



Network and Security Manager Release Notes

***Release 2010.1
23 February 2010***

Contents

- 1** Version Summary on page 2
- 2** Before You Install NSM on page 2
- 3** Upgrade Considerations on page 2
- 4** Limitations on page 2
- 5** Important SSL VPN and Infranet Controller Instructions on page 3
- 6** Best Practices on page 8
- 7** Addressed Issues on page 10
- 8** Known Issues on page 15
- 9** Requesting Technical Support on page 30

**Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net**

1 Version Summary

Juniper Networks Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. With Network and Security Manager, Juniper Networks delivers integrated, policy-based security and network management for all security devices and other Juniper Networks devices in your networks. Network and Security Manager uses the technology developed for Juniper Networks ScreenOS to enable and simplify management support for previous and current versions of ScreenOS and now for JUNOS Software. By integrating management of all Juniper Networks devices, Network and Security Manager enhances the overall security and manageability of the Internet gateway.

NSM releases will henceforth be referred to by the year and the sequence of the release; for example, 2010.1, 2010.2. The previous convention of 'R' versions such as 2009.1r1 will be discontinued.

2 Before You Install NSM

Solaris Locales

Before installing NSM on a Solaris server, you must install a specific set of locales, and make appropriate edits to the `/etc/default/init` file. For more information, see the *Network and Security Manager Installation Guide*.

3 Upgrade Considerations

This section contains information about upgrading NSM and deprecated operating systems.

Upgrading NSM

You can upgrade to NSM 2010.1 from versions 2007.3RX, 2008.1RX, 2008.2RX, 2009.1r1 and 2009.1r1a.

NSM 2010.1 supports only 2000 devices with five user connections. Therefore, upgrade must be carefully considered.

Deprecated Operating System

NSM no longer supports ScreenOS version 4.X. You must upgrade your devices to ScreenOS version 5.0 or later.

4 Limitations

The following items are known limitations in this version of NSM:

- **For JUNOS Software for J Series and EX Series devices:** NSM Configuration Editor cannot completely validate the configuration that an NSM user has created before sending it to the device. The device validates the configuration when the configuration is pushed to the device as part of the Update Device job and may return validation errors to NSM.
- **For SSL VPN SA and Infranet Controllers:** Secure Virtual Workspace (SVW) settings on the SA device cannot be managed with NSM.
- **For EX Series switches:** EX Series switches running JUNOS Software do not support snapshots. Therefore, users should not select the **Backup the current filesystem(s)** on the device check box in the final page of the Install Device Software wizard.

5 Important SSL VPN and Infranet Controller Instructions

This section contains setup instructions and template usage guidelines for SSL VPN SA (SA) and Infranet Controller (IC) devices.

NSM Server

There is no limit to the number of devices that can be simultaneously updated in NSM, provided the configuration size on each device being updated is less than 5 MB. NSM can execute updates in parallel across a maximum of 8 devices while the remaining update jobs are queued up.

If the software version of SA/IC configurations exceeds 5 MB, we recommend a maximum of 4 devices per job for an appropriately sized Linux or Solaris server running NSM.

Due to hardware limitations on NSMXpress, the recommended limit is 2 devices per job for SA/ICs running configurations more than 5 MB.

The following files on the NSM software server must be edited as described below (no changes are needed for NSMXpress):

- In `/usr/netscreen/GuiSvr/bin/.guiSvrDirectiveHandler`, change **Xmx1024800000** to **Xmx2048000000**

```

$LIB_DIR/jre/bin/java -DNSROOT=$NSROOT
-DgproGDM=$DEST_DIR -DNSDIR=$DEST_DIR/var/be
-DSTART_PATH=$DEST_DIR -DBE_CFG=${CFG_FILE}
-DLOG4J_CFG=${LOG4J_CFG_FILE} -XX:PermSize=64M
-XX:MaxPermSize=64M -Xms128000000 - Xmx2048000000
com.netscreen.devicecomm.GUIDirectiveManager -version
-repo ${REPO_DEST_DIR} -conf ${SVC_CFG_FILE}

```
- In `/usr/netscreen/GuiSvr/var/xdb/data/DB_CONFIG`, change the `set_cachesize` parameter from **0 256000000 1** to **0 1024000000 4**
- In `/etc/sysctl.conf`, set the shared memory to a minimum of 1 GB (kernel.shmmax = **1073741824**).

- In `/usr/netscreen/GuiSvr/var/xdb/specs/jax.spec`, change **Xmx512** to **Xmx1024m**

```
:jvm-options (
: ("-DEMBEDDED_JVM=true")
: ("-Xms128m")
: ("-Xmx1024m")
```

- In `/usr/netscreen/DevSvr/bin/.devSvrDirectiveHandler`, change **Xmx102400000** to **Xmx204800000**

```
$LIB_DIR/jre/bin/java -DNSROOT = $NSROOT -DgproDDM = $DEST_DIR
-DNSDIR = $DEST_DIR/var/be -DSTART_PATH = $DEST_DIR
-DBE_CFG = ${CFG_FILE} -DLOG4J_CFG = ${LOG4J_CFG_FILE}
-XX:PermSize = 64M -XX:MaxPermSize = 64M -Xms128000000 -
Xmx204800000 com.netscreen.devicecomm.DeviceDirectiveManager
-version -repo ${REPO_DEST_DIR} -conf ${SVC_CFG_FILE}
```

The server processes must be restarted after you change these parameters.

Setting Up NSM to Work with Infranet Controller and Infranet Enforcer

A ScreenOS firewall that is managed by NSM can also be configured as an Infranet Enforcer in a UAC solution. To prevent conflicts between NSM and the Infranet Controller, configure these firewall devices as described in the following steps:

1. On the Infranet Controller, create the Infranet Enforcer instances:
 - a. On the Infranet Controller, select **UAC > Infranet Enforcer > Connection**.
 - b. Click **New Enforcer**.
 - c. Enter the information requested in the display.
 - d. Enter a password for the NACN password. You will use it again while setting up the Infranet Enforcer. If you are setting up a cluster instead of a single box, enter all the serial numbers in the cluster, one per line.
 - e. Click **Save Changes**.
 - f. Repeat Step 1b through Step 1e until all of your Infranet Enforcers have been entered.

