



# **Network and Security Manager Release Notes**

***Release 2009.1r1a  
18 November 2009***

## ***Contents***

- 1** Version Summary on page 2
- 2** New Features on page 2
- 3** Before You Install NSM on page 6
- 4** Upgrade Considerations on page 6
- 5** Limitations on page 7
- 6** Important SSL VPN and Infranet Controller Instructions on page 7
- 7** Best Practices on page 13
- 8** Addressed Issues on page 15
- 9** Known Issues on page 17
- 10** Requesting Technical Support on page 30

**Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089  
USA  
408-745-2000  
[www.juniper.net](http://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.

## 2 New Features

---

The following is a list of new features and enhancements in the 2009.1 release of NSM:

- **Element management for supported devices.** NSM provides element management support for:
  - SRX3600, SRX3400, SRX5600, SRX5800 gateways on JUNOS 9.4 and JUNOS 9.5. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Configuration File Management, Inventory Management, Logging, Software Image Management, Status Monitoring and Schema Update.
  - SRX240 Modular platform and SRX650 Modular platform. NSM supports the SRX100 Fixed platform on JUNOS 9.6. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Configuration File Management, Schema Update, Inventory Management Software Image Management, Status Monitoring and Security Monitor.
  - SRX5600 and SRX5800 gateways with modular Dense Port Concentrator (DPC) running JUNOS 9.5. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Configuration File Management, Inventory Management, Logging, Software Image Management, Status Monitoring and Schema Update.
  - SA2000, SA2500, SA4000, SA4500, SA6000, and SA6500 SA Series SSL VPN Appliances running SA releases 6.4 and 6.5. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Schema Update, Inventory Management and Status Monitoring.
  - IC4000, IC4500, IC6000, and IC6500 Unified Access Control Appliances running IC release 3.1. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Schema Update, Inventory Management and Status Monitoring.

- MX240, MX480, MX960 routers with MS-DPC PIC running JUNOS 9.4 and JUNOS 9.5 with forward support for JUNOS 9.6. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Inventory Management, Software Image Management and Schema Update.
- J2320, J2350, J4350, J6350 running JUNOS 9.4 and 9.5; and J2320, J2350, J4350, and J6350 routers with IDP running JUNOS 9.5. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Configuration File Management, Schema Update, Inventory Management, Software Image Management, Status Monitoring.
- EX3200, EX4200, EX8200 running JUNOS 9.4 and 9.5 with forward support for JUNOS 9.6. The following Element Management feature set is supported: Connectivity and Bootstrap, Configuration Management, Configuration File Management, Schema Update, Inventory Management, Software Image Management, Status Monitoring.
- **Support for IDP 5.0 devices.**
- **Extension of existing support to the ScreenOS 6.3 release.**
- **Extension of existing support to the JUNOS 9.4 and 9.5 releases.**
- **Provision of DMI schema support for the JUNOS 9.6 release.**
- **Full configuration support for IPv6:** You can create IPv6 objects in the Object Manager with the same functionalities as IPv4 addresses, assign IPv6 address objects in the Policy Manager and view logs related to IPv6 addresses. NSM 2009.1 also supports custom attacks with header matching for IPv6 and ICMPv6 on devices running ScreenOS 6.3.
- **Multiple system log and SNMP server configurations:** You can now specify multiple system log and SNMP servers in the Action Parameters dialog box for forwarding logs from a device. You can list particular SNMP and system log servers for various log action criteria.
- **Policy ID support in the Log Viewer:** In NSM 2009.1, the Policy ID column in the Log Viewer helps you keep track of logs over a period of time. This feature addresses the issues caused by changing policy rule numbers. Policy ID is supported for new logs generated from firewall devices running ScreenOS or JUNOS Software. In older logs, the Policy ID column remains unpopulated.
- **Support for IDP services:** The following NSM features are supported on MX240, MX480, MX960 routers running JUNOS 9.4 or 9.5: Import and update of device configuration, Detector engine update (scheduled and on-demand), Attack database update, NSM attack database update from Juniper Networks security website, Policy Management - IDP rulebases creation and update.

