory and starting the server processes (if configured).

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

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting purposes. The installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/GuiSrv/var/errorLog` subdirectory.

15. After the successful installation, copy the installer file `nsm2007.3r3_servers_cm.sh` to `/var/install` directory and run the following commands as follows:

```
rm -f NSM-CM
chmod 755 nsm2007.3r3_servers_cm.sh
ln -s nsm2007.3r3_servers_linux_cm.sh NSM-CM
```

4.3 Upgrading to NSM 2007.3 release on NSMXpress Appliance (OFFLINE Mode)

The section in this procedure steps on how to upgrade to NSM 2007.3 on the NSMXpress appliance if the NSMXpress Appliance is not connected to internet.

1. From NSM Software Download page, click the **NSMXpress Server** link.
2. Download the file `nsm2007.3r3_servers_upgrade_rs.zip`
3. From NSM Software Download page, click the **NSMXpress Server** link and **NSM Central Manager Offline Upgrade**.
4. Download the file `nsm2007.3r3_offline_upgrade.zip`.
5. FTP or SCP the following files onto your NSMXpress appliance. Download both files to the same location.

```
nsm2007.3r3_servers_upgrade_rs.zip
nsm2007.3r3_offline_upgrade.zip
```

6. Log in as the 'admin' user, and answer **n** when prompted to run the setup wizard.
7. Enter the following command, and then enter the 'admin' password to gain root access.

```
sudo su -
```

8. Confirm the unzip utility is present on the NSMCM appliance by executing the following command:

```
which unzip
```

This gives you the location of the file if it available. If it is not available, the unzip utility is provided on the NSM Software Download page. Use the following command to install this utility.

```
rpm -i unzip-5.51-9.EL4.5.i386.rpm
```

9. Navigate to the directory where you saved the management system installer file, which is typically the `/tmp/` subdirectory.
10. Execute the following command to unzip the files (`nsm2007.3r3_servers_rs.sh`, `upgrade-os.sh`) and create a directory (`apps-rpms`) in which NSMXpress saves the unzipped files.

```
unzip nsm2007.3r3_servers_upgrade_rs.zip
```

11. Run the following command to automatically start the installation.

```
sh upgrade-os.sh nsm2007.3r3_servers_linux_x86.sh Offline
```

The installer begins a series of pre-installation checks that ensure:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.
- You have installed a version of NetScreen-Security Manager preceding the current version you are installing.
- The system has sufficient disk space and RAM.

The installer then stops any running servers.

12. Type **2** to specify that you want to upgrade both device server and GUI server.

The installer next prompts you to configure additional options specific to your installation during the upgrade. This can include:

- Configuring high availability
- Configuring interoperability with NetScreen statistical report server
- Configuring backup options
- Configuring https ports

If applicable, follow the installer prompts to configure these options. The script next prompts if you want to restart the server(s) when finished.

13. Type **y** then press Enter to restart the server(s) when finished or type **n**, then press Enter, if you do not want to restart server processes.

The script prompts you to verify your upgrade configuration settings.

14. Verify your settings, and if they are correct, type **y** then press Enter to proceed or type **n**, then press Enter, for the installer to return you to the original selection prompt.

The upgrade proceeds automatically with the installer performing the following actions:

- Extracts and decompresses the software payloads.
- Upgrades the device server.
- Upgrades the GUI server.
- Installs the HA server.
- Sets start scripts.
- Performs post-installation tasks such as removing the staging directory and starting the server processes (if configured).

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

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting purposes. The installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/DevSvr/var/errorLog` subdirectory.

15. After the successful installation, copy the installer file `nsm2007.3r3_servers_rs.sh` to `/var/install` directory and run the following commands as follows:

```
rm -f NSM-RS
chmod 755 nsm2007.3r3_servers_linux_x86.sh
ln -s nsm2007.3r3_servers_linux_x86.sh NSM-RS
```

4.4 Upgrading to NSM 2007.3 release on NSM Central Manager Appliance (OFFLINE Mode)

The section in this procedure steps on how to upgrade to NSM 2007.3 on the NSM central manager appliance if the NSM Central Manager Appliance is not connected to internet.