2. If you do not have one already, create a CA certificate for each Infranet Enforcer.
 - a. Create a certificate signing request (CSR) for an Infranet Controller server certificate, and use the CA certificate to sign the server certificate.
 - b. Import the server certificate into the Infranet Controller.
 - c. Import the CA certificate into the Infranet Enforcer.
3. On each Infranet Enforcer, create the Infranet Controller instance:
 - a. On the Infranet Enforcer, select **Configuration > Infranet Auth > Controllers**.
 - b. Click **New**.
 - c. Enter the parameters as prompted. The password in the second section must be the NACN password you entered in Step 1.
 - d. Click **OK**.
 - e. Repeat Step 3b through Step 3d for all of the Infranet Enforcers.
 - f. On the Infranet Controller, select **UAC > Infranet Enforcer > Connection** and check that all the Infranet Enforcers have been added.
4. On NSM, delete the Infranet Enforcer firewalls from the global domain:
 - a. In the global domain, select **Device Manager > Devices** to list all the devices.
 - b. Right-click each Infranet Enforcer firewall device and select **Delete** from the list.
5. On NSM, delete the \$infranet instances from the Object Manager:
 - a. Select **Object Manager > Authentication Servers**.
 - b. Right-click each \$infranet_n object and select **Delete** from the list.
 - c. Select **VPN Manager > VPNs**, and check that you do not have any \$infranet objects under VPN Manager. These objects are usually deleted automatically when you remove the firewall.
6. Create a new subdomain for the Infranet Enforcers:
 - a. Select **Tools > Manage Administrators and Domains**.

- b. Select the **Subdomains** tab.
 - c. Click the Add icon.
 - d. In the New Subdomain dialog box, enter an appropriate name for the subdomain so you know what it will be used for, and then click **OK**.
 - e. From the drop-down list at the top left side, select your new domain. The new domain is empty, but it can use objects from the global domain. If you do not remove the \$infranet instances from the main domain you risk having duplicate \$infranet names. In addition, add a Single Infranet Enforcer or Infranet Enforcer Cluster.
 - f. Repeat Step 5 and Step 6 for every Infranet Enforcer or Infranet Enforcer Cluster you need to add to NSM. When finished, you should see \$infranet instead of \$infranet_# in each of the domains except global.
7. In NSM, add the Infranet Enforcer objects to the new domain:
- a. Select **Device Manager > Devices**.
 - b. Click the Add icon, and then select **Device** to start the Add Device Wizard.
 - c. In the New Device window, provide a name for the device, a color for its icon in NSM, and check **Device is Reachable**.
 - d. Follow the instructions in the wizard to add and import the device.
 - e. Repeat Step 7b through 7d for each Infranet Enforcer device.

You must reimport the configuration each time you use an Infranet Enforcer. Otherwise, a NACN password mismatch is possible because the Infranet Controller dynamically changes this password periodically. It is also good practice to do a "Summarize Delta Config" and ensure that no \$infra policies are present. If there are, the Infranet Controller has changed something on the Infranet Enforcer since you last imported the device configuration.

Note: If you choose not to reimport the configuration, be sure to update the Infranet Controller and Infranet Enforcer at the same time.

Usage Guidelines for Applying NSM Templates to SA and IC Clusters

SA/IC cluster configuration data is composed of Cluster Global (CG), Node-Specific (NS), and Node-Local (NL) data, which are abstracted in NSM as cluster objects and cluster member objects. The cluster object contains only CG data, while the cluster member object contains NS and NL data. Template promotion and application to clusters should be compliant with the cluster abstraction.

Recommended

- Templates that are applied to cluster objects should only include CG data. Templates that are applied to cluster member objects should only include NS/NL data. These guidelines apply to templates that are created from scratch or through promotion.
- To replicate the configuration from one cluster (source) to another cluster (target) through templates, promote the configuration from the source cluster object to a cluster template, and then apply that template to the target cluster object.
- To replicate the configuration from one cluster member (source) to another cluster member (target), promote the configuration from the source cluster member object to a member template, and then apply that template to the target cluster member object.

Not Recommended

- Do not apply any template that contains NS/NL data to a cluster object. Application of a template that contains NS/NL data can result in unexpected UI behavior and update results. (NS/NL data from the template could be ignored. NS/NL data in cluster objects is invisible.)
- Do not apply any template promoted from a cluster object or a standalone device to a cluster member object. Node-specific settings in the template appear in the member object but do not appear in the delta configuration. As a result, these settings appear in the template but are not pushed to the backend cluster node.

The following list shows the NS and NL configuration settings. All other settings are CG.

Node-Specific (NS) Configuration:

```
<nsm:path>/ive-sa:configuration/system/log/snmp</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/log/events-log-settings/syslog</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/log/user-access-log-settings/syslog</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/log/admin-access-log-settings/syslog</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/log/sensors-log-settings/syslog</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/network/network-overview/settings</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/network/external-port</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/network/internal-port
</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/network/management-po
rt</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/network/vlans</nsm:pa
th>
```

```
<nsm:path>/ive-sa:configuration/system/network/network-hosts
</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/network/network-conne
ct/network-ip-filter</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/system/clustering/properties
/configuration-settings/collection-of-network-settings</nsm:
path>
```

```
<nsm:path>/ive-sa:configuration/users/resource-policies/netw
ork-connect-policies/network-connect-node-specific-configura
tion</nsm:path>
```

```
<nsm:path>/ive-sa:configuration/authentication/auth-servers/
collection-of-auth-server/union-of-ace/active-directory-win-
nt/settings/advanced/computer-names/ive-name</nsm:path>
```

Node-Local (NL) Configuration:

```
/ive-sa:configuration/system/configuration/dmi-agent/enabled
```

```
/ive-sa:configuration/system/configuration/dmi-agent/device-
id
```

```
/ive-sa:configuration/system/configuration/dmi-agent/hmac-ke
y
```

```
/ive-sa:configuration/system/maintenance/push-config/accept-
push
```

6 Best Practices

This section contains information about recommended practices when using NSM.

6.1 Maintaining the NSM GUI Server

For optimal NSM server performance, follow these maintenance procedures every few months.

On the NSM GUI client:

- Delete old entries from the Job Manager in each domain.

- Purge old database versions using **Tool > Database Versions**.

If the size of the NSM database in `/usr/netscreen/GuiSvr/var/xd` continues to increase considerably despite the recommended practices, you can manually remove all domain versions using the procedure documented in KB11731. For details, see <http://kb.juniper.net/KB11731>.

6.2 Creating a Self-Signed TLS Certificate between the NSM Client and the NSM Server

A self-signed certificate is a certificate that has not been signed by a third party; such as a well-known Certificate Authority (CA).

Follow these steps to create a self-signed certificate between an NSM server and an NSM client:

1. Download the file `CreateCerts.zip` from http://kb.juniper.net/library/CUSTOMERSERVICE/GLOBAL_JTAC/BK14949/CreateCerts.zip

2. Copy the file to the NSM server and unzip it.

```
#unzip createCerts.zip
```

3. Edit the file `createCerts.sh` and modify the section **Default certificate generation fields** to update your current installation and the corresponding contact information of your organization.

```
0.organizationName_default = <Name of Customer's Organization>
stateOrProvinceName_default = <State>
localityName_default = <City>
countryName_default = <Country>
emailAddress_default = user@example.com
```

4. Run the shell script `#sh Createcerts.sh`

NOTE: The script produces a certificate with a timestamp that is nearly ten years beyond the current date.

