



# **NetScreen-Security Manager and NSMXpress Release Notes**

*11/14/07*

*Release 2007.2r2*

## ***Contents***

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Upgrade Considerations on page 3
- 4 Appliance Upgrade on page 3
- 5 NSMXpress Data Migration on page 5
  - 5.1 Solaris to NSMXpress Data Migration on page 5
  - 5.2 Linux to NSMXpress Data Migration on page 7
  - 5.3 PGSQL Directory on page 8
- 6 User Privileges on NSMXpress on page 9
- 7 Addressed Issues on page 9
- 8 Known Issues on page 11
  - 8.1 Limitations of Features on page 11
  - 8.2 Known Issues in NSM 2007.2r2 on page 11
  - 8.3 Known Issues in NSMXpress on page 13
  - 8.4 Known Issues in ScreenOS 5.x Affecting NSM on page 14
- 9 Getting Help on page 16

## **Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 530-021590-01 Rev C

## 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

---

If ScreenOS 6.0 devices are being managed, after upgrading to 2007.2r2, it is required to download the latest version of Forward Support Schema Update and install the same.

### 4 Appliance Upgrade

---

Use the following procedure to upgrade the NSMXpress appliance.

1. Confirm the unzip utility is present on the NSMXpress appliance by executing the below command:
 

```
which unzip
```

This would provide you the location of the file present. If not present, use the below procedure to install this utility:

  - a. Run the nsm\_setup utility.
  - b. Choose "System Security Update" - option 8
  - c. Choose "Check for and Install security updates now." - option 1
2. Load the NetScreen-Security Manager management system installer software onto the server where the NetScreen-Security Manager management system is currently installed. You can run the installer directly from the NetScreen-Security Manager installation CD. You can also copy the installer via SCP to a directory on the server, or you can download the installer from the Juniper Networks Customer Services Online web site.
3. Login as the admin user, and answer "n" when prompted to run the setup wizard.
4. Execute `sudo su -` and enter the admin password to gain root access
5. Navigate to the directory where you saved the management system installer file (typically the `/tmp/` subdirectory).
6. Execute the below command to unzip the file

```
unzip nsm2007.2r2_servers_linux_x86.zip
```

7. Run the management system installer.

On NSMXpress, run the following command:

```
sh nsm2007.2r2_servers_linux_x86.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.
- You have installed a version of NetScreen-Security Manager that precedes the current version that you are installing.
- The system has sufficient disk space and RAM.

The installer then stops any running servers.

The installer next prompts you to specify whether you want to perform a clean install or upgrade both the Device Server and GUI Server.

8. Type 2 to specify that you want to upgrade both the 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

9. If applicable, follow the installer prompts to configure these options. Refer to "Configuration Options" on page 6 for more information. 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" 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.

---



**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 both the Device Server and GUI Server.

---

10. Type y, then press <Enter> to restart the server(s) when finished. Type n, then press <Enter>, if you do not want to restart server processes. The script then prompts you to verify your upgrade configuration settings.
11. Verify your settings, and if they are correct, type y, then press <Enter> to proceed. If you type n, then press <Enter>, the installer returns you to the original selection prompt.

The upgrade proceeds automatically. The installer proceeds to perform 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 tmp subdirectory.

## 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 2007.2 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. Run Importer using the following command:

```
./xdifImporter.sh /var/netscreen/GuiSvr/csvfile.txt /var/netscreen/GuiSvr/xdb/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) 2007.2 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
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 5 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 `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 pgsq1 Directory

1. Execute the following commands to delete the /pgsq1 directory:

```
cd /var/netscreen/DevSvr/  
rm -rf pgsq1
```

2. Create a softlink for the /pgsq1 directory

```
ln -s /var/netscreen/DevSvr/profiler_data pgsq1
```

## 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.

- **217491**—When changing from a route based to a policy based VPN, it was not possible to terminate on a cluster - a cluster member had to be used.
- **225020**—Real-time monitor does not show the status of SSG-550M devices.

- **225574**—Unable to select a local interface on the cluster members for setting the syslog parameters.
- **226231**—NSM sends wrong CLI when adding SNMP target IP to existing community.
- **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.
- **227489**—NSM Policy Merge tools aborts when merging very large policies.
- **226683**—Spurious routes are generated by the VPN manager for some topologies.
- **227730**—Intermittent validation errors appeared in vrouter entries associated with a VSYS.
- **228826**—Summarize config does not export a complete PIM configuration.
- **228943**—When an Auth server is defined in NSM, only the first update to the device which includes the auth-server specific settings will be updated to the device. Subsequent changes to that auth server in NSM will not be pushed to the device.
- **231218**—When you first view the Device Configuration screen from the Auto IKE VPN window the middle column may not be expanded properly.
- **232281**—Job failures are seen when “Summarize Delta Config” is run against thousands of devices at once.
- **231404**—When running the validate policy feature, devices outside the current domain may be visible.
- **231423**—Policy validation does not report shadowing for rules in rulegroups.
- **231981**—Direct upgrade of NSM 2006.1r2 to NSM 2007.2r1 is not successful if the NSM server is run with “nsm” user permissions.
- **234508**—VPN Manager did not properly support the single tunnel interface option for ScreenOS 6.0.
- **234729**—NSM incorrectly displays template overrides on device settings.
- **236859**—SSG-520M/550M devices were not correctly recognized as supported by ScreenOS 5.4 in FIPS mode.
- **237354**—When VPN gateway entries are deleted, invalid references are seen causing errors.
- **238406**—After activating firewall with configlet and pushing first update, undefined reference errors are seen.
- **238989**—The guiSvrManager process failed due to mishandling of an error condition.

- **239564**—When RMA/Activating cluster members, some data is lost including vsd1 settings, ip address and snmp settings.
- **239996**—When a route based vpn is setup with tunnel interface bound to IP Un-numbered trust interface on both ends, the gateway used for the static route is set with the untrust ip (public ip) instead of the tunnel interface ip (which is the trust interface ip).
- **240157**—With vsd group 0 unset, shared interfaces residing in a vsys cluster are lost on import.
- **240444**—File permissions were set incorrectly by the setperms script.
- **241285**—While adding a template and adding a subobject, and then immediately deleting the subobject, a non-unique id would be recorded for the new template object.
- **241466**—The option to add logging options to policies created by VPN Manager is not available.
- **250307**—Drill down report view does not work after clicking the "Save All" option.
- **250943**—Rule IDs in log viewer are incorrect when using policy based vpn manager entries.
- **254115**—Address group cannot be viewed completely by readonly admin due to missing scroll bar.
- **255284**—Last Modified Date Filter for Dynamic Group was incorrectly removed from NSM.
- **258002**—Adding device Logaction criteria by selecting "Action Manager- > Device Logaction criteria" results in NSM GUI client hang.

## 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 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.

### 8.2 Known Issues in NSM 2007.2r2

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:”.

- **258568**—When editing zones in the zone-based firewall or multicast rulebases, no pre/post rule options are available.

W/A: Set the install-on column value to “any” and the problem will not be seen.

- **259349**—Global templates are not visible in sub domains, when logged in as Domain administrator.
- **240157**—Incorrect vsys delta config after device import.
- **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.
- **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.
- **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.

### 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:”.

- **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.

- **255125**—On re-import of a device with both firewall and multicast policies, either both policies must differ from the device policy or neither can differ. If this is not observed, then the re-import will hang at 84%. It is advisable to do delta-config summary before re-import to validate these conditions. Otherwise server restart may be needed.

- **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 5 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
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 © 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>