1. From NSM Software Download page, click on the link Central Manager Server.
2. Download the file `nsm2007.3r3_servers_upgrade_cm.zip`
3. From NSM Software Download page, click on the link NSMXpress Server and NSM Central Manager Offline Upgrade
4. Download the file `nsm2007.3r3_offline_upgrade.zip`.
5. FTP or SCP the following files onto your NSMXpress appliance. Download both files to the same location.

```
nsm2007.3r3_servers_upgrade_rs.zip
nsm2007.3r3_offline_upgrade.zip
```

6. Log in as the 'admin' user, and enter `n` when prompted to run the setup wizard.

7. Enter the following command, and then enter the 'admin' password to gain root access.

```
sudo su -
```

8. Confirm the unzip utility is present on the NSMCM appliance by executing the following command:

```
which unzip
```

This gives you the location of the file if it is available. If it is not available, the unzip utility is provided on the NSM Software Download page. Use the following procedure to install this utility.

```
rpm -i unzip-5.51-9.EL4.5.i386.rpm
```

9. Navigate to the directory where you saved the management system installer file (typically the /tmp/ subdirectory).
10. Execute the following command to unzip the and save two files (nsm2007.3r3_servers_cm.sh, upgrade-os.sh) and a directory (apps-rpms) on the NSM central manager system:

```
unzip nsm2007.3r3_servers_upgrade_cm.zip
```

11. Run the following command to automatically start the installation.

```
sh upgrade-os.sh nsm2007.3r3_servers_cm.sh Offline
```

The installer begins a series of pre-installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.
- You have installed a version of NetScreen-Security Manager preceding the current version you are installing.
- The system has sufficient disk space and RAM.

The installer then stops any running servers.

12. Type **1** to specify that you want to upgrade central manager server.

The installer next prompts you to configure additional options specific to your installation during the upgrade. This can include:

- Configuring High Availability
- Configuring backup options
- Configuring https ports

13. If applicable, follow the installer prompts to configure these options

14. The script next prompts if you want to restart the server(s) when finished.
15. Type **y** then press Enter to restart the server(s) when finished or type **n**, then press Enter, if you do not want to restart server processes.

The script prompts you to verify your upgrade configuration settings.

16. Verify your settings, and if they are correct, type **y** then press Enter to proceed or type **n**, then press Enter, for the installer to return you to the original selection prompt.

The upgrade proceeds automatically with the installer performing the following actions:

- Extracts and decompresses the software payloads.
- Upgrades central manager
- Installs the HA server.
- Sets start scripts.
- Performs post-installation tasks such as removing the staging directory and starting the server processes (if configured).

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



NOTE: The management system installer indicates the results of its specific tasks and checks "Done" indicating 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.



NOTE: If you specify that you want to upgrade the central manger, all data previously configured in the system is restored. If you do not want to restore your previous configuration data, choose to have the installer perform a clean install of central manager.

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting purposes. The installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/GuiSrv/var/errorLog` subdirectory.

17. After the successful installation, copy the installer file (`nsm2007.3r3_servers_cm.sh`) to the `/var/install` directory and then run the following commands.

```
rm -f NSM-CM
chmod 755 nsm2007.3r3_servers_cm.sh
ln -s nsm2007.3r3_servers_linux_cm.sh NSM-CM
```

5 NSMXpress Data Migration

This section provides information on how to port data from an existing

- Solaris server to NSMXpress
- Linux server to NSMXpress

5.1 Solaris to NSMXpress Data Migration

On a Solaris Server

1. Upgrade the Solaris server to the latest NSM 2007.3 build.
2. Run setperms if NSM Server is running as root by using the following command:

```
/usr/netscreen/GuiSvr/utills/setperms.sh GuiSvr  
/usr/netscreen/DevSvr/utills/setperms.sh DevSvr
```
3. Change to “nsm” user using the following command:

```
su – nsm
```
4. Run the exporter using the following command:

```
./xdbExporter.sh /var/netscreen/GuiSvr/xdb /var/netscreen/GuiSvr/csvfile.txt
```
5. Use FTP to copy `csvfile.txt` to a common location.