The following is an example of the output when the script is executed.

```
root@nsm/]# sh createCerts.sh
Enter NSM installation path[/usr/netscreen]>
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Using configuration from cfg/openssl.cfg
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'State'
localityName :PRINTABLE:'City'
organizationName :PRINTABLE:'Name of the Organization'
commonName :PRINTABLE:'NSM'
emailAddress :IA5STRING:'user@example.com'
Certificate is to be certified until Aug 3 22:41:04 2019 GMT (3650 days)
```

```

Write out database with 1 new entries
Data Base Updated
Using configuration from cfg/openssl.cfg
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'State'
localityName :PRINTABLE:'City'
organizationName :PRINTABLE:'Name of the Organization'
commonName :PRINTABLE:'NSM'
emailAddress :IA5STRING:'user@example.com'
Certificate is to be certified until Aug 3 22:41:04 2019 GMT (3650 days)

```

```

Write out database with 1 new entries
Data Base Updated
Certificate was added to keystore
Certificate was added to keystore
[root@nsm/]#

```

This step creates 4 files root.pem, server.pem, truststore.ts, and keystore.ts

NOTE: The files truststore.ts and keystore.ts consist of private keys and must be protected.

5. On the NSM GUI server - Copy the files root.pem and server.pem to /usr/netscreen/GuiSvr/var/certDB/TrustedCA/
6. On the NSM client - Copy the file trustedstore.ts and keystore.ts to NSM_GUI_INSTALLATION/security directory. (default directory is C:\Program Files\Network & Security manager\security). Note that this must be executed on all systems where the client is installed.
7. Restart NSM GUI server services for a new certificate to be used: #/etc/init.d/guiSvr restart

If using a High Availability environment, execute: #/etc/init.d/haSvr restart.

7 Addressed Issues

This section includes issues addressed for NSM, ScreenOS, Secure Access SSL VPN SA Series, and Unified Access Control (UAC) Infranet Controllers. These release notes contain only NSM-related issues. For a complete list of addressed issues for each device, see the release notes associated with the device.

- 236415—NSM erroneously autopopulates interface settings in templates.
- 250830—NSM does not allow you to add SSG500 and SSG500M devices to the same cluster.
- 256770—A template operation directive may incorrectly remove passwords.

- 269588—gl29042 IDP clusters in third party HA configurations display a failed status at all times while IDP clusters in standalone HA installations display correct status.
- 275084—NSM does not display address objects from the global domain under filtered logs within a subdomain.
- 277921—NSM does not allow you to add both SSG550 and SSG550M devices to the same cluster.
- 283064—DSCP values are not exported when a policy is exported to HTML format.
- 289807—When configured, NSM fails to unset the BGP Neighbor route map.
- 290186—NSM does not allow grouping of multicast address objects.
- 294623—In NSM, you can accidentally create a firewall policy with a Policy ID (PID) that is already associated with another policy. If this happens, NSM displays a yellow warning message but allows the action to continue. Then NSM rennumbers the policy and pushes it to the device. However, NSM does not change the PID in the policy list. This can lead to inconsistencies such as a mismatch between policies and PIDs.
- 301001—NSM generates a validation error on subinterfaces based on aggregate interfaces when bandwidth is greater than 100 Mbps.
- 308927—NSM does not import the negate operator for a DI Custom attack.
- 392276—NSM does not remove BGP commands when unsetting a tunnel interface.
- 392731—The Search feature is missing some special characters.
- 394395—The NSM GUI does not display traffic logs.
- 397197—During an attack update in NSM, the GuiSvr manager restarts and performs a core dump.
- 398479—The devSvrLogWalker process crashes frequently.
- 402285—NSM fails to create an MIP on a device resulting in a device update failure when the MIP is included in a policy rule. However, the MIP can be created locally on the device and used.
- 405236, ScreenOS PR 408237—NSM does not provide an option for enabling an NTP server on a firewall running ScreenOS 6.X.
- 405802—NSM does not allow the manual mode setting for interfaces.
- 406401—NSM Security Explorer does not display top attacks or top attackers when an attack log is created.
- 411983—NSM attempts to set OSPF retransmit intervals even when the interface is not part of an OSPF area.
- 412776—If you create a custom view using an existing view, the custom view is not saved in the LogViewer.

- 414615—The NSM GUI is very slow.
- 415598—Importing a firewall into NSM generates a validation error.
- 421675—NSM does not generate unset commands correctly on devices running ScreenOS.
- 436368—NSM displays 'unset interface ethernet0/3 g-arp' in the delta config summary.
- 436779—Editing settings at the member level in NSM deletes settings in multiple clusters.
- 438346—VRRP support for devices running ScreenOS 6.0.
- 438686—Upgrades from ScreenOS release 5.4 to 6.1 in NSM causes template overrides at the cluster level.
- 438804—Deleting a virtual router from NSM also deletes the virtual router configuration on multiple clusters.
- 441419—NSM 2007.3r5 as well as NSM 2008 (with ScreenOS 6.1 schema) does not include the CLI: set flow vpn-tcp-mss and set flow tcp-mss.
- 442379—Tunnel interfaces belonging to shared virtual routers and zones are not available in the Vsys.
- 444462—Updates to devices running JUNOS fail if there are spaces in the name of the address object.
- 451634—NSM incorrectly displays differences immediately after creating a new policy version with the policy versioning tool.
- 453177—When you create a full mesh route-based VPN from the VPN Manager with a numbered tunnel interface and NHTB with next hop IP-enabled, and then you delete a device in the VPN setup and add the same device again, NSM generates a validation error on the tunnel interface. The previous NHTB entries are also lost.
- 454594—When a GRE over IPsec transport mode is selected for a VPN bound to a tunnel interface, NSM generates an error.
- 459772—When you right-click on a device in Device Manager, the software install list is blank.
- 460404—NSM 2008.2r2 does not support the ScreenOS 6.1 MGT zone for modeled SSG5 devices.
- 463817—On a modeled device running JUNOS software, you need to promote a template twice in order to update it. However, after you promote the template, previously edited device settings are erased from the device template.
- 466215—When you install NSM with a custom data directory, NSM changes the ownership and permissions of all files and folders present under the parent directory instead of modifying the custom data directory alone.