- **NSM trial license:** You can generate trial licenses for 30, 60, or 90 days. NSM notifies you when the trial period expires and prompts you to install a new license from the NSM GUI.
- **Export all audit log data:** With enhancements to the audit log exporter tool, you can invoke detailed help and create multiple filters for exporting audit log data. You can view detailed audit logs about modifications made to objects and compare audit log details before and after the modifications were executed.
- **NSMXpress enhancements:** NSMXpress now provides multi-user access with role-based access control to the WebUI. The NSMXpress WebUI now also supports authentication of users defined in the RADIUS servers in addition to local authentication.

The URL to access the NSMXpress appliance from a web browser is `https://<NSMXpress IP address>/administration` and not `https://<NSMXpress IP address>/admin`.

- **Application enhancements:** NSM 2009.1 provides the following enhancements:
  - **Template enhancement:** Device templates can now display the default values for scalar fields from the schema files. You can revert the configuration of a sub-tree to template or default values, retain template values if a template is removed from the device, and export device and device template configuration for all DMI devices to an XML file. Device templates are compatible with standalone, cluster and cluster member devices and inherit information according to the device type.
  - **Add SA and IC devices using reachable workflow:** You can use the NSM Add Device wizard to add SA or IC devices using the reachable device workflow.
  - **Custom expressions for SA and IC devices:** You can create a custom expression, save the custom expression to a catalog, validate the custom expression, and reuse custom expressions in the configuration. You can also reuse existing customer expressions while creating a custom expression.
  - **Software image management for SA and IC devices:** You can upload and delete software images to NSM Software Manager, install a selected image on one or more devices, rollback a software version on a device to the previously installed version, and reboot one or more devices. You can also back up and restore one or more devices.
  - **User Session management for SA and IC devices:** You can query and view user sessions, update the view of active user sessions, refresh the roles of all active user sessions, and delete active user sessions or all user sessions on a selected IC or SA device. You can also enable or disable all users on IC and SA devices.

- **Central Policy Management of BSG policies for M Series and MX Series routers:** You can create and manage Border Signaling Gateway (BSG) transaction policies using the NSM Policy Manager. You can also use shared objects such as BSG Service Points and BSG Admission Controllers in creating these voice policies.
- **Enhanced usability features:**
  - **Enhanced Topology Manager:** In the topology map view, NSM indicates with colored icons whether or not a device is managed. In the topology tabular view, the Device Status column under the Devices and Free Ports tabs indicates the managed status of a Juniper Networks device. Similarly, the Connection status and Alarm status of a device are indicated in the tabular view using the same coloring scheme of the Device Manager. You can launch a port template wizard by right-clicking on the Free Ports tab in the tabular view. You can discover link aggregation group (LAG) interfaces and view them as consolidated links in the topology map view, and view related port information in the tabular view.
  - **Improved policy versioning:** The improved policy versioning feature enables you to compare different versions of the same object that could be created through workflows such as the Update, Import, or Save operations in a device.
  - **Enhanced policy export tool:** With the enhanced policy export tool, you can generate policy reports that include details of shared objects in the policy rules. You can also export policies as a background process.
  - **Enhanced configuration templates for EX Series switches:** The enhanced configuration features for device templates on EX Series switches include template categories that facilitate the creation of templates. Full and partial Config Tree Views allow you to choose either complete or partial views of configuration nodes.
  - **Port template enhancements for EX Series switches:** The enhanced port templates allow you to view configurations, customize the CoS parameters of both predefined and customized port templates, and save the customization as a new template. While you can edit a customized port template, you cannot edit a predefined template. You can delete a customized port template if it does not have associated ports.
  - **Search and Filter enhancements:** You can now use the search feature to search for an exact match of any string. You also have a global search option, which you can use to search across different views.
  - **DB version displayed in Device Manager view:** The Attack DB version installed on firewall and IDP devices is shown in the Attack Db Version column in the Device Manager Table View, and in the tool tip for the device in the Device Tree view.
  - **Individual columns for optional fields in Policy Manager:** In the Policy Manager extended view mode, every custom policy field is displayed as a separate column nested under a header named Custom Field. In the compact mode, the custom field values are listed in a single Optional Field column. You can also edit and filter the values in each column.