On NSMXpress

1. On the NSMXpress server, upgrade to the latest NSM 2007.2 build.

The build on the NSMXpress server must match exactly with the build you upgraded on the Solaris server.
2. Change to “nsm” user with command `sudo su – nsm` and admin password.
3. Use FTP to copy the `csvfile.txt` to `/var/netscreen/GuiSvr`.
4. Stop the GuiSvr and DevSvr processes with the following commands,

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop  
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

5. Run Importer using the following command:

```
./xdifImporter.sh /var/netscreen/GuiSvr/csvfile.txt /var/netscreen/GuiSvr/xdp/init
```
6. Run xdbViewEdit using the following command and with the path of vi editor as /bin/vi,

```
/usr/netscreen/GuiSvr/utills/.xdbViewEdit.sh
```
7. Change the IP address in the server table to that of NSMXpress.

```
Option 7
0.server.0
0.server.1
```
8. Delete the RSA key data from the brackets of `ourRsaPrivateKey` and `theirRsaPublicKey` in the shadow_server table. Do not delete the whole line; delete only the key data inside the brackets.

```
Option 7
0.shadow_server.1
```
9. Copy the one-time password from the shadow_server table.
10. Change the one-time password in `devSvr.cfg` to match the one-time password in the shadow_server table.
 - a. Use the vi editor to edit the `/var/netscreen/DevSvr/devSvr.cfg` file.
 - b. Replace the one-time password to match the one-time password from the shadow_server table.
 - c. Delete the `ourRsaPrivateKey` and `theirRsaPublicKey` lines in `devSvr.cfg`.
11. Start GuiSvr and DevSvr by executing the following commands:

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh start
/usr/netscreen/DevSvr/bin/devSvr.sh start
```

5.2 Linux to NSMXpress Data Migration

This section describes how to port data from an existing Linux server to NSMXpress using the latest Netscreen-Security Manager (NSM) 2007.3 build. This section makes the following assumptions:

- The IP address of the existing Linux server will be assigned to the new NSMXpress server.
- The versions of NSM are the same on the current Linux installation and the new NSMXpress installation.

On a Linux Server:

1. Upgrade a Linux server to the latest NSM 2007.2 build.

2. Stop the nsm processes.

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop  
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

3. Run `setperms.sh` on the Linux server if the NSM server was running as root. (Refer to the NSM installer guide for information on running `setperms.sh`.)
4. Execute the following commands to back up the NSM database from GuiSvr to the `Guidb.tar` archive file.

```
cd /var/netscreen  
tar cvf Guidb.tar GuiSvr
```

5. If you want device logs to be migrated, execute the following commands to back up the NSM database from DevSvr to the `Devdb.tar` archive file.

```
cd /var/netscreen  
tar cvf Devdb.tar DevSvr
```

6. Transfer the `Guidb.tar` and `Devdb.tar` archive files to a place where they can be retrieved later.
7. Shut down the Linux server.

On NSMXpress:

1. Using `nsm-setup.sh` change the ip of the NSMXpress server to the Linux server ip / netmask / gateway. Clean install latest NSM 2007.2 build (same as that on Linux box) using `nsm_setup` utility.

2. Change to “nsm” user and enter the admin password.

```
sudo su - nsm
```

3. Stop the servers after the installation.

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop  
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

4. To avoid conflicts between the NSMXpress xdb database and the database in `GuiDb.tar`, delete the `xdb` subdirectory.

```
cd /var/netscreen/GuiSvr  
rm -rf xdb
```

5. Copy the `Guidb.tar` and `Devdb.tar` archive files to `/var/netscreen`.
6. Extract the database.

```
cd /var/netscreen ; tar xvf Guidb.tar  
cd /var/netscreen ; tar xvf Devdb.tar
```



NOTE: If you migrate only the GuiSvr database, execute Steps 7, 9, 10, and 11 of Section 4.1, “Solaris to NSMXpress Data Migration” on page 15 to delete the existing RSA keys between devSvr and guiSvr from the shadow_server table and devSvr.cfg, so that they can be re-negotiated and established again.

7. Start the GuiSvr and DevSvr processes.

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh start
/usr/netscreen/DevSvr/bin/devSvr.sh start
```

5.3 PGSQL Directory

After porting your data onto NSMXpress, all profile data is copied into the /pgsql directory. On NSMXpress, `pgsql` is a softlink and points to the following directory (on a separate partition), where in all the profiler related data is stored:

```
/var/netscreen/DevSvr/profiler_data
```

Manually move the contents of the /pgsql directory to profiler_data to separate the pgsq and log data on different partitions.