- 466534—When rules are dragged and dropped into Rulegroups, they appear randomly within the policy instead of within the Rulegroup.
- 466683—NSM generates wrong commands when a zone named 'dmz' is created on an NS5GT device.
- 467638—Setting up a TCP connection to port 7808 and then disconnecting causes many errors in the guidaemon log file.
- 468861—NSM does not allow editing of a vsys device.
- 469070—NSM does not allow the deletion of a device from Device Manager if it was part of a VPN with NHTB enabled.
- 469707—NSM displays an error when a VPN is configured to use an outgoing interface at a cluster level.
- 470179—Changing the IP address of a subinterface with OSPF causes an update failure.
- 470698—NSM does not provide an option for setting 'ssh known host' in SRX Series devices.
- 470709—After importing a configuration from the DHCP server, NSM changes the DHCP configuration and tries to update the DHCP server.
- 470784—NSM does not import the device configuration from file correctly. Some fields are either not imported or improperly displayed after import.
- 471128—NSM does not display a warning when a comment for an address object exceeds the supported number of characters.
- 471868—On an NS5400 device, NSM displays a warning that the max User_Zone 1023 is larger than the number of user zones supported by the device.
- 471965—NSM displays a warning when an address object contains more than 31 characters whereas ScreenOS 5.x permits it.
- 473282—NSM 2007.2r2 does not provide the option **avail_vip_same-as-untrust** for an SSG550 device running ScreenOS 6.0.
- 473595—An upgrade from NSM 2008.2 to 2009.1 causes API integration errors.
- 473614—NSM does not provide the option of configuring SSH known hosts on J Series routers running JUNOS 9.4 and later.
- 475784—NSM incorrectly displays denied logs of JUNOS 9.6 as permitted/ accepted.
- 475824—On an SRX Series device running NSM 2009.1r1, the values of **Bytes Total** and **Packets Total** are miscalculated.
- 475862—NSM does not provide a means to execute the ScreenOS 6.1 command 'set flow vpn-tcp-mss'.

- 475961—The NSM UI hangs indefinitely if the RMA/Activate procedure is not successful.
- 476808—The SNMP location field should be a member level setting and not a cluster level setting.
- 477349—If you select the **None** radio button in the NSM GUI, the context is un-initialized and data is lost. A workaround is to save your data before you click the **None** button and then restore the data after you select other options.
- 477575—NSM does not generate encryption commands to SRX Series gateways when AES is chosen as algorithm.
- 478227—After RMA, an SRX 650 device cannot be activated in the unreachable mode.
- 478487—If you remove a VPN created through the NSM VPN Manager, NSM fails to remove the tunnel interface from the zone while updating the device configuration, causing a commit failure.
- 480054—NSM does not allow you to set Certificate Authority revocation to **None**.
- 480114—When a user is created on the SRX Series device template, applied to the device, and the device is updated; NSM always displays differences in the delta config for the encrypted password configured in the template.
- 480558—The NSM UI client freezes when you create and save multiple rule groups.
- 480566—When the DHCP domain is set in a template, the CLI is not updated to an SSG5 device running ScreenOS 6.2.
- 480583—NSM does not provide an option to set policy based routing on redundant interfaces.
- 482295—NSM unsets DI pack on a device running ScreenOS if Base pack is selected.
- 484916—NSM settings for the minimum and maximum number of packet logs that can be stored in IDP devices need to be modified.
- 485633—NSM does not allow custom ICMP services without code values.
- 485646—During the initial update after importing a new device, NSM deletes console port configurations from the device.
- 485648—Device updates from NSM fail erroneously stating an application timeout.
- 485656—After importing a new device, NSM tries to change its priority of redundancy group value from 1 to 0.
- 485773—NSM incorrectly generates validation errors when importing group configurations from an SRX series device.
- 485897—NSM displays a validation error on predefined JUNOS GTP services.

- 488384—NSM does not delete custom zones defined in separate VSYS devices in separate subdomains.
- 491156—The NSM error message for duplication of objects is not sufficiently informative.
- 494878—During a fresh installation of NSM 2009.1r1a, predefined service objects are not converted to xdb.init.

8 Known Issues

This section describes known issues with the current release of NSM. Whenever possible, a workaround is suggested. These release notes contain issues related to NSM only. For a complete list of addressed issues for each device, see the release notes associated with the device.

8.1 NSM

- 266865—When you use NSM to edit a device's startup information and change the "Use Device Server Through MIP" setting to "Use Default Device Server IP Address and Port" or make the opposite change, NSM does not push the change to the device.
- 277604—Interface configuration screens show more settings than are supported by the actual interface.
- 277718—When you use NSM to set Antivirus (AV) parameters for a policy on a Juniper Secure Services Gateway (SSG) 300 Series device running ScreenOS 6.0r4, the new setting is not pushed to the device. However, NSM can be used successfully to send AV parameters settings to SSG 140 Series devices running ScreenOS 6.0r4.
- 277997—Device updates fail when a policy that references address objects for ScreenOS devices is assigned to a J Series device because the address object naming conventions for J Series devices are more restrictive than the naming conventions for ScreenOS devices. For J Series devices, the address object name must be a string that begins with a letter and consists of letters, numbers, dashes, and underscores. For ScreenOS devices, the address object name can include a combination of numbers, characters, and symbols. To ensure that a J Series device can use the Address Objects referenced by the security policy that is assigned to the J Series device, all address objects in that policy must follow the address object naming conventions for J Series devices. If the policy that is assigned to a J Series device contains preexisting address objects for ScreenOS devices, these address objects must be renamed to follow the same address object naming conventions for J Series devices.
- 284698—NSM users that do not have the 'View Security Policies' role can still see the policy node within devices that have their Policy Management Mode set to In-Device.

- 286643—When you create a virtual system device with '.' in the name, it causes the firmware upgrade to fail. The root device will reflect the change, but the virtual system does not.
- 287814—NSM users with IDP administrator credentials logged into a subdomain can edit shared address objects that are also visible in the global domain.
- 288309—For J Series routers in an NSM cluster, when the cluster member device reboots and reconnects to NSM, the hardware inventory displays **out-of-sync** in the Device list table. To work around this issue, execute the Reconcile Inventory directive to synchronize the inventory state of the device.
- 288993—When you customize a predefined report, guiSvrCli.sh does not generate it correctly and causes subsequent reports to fail.
- 291820—When you find shared objects within the Policy Manager, the window for groups may freeze. This situation occurs if you do the following in NSM:
 1. Select **Policy Manager > Security Policies**.
 2. Select a firewall policy.
 3. Find usages on a grouped address object in Shared Objects for the policy.
 4. Click on a link to a policy in the Rule Reference window.
 5. Close the Security Policy window, and click **Finish**. The NSM main window may change to gray with no information displayed.

You can recover from this condition by returning to the NSM security policy list and deselecting the previously selected policy.

- 292369—When you create a policy-based VPN and then update the device and import it back into NSM, the VPN rules previously created with VPN Manager and updated to the device are now imported in the new policy created under **Policy Manager > Security Policies**, and the new policy is assigned to the device. However, if the VPN is subsequently deleted by the user, the VPN and all rules associated with the VPN are removed from the VPN Manager, but not the Policy Manager policy. Before you can successfully update the devices, you must manually delete these VPN rules in the policy under Policy Manager.
- 292522—On a Secure Access SSL VPN SA Series device, when a user creates a resource profile, updates the device, and tries to add another bookmark, the new bookmark page does not show the **Host** and **Server port** values.
- 294769—When you use the script guiSvrCli.sh to generate reports by e-mail, the FTP fails even though the command shows a successful completion status.

