



NetScreen-Security Manager and NSMXpress Release Notes

8-27-07

Release 2007.2 Contents

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Upgrade Considerations on page 3
- 4 NSMXpress Data Migration on page 3
 - 4.1 Solaris to NSMXpress Data Migration on page 3
 - 4.2 Linux to NSMXpress Data Migration on page 5
 - 4.3 PGSQL Directory on page 6
- 5 User Privileges on NSMXpress on page 7
- 6 Addressed Issues on page 8
- 7 Known Issues on page 9
 - 7.1 Limitations of Features on page 9
 - 7.2 Known Issues in NSM 2007.2 on page 9
 - 7.3 Known Issues in NSMXpress on page 11
 - 7.4 Known Issues in ScreenOS 5.x Affecting NSM on page 12
- 8 Getting Help on page 14

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-021590-01 Rev B

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.

2 New Features

The following is a list of new features and enhancements in this NSM release:

- **Central Manager**—Features of the Central Manager include:
 - **Management of Regional Servers**—The primary function of your Central Manager will be the management of Regional Servers. From the Central Manager you will be able to add, delete and manage Regional Servers.
 - **Global Pre/Post Rules**—In NSM, a policy supports many kinds of rulebases. Each rulebase is an ordered list of rules. Pre-rules and Post-rule are two ordered lists of rules, which are defined on the Central Manager as part of a policy and pushed to the desired Regional Servers (Global Policy Install).
 - **Polymorphic Objects**—Pre/Post Rules defined on the Central Manager may use some shared objects where one or more fields may be defined in the context of the Regional Server to which the rules will be pushed. To provide the regional server admin the capability of customizing Central Manager pre/post rules to their specific environment, the concept of Polymorphic Objects has been established. In NSM, the following objects categories can have a polymorphic type: Address, Service, Zone, and NAT objects.
- **Regional Server**—Features of the Regional Server include:
 - **Pre-and-Post Domain Rules**—A Domain Administrator can specify a policy definition at a domain level that will apply to all devices within the specific domain and all subdomains. The rules can be applied as pre and post rules for any device in the given domain and subdomains.
 - **High Availability (HA) Enhancements**—These enhancements includes:
 - Improved database synchronization by utilizing database replication feature of Berkeley Database
 - Support for HA server running as a non-root process
 - Additional parameters to make HA control more configurable
 - Enhanced HA notification and logging mechanism.
 - **Identity Enabled Profiler**—This feature correlates UAC logs (user information) with Profiler Data (application information). It is available for use with ISG devices with IDP configurations and support for profiler. This feature provides administrators a view of what applications are being used at the user level. This feature will be released under a different name.

- **NSM Information Banner after Login**—Optional server-wide setting that allows the super administrator to create custom text that is shown on an information banner after login credentials are accepted by the NSM Server.
- **Job Manager Usability Enhancements**—The admin name associated with a submitted job is now displayed in the Job Manager to improve usability.
- **NSMXpress**—NSMXpress is an appliance version of NetScreen-Security Manager. It installs in minutes with full support for High Availability (HA), making it easy to scale and deploy. This fully-integrated appliance provides out of the box installation and Management of NSM. You can configure your NSMXpress to be a Central Manager (CM) of Regional Server(s).

3 Upgrade Considerations

Direct upgrade of NSM 2006.1r2 to NSM 2007.2r1 is not successful if the NSM server is run with “nsm” user permissions. The upgrade must be executed in two steps:

1. Upgrade the existing 2006.1r2 version to 2007.1r2.
2. Perform the upgrade from 2007.1r2 to 2007.2r1.

When managing IDPs or ISG-IDPs with Profiler enabled, the GUI server must have 2GB of memory.

4 NSMXpress Data Migration

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

- Solaris server to NSMXpress
- Linux server to NSMXpress

4.1 Solaris to NSMXpress Data Migration

On a Solaris Server

1. Upgrade the Solaris server to the latest NSM 2007.2 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. To avoid potentially conflicting transaction logs, perform the following steps.
 - a. Navigate to the `/var/netscreen/GuiSvr` directory.
 - b. Remove the `/xdb/log` directory.
 - c. Remove all files in the `/xdb/data` directory except the `DB_CONFIG` file.
 - d. Remove all files in the `/xdb/init` directory, but keep the `/xdb/init` directory.
6. Run Importer using the following command:

```
./xdifImporter.sh /var/netscreen/GuiSvr/csvfile.txt /var/netscreen/GuiSvr/xdb/init
```

7. Run `xdbViewEdit` using the following command and with the path of vi editor as `/bin/vi`,

```
/usr/netscreen/GuiSvr/utills/.xdbViewEdit.sh
```

8. Change the IP address in the server table to that of NSMXpress.

```
Option 7
0.server.0
0.server.1
```

9. 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
```

10. Copy the one-time password from the `shadow_server` table.
11. 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`.

12. Start GuiSvr and DevSvr by executing the following commands:

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

4.2 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) 2007.2 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/GuiSvr
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/DevSvr
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 transaction logs and the transaction logs 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/GuiSvr ; tar xvf Guidb.tar
cd /var/netscreen/DevSvr ; 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 3 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
```

4.3 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 `pgsql` and log data on different partitions.