Separate pgsq Directory

After your database is untarred on NSMXpress, use the following steps to copy the pgsq directory to profiler_data to separate pgsq and log data on different partitions:

1. Navigate to the /pgsql directory by executing the following command.

```
cd /var/netscreen/DevSvr/pgsql
```
2. Copy the contents of the /pgsql directory to the /profiler_data directory

```
cp * /var/netscreen/DevSvr/profiler_data
```

Remove pgsq Directory

1. Execute the following commands to delete the /pgsql directory:

```
cd /var/netscreen/DevSvr/
rm -rf pgsq
```

2. Create a softlink for the /pgsql directory

```
ln -s /var/netscreen/DevSvr/profiler_data pgsq
```

6 User Privileges on NSMXpress

NSMXpress gives you the opportunity to execute commands with “root” privileges or “nsm” privileges and to switch back and forth.

- Log in as “admin” and execute the `sudo su - nsm` command any time you want to run an nsm-specific command, such as starting or stopping a service manually or running a CLI command.

- Log in as “admin” and execute the `sudo su -` command any time you want to reboot or shut down.
- Log in as “admin” to run the `nsm_setup` utility to configure various system settings and to install Regional Server or Central Manager.

The following procedure assumes you have initially logged in using “admin” and the default password “abc123”.

To change user privileges from user to admin:

1. Log in as an “nsm” user by entering the following command at the prompt:

```
[admin@NSMXpress ~]$ sudo su - nsm
Password: [admin password]
```

2. Change user privileges to “admin” by entering the following command at the prompt.

```
[nsm@NSMXpress ~]$ exit
```

3. Change to “root” by entering the following command at the prompt.

```
[admin@NSMXpress ~]$ sudo su -
Password: [admin password]
```

7 Addressed Issues

The following issues are addressed in this release.

- **293365**—When selecting the policy rules link in the override section of VPN Manager, the screen is not refreshed properly.
- **293065**—NSM is unable to create a sub-interface in a virtual system cluster without virtual security device 0
- **292579**—NSM does not create a core dump when running as non-root user.
- **291642**—When users in subdomains run the `guiSvrCLI` utility to update the attack database, the `guiSvrCli` utility updates all devices in all domains.
- **291558**—NSM upgrade changes rule-ids in a policy.
- **290219**—NSM generates an exception if the virtual router of a zone is changed while that zone has an interface configured to be monitored.
- **289542**—NSM `guiClient` is not refreshing views and device list properly.
- **288217**—While upgrading from 2007.3r1 to 2007.3r2 the 2007.3r2 installer prompts for the license file when the license is already installed.
- **285986**—Agent is unable to reconnect to NSM, after connectivity problems in high latency environment.
- **285360**—The IDP detector engine version is replaced by the ScreenOS version at the member level of a ISG-IDP cluster when you upgrade firmware.

- **282699**—Deleting a policy set may take several minutes in a system with a large number of devices and policy sets.
- **282695**—It takes several minutes to view the policy manager at login in a system with a large number of devices and policy sets.
- **282693**—Cancel button and the close dialog box button are unresponsive while using find usage for device templates.
- **282688**—While adding a device that has already been added, NSM displays the message that it is a duplicate serial number but does not provide any other information.
- **281071**—NSM does not trim extra spaces in policy names as ScreenOS does, causing an exception.
- **279273**—In an environment with a large number of devices, starting a secondary device server in an HA pair may cause a crash and failover if e-mail notification is configured on the device server.
- **279265**—Editing a template which contains a policy exposes a memory leak and may cause the GUI server manager process to stop.
- **277070**—Device config status is not updated in the UI without user interaction.
- **283173**—Drag and drop of a shared object does not work when the drop target is in a policy rule contained within a rule group.
- **279212**—Some policy rules may not appear in the UI client properly when switching sub-domains.
- **277625**—Setting VIP using same-as-untrust interface for an SSG550 is not possible. This results in validation errors while configuring VIP using the ip address of the untrust interface.
- **275528**—NSM primary server incorrectly failover to secondary server if the connection between the two is broken while in High Availability mode.
- **271557**—NSM cannot save vpn filter in VPN monitor.
- **267281**—NSM server installer permits install on 64 bit Linux OS even though that OS is not supported.
- **266262**—It may become impossible to execute directives (i.e. updates and imports) on devices in some subdomains. This problem is associated with systems where subdomains have been added or removed.
- **266108**—When right-clicking on device and selecting “Assign policy” and clicking “OK”, the device administrator information becomes blank.
- **265937**—Template operations do not correctly update the device sync status displayed in NSM.
- **263162**—When a secondary banner is set on a device, NSM reports incorrect values for the device sync status after server restart.