- 295156—On a Secure Access SSL VPN SA Series device, the order of the policies within a SAM policy is not maintained when the SAM policy is edited with the NSM GUI.
- 295314—After the initial import of a device, the database version feature shows the user who performed the import as 'unknown.'
- 299504—When you promote a device with a medium-sized configuration to a template from the root configuration level, it is necessary to wait at least 1 minute for the change to take effect before opening the template.
- 299014—During an upgrade installation, license information is required to complete the installation.
- 302289—The virtual management Ethernet interface must be set as the management interface on the Virtual Chassis for it to be managed through NSM.
- 302500—If you perform a firmware upgrade from JUNOS 9.0 to 9.1 through the device UI (or CLI) and not through NSM, you must reimport the device in NSM and adjust the device's operating system version. To adjust the OS version in NSM, open Device Manager and right-click the device. Select either View/Reconcile Inventory or Adjust-OS Version. Ensure that the OS version running on the device matches the one recorded in the NSM database.
- In NSM 2008.2, the NSM UI connects with the GUI server through port 7808, which is FIPS compliant. When installation is complete, you see the following message: "Please note that TCP port 7808 is being used for server-UI communication". Earlier versions of NSM connected through port 7801, which was not FIPS compliant.
- 303308— Excessive retry operations can cause a DMI device to malfunction if NSM closes the connection to the device while the device is trying to connect to NSM. When you add a DMI device through the NSM UI, you first add an unreachable device and then use the generated key to configure the device so that the device can initiate the connection to the NSM server. The connection will fail, however, if NSM closes the connection because:
 - The device is in the modeled RMA state.
 - The device shares a duplicate sequence number with another managed device.
 - The platform or device type (cluster member, virtual chassis, and so on) you specified while adding the device does not match the device itself.

You can check for these conditions by examining the Configuration Status in the Device List. If the Configuration Status is "RMA," "Detected duplicate serial number," "Platform mismatch," or "Device type mismatch," delete the device immediately from NSM to prevent excessive connection retries from causing a device malfunction, such as exceeding the maxproc limit, or reaching 100% CPU utilization. To add the device again, make sure the platform type and device type specified in the device add workflow match those of the device itself.

- 304406—During an NSM installation in a HA environment, when performing a refresh with the NSM installer or NSMXpress UI, the HA peers may not initialize communication properly. This problem commonly occurs when you migrate from a single NSM server to a HA configuration. The error does not occur when you perform a clean install or an upgrade using the NSM installer.
- 305451—On a subinterface, the NSM template does not display a data origin icon under the Service Options.
- 313889—When you connect 3000 or more devices to NSM, the GUI client freezes for a couple of minutes because of the large number of notifications from the GUI server.
- If you add a JUNOS device to the NSM database through the reachable device workflow, you need to enable netconf for SSH (specific to system services) by running this command in the device CLI: **set system services netconf ssh**
- 394543—When you update the configurations of more than 30 devices together, the update device operation could take up to 10 minutes.
- 396285—The rebooting of NSM servers fails in a Solaris 10 environment. You can use either of these workarounds to start or stop an NSM server:
 - Use `/etc/init.d/guiSvr` and `/etc/init.d/devSvr` as the Root user.
 - Use `/usr/netscreen/GuiSvr/bin/guiSvr.sh` and `/usr/netscreen/DevSvr/bin/devSvr.sh` as an NSM user. You cannot use this script as the Root user.
- 400850—Physical interfaces do not appear in the PBR policy non-member list if you bind them to the same security zone as the redundant interface.
- 404479—NSM does not list physical interfaces imported to vsys or cluster vsys devices if they are configured in the shared zone. If the interface is not configured in the shared zone, NSM displays it in the interface list.
- If you add a JUNOS device to NSM through the unreachable workflow, execute the following commands on the device CLI to enable logging on it:


```
set system syslog file default-log-messages any
set system syslog file default-log-messages structured-data
```

- 404943—When the predefined service 'any-ip' is selected in a policy based VPN and the device updated, NSM generates an invalid CLI.
- 406791—After migration from NSM 2008.1R1 to 2008.2, editing a VPN results in a reference error under the manually created NHTB entry in NSM 2008.1R1.
- 407541—When you add JUNOS devices in cluster mode through the reachable device workflow, device status is "Import Needed" if you first add the primary and then the secondary device. To change the cluster status to Managed and In Sync, you must import the cluster. To work around this issue, first add the secondary device and then the primary device.
- 409350—After a software upgrade, a JUNOS device automatically transforms its configuration to work with the new version of the operating system. The transformed configuration needs to be imported to NSM after the upgrade. Please refer to the *NSM Administration Guide* for more details.
- 410009—When a large number of devices are discovered, topology discovery displays unconnected devices, connected devices and links as overlapping each other. The workaround is to manually drag unconnected device icons to free areas in the topology map, or view connected and unconnected devices separately.
- 422422—With every action, the NSM server increases its usage of memory which does not get freed later.
- 426324—The NSM guiSvrManager does not scale up to manage 6000 devices. You must limit the number of managed devices to a total of 3500 firewalls and DMI devices with 10K configurations and 5 GUI clients.
- 431058—Backup of XDB data fails when the GuiSvr data directory is not named "GuiSvr". This is because the path to the destination directory is hard coded in the backupLocal function of the .haScriptLib script.
- 431656—When a standalone IDP device is added through a non-reachable workflow, the device update operation fails.
- 437109—If you disable backup during a high availability installation of NSM, then manual backups using the script **replicateDb** present in **/usr/netscreen/HaSvr/utills/directory** are not allowed as well.
- 440152—In a high availability installation of NSMXpress, NSM 2007.3R5 does not failover as expected, when the disk partitions are completely utilized.
- 402298—When you apply a firewall policy with network address objects to devices running JUNOS Software, the device update operation in NSM fails, because DMI devices do not support network address objects.