Separate pgsql Directory

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

1. Navigate to the /pgsql directory by executing the following command.
`cd /var/netscreen/DevSvr/pgsql` command.
2. Copy the contents of the /pgsql directory to the /profiler_data directory
`cp * /var/netscreen/DevSvr/profiler_data`

Remove pgsql Directory

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

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

2. Create a softlink for the /pgsql directory

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

5 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]
```

6 Addressed Issues

The following issues are addressed in this release.

- **227609**—Bulk-add configlet assigns secondary devSvr IP as 0.0.0.0.
- **227240**—Long delay in drill down from custom reports.
- **227165** —When the HA server processes are reloaded on a secondary server running on Solaris 10, the heartbeat connected between the servers may be briefly interrupted.
- **226961**—Sensor cannot be added to the device using a MIP address.
- **223234**—When uploading firmware 5.4r2tmav and 5.4r2av-k to NSM, the incorrect version is updated to the device.
- **223176**—Template within a template required GUI client to restart for displaying values correctly.
- **223079**—NSM VPN Manager assigns in-use tunnel interfaces to VPNs.
- **221007**—HA replication working incorrectly with the older domain versions.
- **219859**—VPN Monitor filter does not display any information in the “ToHostname” column.
- **219303**—Custom attack signatures do not allow you to modify the supported platforms.
- **217407**—RSYNC process is not killed when HA Server process is stopped.
- **210914**—When filtering by “device group” under Log Viewer for the devices column, no logs are returned from the filter.
- **210576**—Last Modified Date should not be used for determining the changes to the attack signatures. To find the new or changed signatures, user should go to the job manager and check the job status after the security update is done in NSM.
- **191931**—NSM sends no CLI changes to the device after binding a VSI to a loopback group.

7 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.

7.1 Limitations of Features

Installation of “Forward Support Update” files on NSM*Xpress* 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.

7.2 Known Issues in NSM 2007.2

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:”.

- **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.
- **234729**—NSM incorrectly displays template overrides on device settings.
- **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.
- **232281**—Job failures are seen when “Summarize Delta Config” is run against thousands of devices at once.

W/A: Run Delta in small groups of devices.

- **231981**—Direct upgrade of NSM 2006.1r2 to NSM 2007.2r1 is not successful if the NSM server is run with “nsm” user permissions.

W/A: Upgrade from NSM 2006.1r2 to NSM 2007.1r2, then upgrade from NSM 2007.1r2 to NSM 2007.2r1.

- **231423**—Policy validation does not report shadowing for rules in rulegroups.
- **227489**—NSM Policy Merge tools aborts when merging very large policies.
- **227458**—After auto-purge, the Application/Network/Violation profiler views no longer show data for some ISG devices.
- **226886**—Unable to update the firmware for Cluster in NSM - does not show members when Update firmware is selected by right-clicking on the device.

W/A: Use updated firmware from the top menu.

- **226340**—VPN monitor does not save filters.
- **226231**—NSM sends wrong CLI when adding SNMP target IP to existing community.

W/A: 1. Delete the snmp community, update the device. 2. Add the snmp community back with all the snmp hosts including additional ones try to add early, update device again.

- **226147**—Configuration of Dead Peer Detection parameters in VPN IKE Gateway is currently not supported in NSM.
- **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.
- **225574**—Unable to select a local interface on the cluster members for setting the syslog parameters.
- **225020**—Real-time monitor does not show the status of SSG-550M devices.
- **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.
- **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.
- **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.

7.3 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:”.

- **234333**—Warning messages regarding NFS are seen when NSMXpress is configured with shared disk configuration.

W/A: Ignore these warning messages.

- **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.

- **229603**—Installation of NSM as a Regional Server fails on NSMXpress when HA is configured with shared disk.

W/A: When installing NSM Regional Server in HA with shared disk, the system must first be reverted to factory default from the boot menu.

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

W/A: Refer to Section 4, “NSMXpress Data Migration,” on page 3 for steps to migrate NSM data.

7.4 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
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

8 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 © 2007 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>