- **262995**—VPN manager adds extra static routes between branches in a main-branch topology when using “route options” for automatic route generation.
- **261479**—Can not delete a custom attack object if it is selected in Action Manager based alerts
- **261398**— The following options should be editable at cluster not at cluster member level:
 - Under Interfaces/Vlan1 interface:
 - - Bypass Non-IP Packet
 - - Bypass bcast/multicast non ip packet
 - - Bypass IPSec packets for others
 - - Enable DNS Proxy
 - Under Interfaces/Physical interfaces:
 - - DOT1x settings
 - - Policy-based Routing
- **260475**—Template operations do not list selectable cluster members under clusters.
- **258568**—When editing zones in the zone-based firewall or multicast rulebases, no pre/post rule options are available.
- **256793**—The expand all feature does not show all rules in the selected rule group.
- **254189**—Deleting VSYS from NSM causes VSYS interface in non-shared zone to become part of the root device.
- **253589**—Pre and post rules may be duplicated in Central Manager if a device is re-imported.
- **253208**—Install script uses /tmp to move old profiler data causing an out of disk space install failure.
- **241126**—When creating a dynamic group of attack objects, it is not possible to filter on a specific OS.
- **238454**—VPN related configuration is not correctly generated after a user changes route options in the VPN Manager.
- **236427**—When the syslog enable checkbox is set in a template, a syslog server definition is required. This is not correct behavior for a template.
- **234487**—Excessive redrawing of screens in the Policy Manager causes UI performance issues.

- **231946**—It is necessary to add a valid IP address to an interface in a template in order for the interface to be referenced as a source interface when adding an SNMP community. This should not be the case.
- **228605**—Log action options are not copied when dragged and dropped from one rule to another.
- **223573**—Adding rule after creating rulegroups creates duplicate IDs. This problem is not seen if rulegroups are not present.
- **223518**—Using custom CA certificates, when Best effort for Revocation checking method is used, these CLI's do not get updated to the device.

8 Known Issues

This section describes known issues with the current release. Known issues updates are released bi-monthly. You can subscribe to the updates by going to <http://www.juniper.net/customers/support> and selecting the Subscribe to Technical Bulletins option.

8.1 Limitations of Features

Installation of “Forward Support Update” files on NSMXpress must be performed using root privileges. You can temporarily acquire root privileges by executing the command “sudo su -” after which you can run the install script.

8.2 Known Issues in NSM 2007.3

This section describes known issues with the current release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:”.

- **280462**—Some custom attack signatures may appear in predefined attack groups.
- **277921**—SSG 550 and SSG 550M devices cannot be managed together in the same NSRP cluster. This is permitted by ScreenOS.
- **276431**—For redundant VPN configurations, the same vpns get listed in multiple groups.
- **275084**—Source or destination address filters in the log viewer do not allow application of address objects from the global domain. Only subdomain address objects are visible when creating the filter.
- **275027**—DELETED (predefined) object appears in IDP groups, when creating filter in the Log Viewer. 270452
- **273837**—Empty rulegroups may appear after filtering a policy rulebase. W/A: Expand rulegroups before filtering.
- **270452**—NSM does not support Screen OS 6.0R1.

- **270343**—It is not possible to select the loopback interface as the source interface for a device to use to connect back to nsm. It is possible to do so via device cli or web ui.
- **269510**—A redundant set interface command executed during configlet activation causes an error and activation fails.
- **259834**—If a dynamic untrust interface is selected as a tunnel interface source, an IP address (such as 10.88.x.y) should be generated to use as the next-hop address (for static routes and NHTB entries) on peer devices.
- **259141**—SSU does not work after specified time from drop down.
- **258759**—SSG 320/350 - The 8xGE and 16xGE PIMs present in the device cannot be seen in NSM
- **256538**—When VSYS name is created with 20 characters, NSM creates the VSYS in untrust with the truncated characters
- **254601**—NSM profiler shows static data in “Detailed View” for approximately 30 min.
- **252614**—NSM will not support configuring the Blacklist with a nonzero timeout value. Import of blacklist entries having non-zero timeout from Device not supported.
- **241230**—NSM GUI becomes blank for some-time while importing large number of VSYS existing in device. W/A: Launch another GUI for regular operation leaving the existing GUI to complete the task.
- **236415**—Defaults are set for some values in pre-defined interfaces in templates. Default values should not be set in templates.
- **235779**—Policy validation will result in an error with empty Polymorphic objects.
- **235765**—An error will occur if the destination address of a Policy in Central Manager has an empty Polymorphic address object and the policy is updated to the regional server.
- **233940**—Job Manager shows success for a failed profiler start directive.
- **233465**—NSM client does not get redirected to the master server if backup server MIP IP is used.
- **227458**—After auto-purge, the Application/Network/Violation profiler views no longer show data for some ISG devices.
- **226340**—VPN monitor does not save filters.
- **226083**—After upgrade to 2007.1r2, the setperms.sh script has to be executed such that all the processes are started as a non-root user.
- **226080**—Installer exits with a -1 error when the /etc/sysctl.conf parameters are not updated.