- 443271—When a device reboots, the hardware-inventory status may be set to out-of-sync in NSM even when there is no change in the device's hardware. A workaround is to refresh the inventory. The status reverts to in-sync in NSM.
- 450863—NSM does not display a validation error if an IPv4 address is added to an IPv6 address group using the **Replace with** option.
- 450906—When an interface is configured in the IPv6 host/router mode, NSM does not show or generate the interface ID which is generated by default in the device. Instead NSM generates an interface ID randomly.
- 450964—When you log in to NSM for the first time on the NSMxpress appliance, the System Information page opens first instead of the Install NSM page.
- 452182—While searching for IPs using the Global Search feature, you can search for a specific IP address and netmask. However, you cannot search for all IP addresses in a particular subnet. You also cannot search for all IPs beginning or ending with a particular number.
- 452960—To create a multiple IP range DIP, you must configure the extended IP under two options: **Device supporting IPv6** and **Device not supporting IPv6**.
- 452898—The sequence of nodes under the Network tab changes when an interface is configured. Closing and reopening the interface window restores the original order of nodes.
- 453968—The Search option under IPv6 and IPv4 policies does not allow you to enter a complete string or word.
- 454983—The device cannot send the configuration file to the NSM server after a commit. The workaround is to run the `passwd cfmuser` command as root on the NSMxpress device and enter the same password configured at the install time.
- 455944—Under the Route-map, the Metric Options field entries and Local Preference values are not properly displayed on the template.
- 457072—In NSM, you cannot create node-specific entries for a cluster.
- 457242—The graph in myreport displays 0.0.0.0 before displaying the correct IPv6 address.
- 457557—When you log in to NSM as a custom administrator in a custom role with a **Create Security Policies** privilege and create a new policy with an IPv6 rulebase, a Java Null Pointer error is shown for the rulebase.
- 458585—NSM does not display a validation error for an invalid Attack Database Server path: **Device > Security > Expand Attack DB > Settings**.
- 459052—While creating gateway VPN settings, the NSM update often sends the following commands:

```

set ike gateway g1 dpd-liveness interval 0
set ike gateway g1 dpd-liveness retry 5
unset ike gateway g1 dpd-liveness always-send
unset ike gateway g1 dpd-liveness reconnect
unset ike gateway g1 nat-traversal

```

- 459323—NSM does not display validation error messages for low or high values under Destination or Source ports.
- 459330—NSM fails to update the PBR match-group, Action-Group and PBR policy names if the name string contains spaces.
- 459949—When AVT is enabled on a device, the Profiler is not automatically enabled during a device restart. The workaround is to right-click on the device and select Start profiler.
- 460492—When installing a system update on RHEL 4.6, you receive a warning for the SE Linux package. However, the installation works.
- 460645—The default screen view does not display all the options under Devices > Configuration > Update Device Config > ScreenOS and IDP options. The workaround is to extend the length of the window to view all the options.
- 460894—The NSM Object Manager does not display Zone object details.
- 461192—NSM displays all the interfaces under the Route-map > Match Interface list instead of displaying only the configured interfaces.
- 461266—NSM topology displays different icons for the M10i, MX480, J4300 and other routers.
- 463254—The order of nodes under the Network tab changes if the Transparent mode option is checked for a template. Closing and reopening the template restores the original order of nodes.
- 463559—When you use the Import Device config option to import a configuration file, NSM displays a validation error for the serial number.
- 463738—When you model a device enabled with a transparent interface, the interface is incorrectly displayed as Route mode in the device configuration, and you cannot edit the mode field.
- 463788—The NSM UI displays a validation error for Route-map strings when Route-maps are configured without any entries such as permit/deny, match, set and Metric Parameters.
- 464029—NSM incorrectly displays the validation **IP Address can't be unset since it's being used by VPN** on an IPv6 VPN though the IPv6 address is part of the VPN.
- 464071—SCTP, UTM and GTP objects are visible in the expanded display mode after they have been deleted from the policy.
- 464094—NSM allows you to create IPv6-based DIP objects when the IPv6 mode is set to none.

- 464145—The VPN monitor does not display content for the Local address and Peer address fields.
- 464404—When existing custom virtual routes are configured using a template, you see a **Revert to template/default value** option when you right-click on the virtual router name field. If you select this option, the virtual router name becomes a null value and you see a validation error.
- 464834—In the NSMXpress multi-user access feature, you can map predefined users such as nsm and cfmuser to have access to the WebUI. However, these predefined users cannot log in because they do not have the defined password. We recommend that you do not map predefined users to WebUI users through Unix authentication.
- 465023—The quick configuration editor Interfaces page is not refreshed when an interface is edited from a regular config editor. Functional zone tables are not validated when any node under functional zones is configured.
- 465407—NSM allows you to configure IPv6 options on a device running ScreenOS 6.3 even after IPv6 is disabled on that device.
- 465748—If you try to download the NSM client from an NSMXpress appliance with a different NSM UI client version, NSM prompts you to download the client from the server, but the download fails. A workaround is to download the client directly from the NSM server (<https://<ApplianceIp>/>) or change the guiSvrWebProxy.port value to 443 in `/var/netscreen/GuiSvr/guiSvr.cfg`.
- 466039—The Interface Quick Configuration landing page usually shows **Could not Create View** for EX Series, MX Series and SRX Series devices.
- 466233—After configuration, the routing table of model vsys devices does not display IPv6 route entries. However, the same route entries are visible in the delta config summary and are successfully updated in the device. A workaround is to import the vsys device.
- 466335—You cannot change the superuser password from the WebUI of an NSMXpress device.
- 466349—NSM does not filter IPv6 policy rules from the Central Manager during an update to a ScreenOS device that does not support IPv6.
- 466934—The NSM database backup operation fails to execute from the WebUI on NSMXpress devices. The workaround is to log off, log back in and execute the operation again.
- 467745—The NSM 2008.2r2 client often displays an empty device list.
- 468189—When migrating from NSM 2008.2R2a to 2009.1, the installer script does not display the version correctly. NSM 2008.2r2a is displayed as 2008.2r2.

- 470405—An NSM installation on an NFS environment hangs during the execution of the nacnCertGeneration script.
- 472185—The NSM Device monitor and the VPN Monitor are slow to detect changes in state.
- 473963—During a shared disk installation on an NSM appliance, you receive an error message that the password for the Device Server is too short and that the minimum length should be 8 characters.
- 474008—When you install a regional server on a new NSMXpress appliance through the WebUI or nsm_setup, you occasionally see the following message: **Stopping NFS staid: [FAILED]**. However, the installation is successful.
- 474518—The check box option for enabling NTP on redundant interfaces within NSM is missing.
- 475084—You cannot create a user with a Unix authentication password option in the NSMXpress User list.
- 477214—The reboot device operation does not work for devices added in a non-reachable work-flow.
- 477341—Under **Security Policies > Shared objects**, a fast scroll Screen refresh does not happen properly.
- 477347—In NSM 2009.X, under **Security Policies > Shared objects**, the Search feature for services is slower than in previous releases.
- 477352—After you create an object under **Security Policies > Shared objects**, NSM takes time to refresh the screen.
- 477355—The JUNOS software does not validate configurations from NSM.
- 478484—During a regional server installation on an NSMXpress appliance, you see the following error message at the post-installation tasks stage:


```
"No such file or directory" (/bin/cp: cannot stat
`/usr/netscreen/GuiSvr/var/metadata_table.nml': "var/install/NSM-RS).
However, the installation is successful.
```
- 479624—When you edit virtual routers with large numbers of static routes and ACL entries, the CPU utilization of the NSM GUI is very high.
- 479859—NSM incorrectly allows you to create address objects called ANY-IPv4 and ANY-IPv6.
- 480429—Device Statistics do not display policy distribution information.
- 481088—The SMTP Protocol Anomaly attack object does not contain recommended actions.
- 481124—A DI signature is displayed as member of the IDP dynamic attack group.