- **New Shared Objects:** NSM 2009.1 introduces the following shared objects that you can configure from the Object Manager.
  - **Applications:** A new shared object called Applications enables you to view predefined applications as well as add, edit, and delete custom applications by using protocol, port and signature patterns. You can create a policy with APE rules, add custom applications to an APE rule, and push APE policy with custom applications to a device.
  - **QoS profiles:** You can define an IP precedence profile (IP) and a DSCP profile (DP) in the Object Manager, to determine the quality of service for an incoming packet in the network. After creating these objects, you can match them with specific policies. However, Quality of Service (QoS) profiles cannot co-exist with traffic shaping in the same policy. This feature is supported on the SSG Series Secure Service Gateways running ScreenOS 6.3.
  - **SCTP objects:** You can create shared Stream Control Transmission Protocol (SCTP) objects. You can use the SCTP protocol filtering tool to configure protocols such as IUA, SUA, M2UA, M3UA, H.248, DIAMETER and so on, to run on these SCTP objects.
  - **BSG service point objects:** The Border Signaling Gateway (BSG) service point object is a shared polymorphic object with which you can specify the egress service point in a transaction policy's route action. You can specify the device, the gateway in the device, and a service point for every BSG service point object.
  - **BSG admission controllers:** You can set the maximum concurrent number, committed attempts rate, and committed burst size for both dialogs and transactions on BSG Admission Controllers. You can define an admission controller per gateway, and reference the controllers from the BSG transaction rulebase in the Policy Manager on devices running JUNOS 9.5 and later.

For more information, see the *Network and Security Manager Administration Guide* or the *Network and Security Manager Online Help* available through the NSM UI.

### 3 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*.

### 4 Upgrade Considerations

---

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

## Upgrading NSM

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

2009.1r1a supports only 3500 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.

## 5 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.

## 6 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 25600000 1** to **0 102400000 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 **Xmx1024000000** to **Xmx2048000000**

```

$LIB_DIR/jre/bin/java -DNSROOT=$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 -
Xmx2048000000 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-setti
ngs/syslog</nsm:path>
```

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

## 7 Best Practices

---

This section contains information about recommended practices when using NSM.

### 7.1 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>.

### 7.2 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](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.

## 8 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.

- 284305—The NSM license key enforcement system for NSM 2007.3r1 is not secure.
- 394318—The summarize delta configuration operation may sometimes return differences in hostchecker / patch-assessment/bullets in the configuration even when there is no change on the device.
- 406061—When a template configured with the enforce manager IP is applied on a vsys device, the device takes the template value for the enforce IP and update fails.
- 414483—After a device import, if the device policy is not in sync with the NSM policy, a new day's log directory is not created. Instead the logs are appended to the same day's log directory.
- 417134—The NSM GUI does not have VLAN retag management.
- 427132—Using an NSM pre-defined traceroute service causes a device update failure.
- 427317—Changes in domain versions are not visible unless an initial domain version is saved.
- 433159—You cannot connect to NSM from a remote location over a virtual private network.
- 438056—The NSM devSvrManager discards logs that have a timestamp that is earlier than the last timestamp on the writer thread.
- 438698—The XDB directive handler container does not reclaim unused disk space when data or database versions are deleted.
- 444483—NSM does not push all details related to the scheduler object on to devices running JUNOS Software.
- 444503—NSM does not import a scheduler object completely from a device running JUNOS Software.
- 444957—The detector and signature updates in guiSvrcli.sh are not separate.
- 445965—NSM does not push the proper commands to SRX Series devices to implement infranet authentication.
- 447787—Updating or performing a delta config operation on one device from NSM, affects all devices in the device group.
- 448231—You cannot assign a custom zone to an ADSL interface using NSM.