W/A: Add the Shared memory shmmax values in the respective configuration & reboot the NSM server before starting the upgrade.

- **225681**—NSM is setting improper src interface while updating the device after the RMA device.
- **224573**—Wireless Interface Configuration is not supported for SSG Wireless devices.
- **224319**—Log Investigator times out when the NSM GUI has been idle for 30 minutes and an error “Index Timed Out” is displayed.

W/A: Ignore the error and select OK for the query to happen again.

- **224045**—Policy rule groups creation is displayed incorrectly in audit log.
- **224044**—NSM audit log shows a generic entry when a template is created with missing data.
- **223661**—NSM does not allow defining Supplemental CLI commands on a Cluster.
- **223131**—NSM GUI does not allow creation of a sub-interface on a cluster level when VSD 0 is unset.

W/A: Contact JTAC for a workaround.

- **222554**—While re-installing the management system, the “Refresh” option does not prompt you to change previously configured server parameters.
- **221479**—NSM does not allow changing VSD group for NSRP lite.
- **219858**—VPN monitor displays the cluster member name instead of cluster members.
- **219702**—NSRP Monitor does not show correct information when one of the NSRP peer devices is powered off.
- **216303**—A route created in shared vr of a custom vsys is not available in the routing table of root vsys.
- **215443**—AuditLog viewer does not show the policy changes correctly.
- **212199**—If you update a device and the update is unsuccessful, the Audit Log Viewer “device” value is NULL.
- **210073**—Import of the device fails if keyword “admin” is used in the configuration.
- **209934**—Secondary NSM server is not configured on the IDP Sensor when the device is added to NSM. Sensor disconnects from NSM if primary server fails over to backup.

W/A: Use ACM to specify secondary server for each Sensor.

- **209464**—Invalid reference when trying to delete redundant sub-interface.

8.3 Known Issues in NSMXpress

This section describes known issues with NSMXpress. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:”

- **277916**—NSM does not check for dependencies when moving a loopback interface from one zone to another. This may result in a failure to update the device.
- **276518**—Running setperms.sh before migrating from NSM Server to NSMXpress is not necessary. W/A: Run setperms on NSMXpress after moving the data and before starting the services.
- **276251**—More than 10 administrators cannot be connected concurrently to NSMXpress.
- **270212**—It is not possible for the nsm user to manually execute scripts in /etc/init.d. W/A: Use scripts /usr/netscreen/[Gui|Dev|Ha]Svr/*.sh instead.
- **265342**—The root user is not blocked from attempting to restart HA server processes on NSMXpress. When root attempts to restart, the processes stop but do not start again. This restart should only be done by the nsm user.
- **263521**—HA installations using Shared Disk (new install or upgrade from 2007.2) may cause database backups to grow increasingly large. Remote backup of a new installation of NSM central manager with shared disk configuration may fail due to permissions of directories in /var/netscreen/DevSvr.

W/A: Run the following commands:

```
[admin@NSMXpress ~]$ sudo su -
[root@NSMXpress ~]# echo ".latest-db.backup/" >> /usr/netscreen/HaSvr/var/exclude.rsync
[root@NSMXpress ~]# echo ".latest-db.backup/" >> /usr/netscreen/HaSvr/var/excludeRemote.rsync
[root@NSMXpress ~]# echo "lost+found/" >> /usr/netscreen/HaSvr/var/exclude.rsync
[root@NSMXpress ~]# echo "lost+found/" >> /usr/netscreen/HaSvr/var/excludeRemote.rsync
[root@NSMXpress ~]# exit
```

- **263021**—When installing NSM using HA with Shared Disk, the secondary server must be installed with the following procedure:

1. Initial setup via serial cable, as normal.
2. Immediately after the initial setup and before opening the Web UI or using nsm_setup, run the following command:

```
# sudo rm -rf /usr/netscreen
```

3. Installation can proceed as normal, using either the Web UI or the nsm_setup command-line tool.

- **263006**—When installing NSM using HA with Shared Disk via the Web UI, an internal timeout may prevent all install messages from being displayed. All messages are displayed if NSM is installed using the `nsm_setup` command-line tool.