- 481645—NSM does not set a warning flag for IPv6 address objects containing duplicate networks.
- 484205—Community list commands for Border Gateway Protocols in the device differ from those in the job information.
- 484701—When selecting rules in a complex policy (around 1000 rules), the NSM GUI of release 2009.1r1 responds more slowly than in release 2007.3r4.
- 486191—After an upgrade on NSMXpress, you must manually delete the file **nsm-scripti-vals.new** if available under the **/tmp** directory. You must then reconfigure NSMXpress through **nsm_setup**.
- 488187—When you install NSM3000, disk partitioning may fail on the first attempt. The workaround is to erase the disk and reinstall the appliance.
- 489761—In an extended high availability setup, DMI devices do not reconnect to NSM after a GUI server failover. The workaround is to restart the Device server.
- 493491—The **Random-port** option is not available when configuring DIP on an interface running ScreenOS.
- 495586—NSM reorders NAT rules incorrectly on an SRX device cluster member.
- 495927—In the Policy Manager, if you select a rule containing either a source or destination IPv6 address and right-click on it, the **Add Address** and **Filter** options are not available. The workaround is to directly right-click on the rule without first selecting it.
- 496118—NSM fails to update an ISG2000 cluster with a 'Manage-IP of redundant IP' configuration.
- 496177—On an ISG2000 device, updating a physical interface with an IPv6 prefix list fails.
- 496199—On an IPv6-disabled device, configuring an IPv4 neighbor in BGP causes NSM to wrongly update IPv6 configurations leading to an update failure.
- 496395—When you apply an OSPF and BGP-enabled template to a device, NSM displays a validation error for the **Virtual router ID** under **VR**.
- 496431—On an ISG2000 device, NSM pushes the redundant interface configuration on every update of the device.
- 496701—After upgrading an ISG2000 running ScreenOS 6.2 to release 6.3 through the NSM Software Manager, NSM wrongly creates CLI 'set cpu-protection threshold 0' causing updates to fail.
- 496705—When you configure DIP for an interface in a ScreenOS template, the Wizard is not displayed completely. The workaround is to drag the wizard open completely. On subsequent edits, the wizard opens in the same size as dragged earlier.

- 496721—After a peer group member is removed from a peer group in BGP and the device updated, NSM does not delete the member from the group.
- 497112—If an IDP policy with all filters enabled in a dynamic attack group is pushed to an SRX3600 device, the update fails.
- 497349—You are unable to validate J series devices through NSM.
- 497949—NSM incorrectly allows the same user role to be added as both member and non-member of a user group in an IDP policy.
- 498731—On an ISG1000 cluster running ScreenOS 6.2 or lower, NSM erroneously displays the IPv6 tab on the VSI interface.
- 498733—The NSM GUI does not provide a check box for enabling **Track IP** under **VSD Group Monitoring** for cluster members.
- 499146—After an RMA/Activate of an NS204 device, the NSM server primary interface displays a delta.
- 499174—When service applications are configured on policies in a JUNOS device template and applied to devices through NSM, the update fails.
- 499181—The NSM GUI erroneously displays the **Gateway Tracking On** option for IPV6 destination based routes. IPV6 routes do not support this feature causing the update to fail.
- 499642—While executing Get Delta Config Summary and Update directives, NSM reports an error 'Failed to acquire lock on device' even when no other user is logged in.
- 501774—When a port template configuration is pushed to an EX series switch, Device Connectivity status goes down and then comes up.
- 502716—While updating IDP policies on an MX960 router, NSM only updates the name of the policy but not its contents such as address, attacks, action, notification and so on.
- 503701—When selecting enforcement points to associate with ICs on an EX series switch, the NSM GUI does not display the **Select Cluster Member** option. Drag the window open to see an extra field for selecting IC A/A cluster members.
- 504876—NSM is unable to connect with EX8216 switches running JUNOS 10.0r1.8.
- 504886—When a device is added through any workflow, NSM requires you to perform an import device config operation before you can view the **Advanced > Predefined Service Session cache > Predefined Services** option.
- 505299—Under Device Discovery rules, NSM is unable to discover J4350 and J6350 devices.

- 506135—NSM does not display variables for a query expression in the filter node under **Configuration > System > Log monitoring**. You can however, create a query expression in a template where these variables are visible and successfully update a device in NSM with the template.

8.2 EX Series Switches

- 271590—Deleting the “system services outbound-ssh” stanza does not cause existing connections to be dropped.
- 394552—NSM allows you to apply Layer 2 Uplink port templates on LAG interfaces (ports names beginning with ‘ae’). NSM cannot automatically detect whether a LAG interface is deleted from the switch configuration after you apply the port template. It is therefore recommended that you manually remove the LAG interface from the ports associated with this template.
- 398326—After enabling the automatic import of configuration files on an EX Series switch running JUNOS Software versions prior to 9.3R2 and 9.2R3, you need to manually add the NSM Device Server as a known host to the switch. To do this, log into the EX Series switch through Telnet or SSH and then SSH to the NSM Device Server IP. This adds the NSM Device Server as a known host in the switch. Without this manual intervention, automatic import of config files does not take place from EX Series switches.

You do not need to perform this step for EX Series devices running JUNOS 9.2R3 or 9.3R2.

- 398860—If you use LLDP, IP phones connected to 9.2R1.10 EX Series switches are not discovered. You need to upgrade to EX Series 9.2R2.15 or later.
- 402243—On a virtual chassis, if there is a physical link through the vme0 interface to an adjacent EX Series switch, topology discovery records two links, one from the vme interface and another from the me0 interface.
- 406887—Topology discovery commits data in small chunks to the database. If one of many such transactions fails, the remaining data is not committed. This could create inconsistent data in the database.
- 427855—When both master and backup router engines in a grande device are reachable by SNMP, topology discovery displays it as two separate devices in the topology map.
- 444091—Wrong links are discovered with EX8200 devices with only STP/RSTP. Enable LLDP on all the switches to ensure that links are discovered properly.
- 446950—Because of a UI issue, NSM incorrectly allows you to create virtual chassis with EX3200-24P. Virtual chassis should be created with EX4200 platforms only.