- 451113—Making adjustments to the access list disables RIP on redundant subinterfaces.
- 454581—Setting the default metric of RIP in a vrouter template unsets existing RIP protocol settings on the interface.
- 457679—You cannot add a redundant ethernet interface to a J Series or SRX Series cluster.
- 457797—The SNMP trap message has an extra field after Device Family and the MIB file is not updated.
- 459124—The Interface monitor tab is missing on a firewall cluster member.
- 458030—NSM displays a blank device list when an administrator logs in while another administrator is performing a delta operation.
- 459874—The Job Manager does not provide updated status information when an IDP appliance is updated with an APE rulebase.
- 465613—The GuiSvrManager crashes if the IP address of the client system contains 15 characters.
- 466011—Migration takes longer in an environment that has device action criteria defined.
- 466060, 475939—During a device update on NSM, the default-route for IPv6 (::/0) displays a verification failed message even though the CLI is updated to the device. However, you can see the route if you import the configuration.
- 469779—If you upgrade from NSM 2008.2rX to NSM 2009.1r1, all IDP appliances added before the upgrade do not reconnect.
- 473016—NSM stops forwarding system logs. After several days, the newLogWalker reports "errno=12 Cannot allocate memory."
- 473978—You cannot see AVT data in the profilerDb in NSM.
- 474065—The **Download Backups** option under **NSM Database Backup** does not work in the NSMXpress appliance.
- 475784—Junos 9.6 shows denied logs as permitted/accepted in NSM.
- 480558—The NSM UI client freezes when you create and save multiple rule groups.
- 480583—NSM does not provide an option to set policy based routing on redundant interfaces.
- 483397—The device configuration on NSM is incorrectly changed after running template operations on the device.
- 485523—You cannot add an NSM license to NSM3000 appliances.

## 9 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.

### 9.1 NSM

- 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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 299014—During an upgrade installation, license information is required to complete the installation.
- 277604—Interface configuration screens show more settings than are supported by the actual interface.
- 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.
- 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.
- 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.
- 302289—The virtual management Ethernet interface must be set as the management interface on the Virtual Chassis for it to be managed through 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 394543—When you update the configurations of more than 30 devices together, the update device operation could take up to 10 minutes.

- 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**
- 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.
- 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
```
- 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.
- 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.
- 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.

- 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.
- 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/utils/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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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 statd: [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.
- 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.
- 477214—The reboot device operation does not work for devices added in a non-reachable work-flow.
- 477349—If you select the "none" radio button in the NSM GUI, the context is uninitialized 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.
- 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.
```
- 479859—NSM incorrectly allows you to create address objects called ANY-IPv4 and ANY-IPv6.
- 480054—You cannot set Certificate Authority revocation to "none" from NSM.
- 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.
- 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.

## 9.2 EX Series Switches

- 271590—Deleting the "system services outbound-ssh" stanza does not cause existing connections to be dropped.
- 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.
- 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.
- 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.

### 9.3 **Devices Running ScreenOS**

- 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.
- 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.
- 431638—Enabling IPv6 support in an NS500 device causes the firewall policy update to fail.
- 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.
- 436587—In NSM 2008.1, the value of the NHRP field in the vrouter schema was "true" thereby enabling NHRP on all vrouters by default. In NSM 2008.2R2, the NHRP default value was "false". Migrating from either NSM 2008.1R2 or NSM 2008.2R1 to NSM 2008.2R2 ensures that wrongly enabled vrouters are reset.
- 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.
- 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.
- 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.

#### **9.4 Secure Access SSL VPN SA Series and United Access Control Infranet Controller**

- 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.

## 9.5 **SRX Series Services Gateways**

- 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.
- 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.
- 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.
- 477575—NSM does not generate encryption commands to SRX Series gateways when AES is chosen as algorithm.
- 480097—You cannot add an SRX Series cluster member in the auto-import configuration list.
- 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.

## 10 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.

### 10.1 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/>.

## **10.2 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](mailto: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 © 2009; 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.