- **234330**—Root emails are not forwarded after changing the hostname.

W/A: After changing host name, enter the following command:

```
$ sudo /sbin/service sendmail reload
```

Alternatively you can reboot the system.

- **232842**—More than one static route cannot be added or deleted using `nsm_setup` script on NSMXpress.

W/A: You can add or delete routes manually.

- **231152**—Hostname configuration on NSMXpress consisting of 4 or more labels set through `nsm_setup` does not get updated in `resolv.conf` and host files.

W/A: Manually edit the `/etc/hosts` file.

- **225966**—Migration from software only installation to NSMXpress requires removal of `xdb` directory.

W/A: Refer to Section 4, “NSMXpress Data Migration,” on page 15 for steps to migrate NSM data.

8.4 Known Issues in ScreenOS 5.x Affecting NSM

The following are known issue in ScreenOS 5.x that specifically affects this release of NetScreen-Security Manager:

- **220967**—NSM is unable to add a device running ScreenOS 5.4r3 code if telnet is used as the method of initial connection.

W/A: Reboot the device and re-add the device in NSM.

- **197124**—While using NetScreen-Security Manager with DI enabled on an NS-500 device running ScreenOS 5.3, you may experience issues when downloading configurations larger than 1.7MB.

- **195025**—NetScreen-Security Manager reports an error when trying to set link-down an interface on an ISG 2000 device.

- **194320**—When upgrading a device from ScreenOS 5.0r10 and lower to ScreenOS 5.3, devices crash.

- **194266**—Devices running ScreenOS 5.3 may crash when generating Deep Inspection logs.

- **194211**—Wireless interface zone settings on devices running ScreenOS 5.3 are always displayed as “none” in the NetScreen-Security Manager UI.

- **193924**—It is not possible to set the bandwidth on interfaces for a VSYS in ScreenOS 5.3.
- **193654**—If you change the Device Server IP address, devices running ScreenOS 5.3 are not able to connect.

W/A: Perform an “RMA Device” and “Activate Device” workflow to continue managing the device.

- **193175**—You can not nest local user groups in ScreenOS 5.3.
- **192644**—NSRD in transparent mode is not functional in ScreenOS 5.3.
- **185847**—Using NetScreen-Security Manager to upgrade security devices running ScreenOS 5.0.0 over a slow network connection (if the image download takes over 5 minutes), occasionally causes updates to time out.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **179994 and 185048**—Devices are not able to save the key used to connect to the NetScreen-Security Manager Device Server. This causes the NSM agent on the security device to have to re-negotiate the key every time the security device restarts. The key re-negotiation process can take up to 15 seconds. One side effect of this issue is that when you restart the Device Server, this will also cause key renegotiation for all other security devices running it manages. This may cause system performance degradation that then affects the management of all security devices.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **171897**—It is not possible to create a configlet for a device in transparent mode.
- **174051**—If you use NetScreen-Security Manager to upgrade the firmware on a device from ScreenOS 5.0.0 to ScreenOS 5.1, the security device crashes.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

Table 1 describes specific releases of ScreenOS that resolve the issues referenced above or provides other workaround information.

Table 1: ScreenOS Releases for Specific Issues

Issue	5.0.0	5.0.0 r9 for 5000 M2	5.0.0-GPRS.r8.5	5.0.0 WLAN	5.0.0 r9 for ISG 1000/ISG 2000	5.0.0IDP1
185847	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2

Table 1: ScreenOS Releases for Specific Issues

Issue	5.0.0	5.0.0 r9 for 5000 M2	5.0.0-GPRS.r8.5	5.0.0 WLAN	5.0.0 r9 for ISG 1000/ISG 2000	5.0.0IDP1
179994 and 185048	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2
174051	5.0.0 r10	5.2	5.2	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2

9 Getting Help

For more assistance with Juniper Networks products, visit:

<http://www.juniper.net/support>

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your NetScreen device with Juniper Networks at the above web address.

Copyright © 2008 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners.

All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication 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:

Juniper Networks, Inc.
 ATTN: General Counsel
 1194 N. Mathilda Ave.
 Sunnyvale, CA 94089
 U.S.A.

<http://www.juniper.net>