8.3 Devices Running ScreenOS and IDP

- 294030—On an ISG device, sufficient device memory is required to compile the policy during an update from NSM. A policy that specifies **All attacks** needs 600 MB or more RAM on the device. The update fails if the amount of RAM is insufficient. You can contact JTAC for a workaround.
- 431638—Enabling IPv6 support in an NS500 device causes the firewall policy update to fail.
- 436587—In NSM 2008.1, the value of the NHRP field in the vrouter schema is **True**, thereby enabling NHRP on all v routers by default. In NSM 2008.2R2, the NHRP default value is **False**. Migrating from either NSM 2008.1R2 or NSM 2008.2R1 to NSM 2008.2R2 ensures that wrongly enabled v routers are reset.
- 437457—When you update an ICAP profile in a vsys device, the update fails. The workaround is:
 1. Add an ICAP server to NSM from Object Manager > ICAP > Server & Server groups.
 2. Create a custom ICAP profile by adding the new ICAP server from Object Manager > UTM > ScreenOS > ICAP > Custom Profiles.
 3. Apply the ICAP profile and update the root device.
 4. Add any vsys device to NSM.
 5. Create a policy in the vsys device and assign the ICAP profile to it.
 6. Save, and update the vsys device.
- 438631—When an IDP device is upgraded from 4.1R3 to 5.0, the IDP configuration files are not imported to NSM. This is because the packet capture settings in IDP 5.0 devices are configurable from NSM, and are limited to 1000-65535, unlike in IDP 4.1R3 devices.
- 446392—When migrating from 2007.3R1 to 2008.2R2, NSM unsets the loopback and subinterface configurations created in the 2007.3R1 setup. Migration from 2007.3R4 to 2008.2R2 succeeds.
- 450906—When IPv6 is enabled on an interface in host mode, NSM does not generate any interface ID unless configured by the user whereas ScreenOS does, causing a mismatch. A workaround is to import the device into NSM after you update the IPv6 settings.
- 454755—ScreenOS does not treat DI profiles as standard shared objects. Hence NSM does not reflect changes in the profiles after you import a device.
- 458945—NSM cannot manage a device running a ScreenOS version earlier than 6.3 with IPv6 configuration. For NSM to effectively manage the device, it needs to be upgraded to ScreenOS 6.3 and added or imported into NSM.
- 461167—You cannot export device logs using the syslog option from the NSMxpress WebUI.

- 461181—Updating fails when a policy with web filtering enabled is pushed to a vsys device from NSM.
- 461986—You cannot generate reports and e-mail them using the email.sh option in the NSMXpress appliance.
- 462408—NSM displays **Unable to acquire lock, Locked by admin, Open read-only** when you edit a device. This issue has been observed when editing an ISG200 cluster member and also on a J6350 device. This issue is not always reproducible. The workaround for this problem is to restart the GuiSvr.
- 464396—On a modeled ScreenOS root device with a modeled vsys device, NSM does not display the IPv6 option on the modeled vsys.
- 464517—When a rule is added to a policy and the Notify Closed Session option is enabled, NSM shows the 'unset IDP' command in the delta configuration. If IDP is enabled on the device, IDP does not get unset.
- 465144—NSM does not display the option to monitor the IDP security module under the VSD group monitoring section.
- 478268—An update to an SRX Series device fails if the **Confirmed commit** option is enabled in the GUI.
- 479370—NSM does not generate dead peer detection configuration for IKE gateways on SRX Series devices.
- 481066—SRX Series device with IDP logs contain Severity level information while other fields are not mapped.
- 489282—When you update an SSG5 running ScreenOS 6.1, NSM unsets eth0/0 and BGP even when an eth 0/0 change is unnecessary and BGP is not enabled. The workaround is to enable BGP on tunnel 1.1.
- 490931—The NSM devSvr Manager crashes during the import of an IDP device
- 497114—Updates to an SRX3600 device fail because NSM repeatedly displays a hardware OutofSync message. The workaround is to manually right-click on the device and reconcile inventory.
- 497120—Updating an SRX3600 device with an IDP policy fails, displaying a 'Previous commit is in progress' error message. The workaround is to wait for several minutes until the back-end commit process is completed.

8.4 Secure Access SSL VPN SA Series and United Access Control Infranet Controllers

- 436750—NSM cannot import an IC if the IC has more than 5100 resource access policies. The import operation does not complete.
- 455844—Deleting an SA device object from NSM does not remove the object until services are restarted. This is seen intermittently.

- 460586—When a JUNOS SA/IC template is removed from a device, the template values are not retained even if the **Retain Template values on removal** option is checked.
- 465450—While creating a new custom expression under Role mapping, if you choose Directory/Attribute: as any LDAP server on NSM when you configure the User/Admin/MAC Realm General settings, the update to an SA/IC device fails.
- 502390—If you use NSM 2009.1 and intend to upload either the SA 6.5r2 or IC C3.1r2 software into NSM, you must run a Juniper Update to enable subsequent device software upgrades through NSM.

8.5 SRX Series Services Gateways

- 312509—When you configure the Network Address Translation (NAT) rule set on an SRX Series device running JUNOS 9.2, it is not imported correctly into NSM.
- 395329—NSM cannot update the following attacks to SRX Series devices:
 - All attacks
 - Product filter as part of a dynamic attack group
 - Anomalies as part of a compound attack group
 - Recommended filter as part of a dynamic attack group where the value is set to false
- If your previous NSM release managed IDP devices and you migrate to NSM 2008.2 enabling the FIPS mode, the IDP device connection status is down. You should reconnect all IDP devices to the FIPS-enabled 2008.2 NSM server. This happens because earlier NSM versions used MD5 HA to store device fingerprints while FIPS compliance requires SHA-1. However, if the server is migrated to a non-FIPS 2008.2 setup then devices are connected automatically.
- 430886—In order to add J Series and SRX Series devices configured in cluster mode, the secondary cluster member needs to be added / imported, followed by an add/import of the primary device.
- 439567—Since IDP and ISG devices support multiple services, NSM also allows multiple services to be added in an IDP policy. However since SRX Series devices do not support multiple services in IDP policies, a device update fails after a service field is changed in the IDP policy. To workaround this issue, select only one service when using an IDP rule with SRX devices.
- 439732—An upgrade of an SRX210-hm device from JUNOS 9.4R1.8 to 9.4R2.9 fails.
- 448239—Predefined IDP policies cannot be pushed to an SRX Series device. The workaround is to create the custom policy from the predefined policy, and then delete the disabled rule in the custom policy before making a policy update.

- 449045—When deleting the SRX family of devices, certain Java exception errors are logged into the file gproGDM.log of the GuiSvr errorlog directory.
- 450626—Update fails on an SRX Series cluster when the Dynamic Db option is selected. The workaround is to disable the Dynamic Db option.
- 452275—VLAN configurations are not applicable for SRX3400, SRX3600,SRX5600 and SRX5800 devices. However, the configuration editor and the quick configuration editor list the VLAN configurations.
- 458973—NSM displays validation errors under all occurrences of 'isis' node when the JUNOS 9.6 schema is applied. This issue is seen on all J Series and SRX Series devices.
- 460593—The system services RSH and Rlogin are not configurable from NSM.
- 461264—At times, an update on an SRX Series device fails with the error message **Previous commit in progress**. A workaround is to add the device again.
- 477359—The private edit mode used in SRX Series clusters does not block NSM.
- 480097—You cannot add an SRX Series cluster member in the auto-import configuration list.

9 Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/customers/support/downloads/710059.pdf>
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

9.1 Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>

- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at <https://tools.juniper.net/SerialNumberEntitlementSearch/>.

9.2 Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>

If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number

Software release version (not required for *Network Operations Guides* [NOGs])

Copyright © 2010; Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.