



Network and Security Manager Release Notes

***Release 2008.1r2
19 March 2010***

Contents

- 1** Version Summary on page 2
- 2** New Features on page 2
- 3** Before You Install on page 5
- 4** Upgrade Considerations on page 8
- 5** Limitations on page 9
- 6** Important SSL VPN and Infranet Controller Instructions on page 9
- 7** Fixed Issues on page 14
- 8** Known Issues on page 16
- 9** Requesting Technical Support on page 22

**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 future versions of ScreenOS and with the latest version of NSM, for JUNOS. 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 2008.1 release of NSM:

- **Supported device families:** In addition to Juniper Networks firewall/VPN and IDP devices, you can manage the following device families through NSM:
 - Devices running JUNOS software with enhanced services for J-series routers and clusters. Supported devices include Juniper Networks J2320, J2350, J4350, and J6350 routers running JUNOS software with enhanced services 9.0, 9.1, and 9.2 (9.2 is supported for J-Series).
 - EX-series switches, including virtual chassis configurations. Supported devices include Juniper Networks EX3200-24P, EX 3200-24T, EX 3200-48P, EX 3200-48T, EX 4200-24F, EX 4200-24P, EX 4200-24T, EX 4200-48P, and EX 4200-48T switches running JUNOS 9.1 and 9.2 (9.2 is supported for EX-Series).
 - Secure Access SSL VPN series devices (SA) and clusters. Supported devices include Juniper Networks Secure Access 2000, 2500, 4000, 4000 (FIPS), 4500, 6000, 6000 (FIPS), and 6500 devices running SSL release 6.3.
 - Unified Access Control (UAC) Infranet Controller devices (IC) and clusters. Supported devices include Juniper Networks Infranet Controller 4000, 4500, 6000, and 6500 devices running Infranet Controller Release 2.2.
- **Element management for supported devices.** NSM provides the following features to manage elements across your network:

- **Device connectivity:** You can add all supported devices from the NSM user interface (UI). Connectivity can be achieved through reachable or nonreachable workflows. Reachable workflows establish connectivity with devices that have static IP addresses. Nonreachable workflows establish connectivity with devices that have dynamic IP addresses. ScreenOS devices, IDP devices, and EX-series switches and virtual chassis can be configured with static IP addresses and added through the reachable workflows. All supported device families can be configured with dynamic IP addresses and added through nonreachable workflows. For more information, see the *Network and Security Manager Administration Guide* or the *Network and Security Manager Online Help* available through the NSM UI.
- **Configuration management:** All configuration options are available from the NSM UI. For example, the **Edit Device** option displays detailed device information relevant to each device type. In addition, support for common directives such as Import, Update, and Delta is provided.
- **Configuration file management:** You can get configuration information for one or more devices on demand or on schedule, create a schedule to retrieve and archive configuration information periodically, display and view saved configuration files, compare two versions of a device's configuration file, and select a version and push a selected configuration version to a device. This feature is supported only for JUNOS-based devices.
- **Schema update:** Download the latest device schema set from the Juniper Update Server (Central Schema Repository) without upgrading NSM. New versions of the device schema can be downloaded manually or on schedule. This feature is not supported on IDP devices or ScreenOS-based devices.
- **Inventory management:** You can display inventory capability and support for on-demand retrieval (import) of inventory data, such as modeling of hardware inventory for adding and configuring interfaces, software modeling at the time you add the device, and modeling of the license inventory that is not supported. In addition, you can use Device Monitor and Tool Tips to view the status of inventory synchronization.
- **Software monitor:** Manage and change software images for all supported devices from a central location. This feature is not available for SSL VPN, Infranet Controller, and J-series devices.
- **Status monitoring:** Quickly ascertain which devices have the most severe alarms. The NSM UI uses color codes to display alarm severity. Status monitoring also provides device connection and configuration status.

- **Device discovery:** You can use sets of rules to find, add, and import multiple EX-series devices into NSM. You can configure and run rules to search a network for devices in a specified subnet or within a specified range of IP addresses. EX-series devices must be configured with static IP addresses to be found by device discovery rules.
- **Application management.** Manage supported devices through NSM using the following features:
 - **Policy management:** You can manage the policies for all supported devices through the NSM UI or create policies centrally using the NSM UI and share them across multiple devices.
 - **Central management:** Policies are shareable with Policy Manager across ScreenOS-based firewall devices, standalone IDP devices, and J-series routers. Objects created for policy rules are shared between central policy methods. This feature is supported for IDP, ScreenOS, and J-series platforms.
 - **In-device management:** The NSM Device Editor provides a hierarchical file structure where you can configure and manage the device policies from a central location. Templates provide the method to share policies across multiple devices.
 - **VPN management:** Centrally manage VPNs for both ScreenOS devices and J-series routers. With VPN management, the differences between VPN implementations are handled automatically.
 - **Cluster management:** Support for active/passive pairs for high availability, or active/active configurations for ScreenOS, J-series, SSL VPN SA, and Infranet Controller devices for scaling.
 - **Templates:** Device template support for all supported device families. New base templates for each device family allow rapid configuration of similar data across multiple devices in the same family.
 - **Configuration group:** Support for J-series and EX-series platforms. NSM supports this JUNOS feature allowing replication of configuration data at multiple levels within a J-series or EX-series device configuration.
 - **Role-based administration:** You can set permissions for new activities, including managing database snapshots that are used to identify the policy version, importing device inventories, and downloading and applying new device schema from the Juniper Update Server.
 - **Log manager:** Support for predefined and customized log filter views for user and administration logs, event logs, sensor logs, and VLAN ID assignments for all users.

- **Report manager:** Support for predefined and custom reports for each device family. You can view the most active users based on bytes in/out and monitor the authentication failures per user realm.
- **Policy versioning with rollback:** Manage NSM device policies with automatic policy versioning. This feature allows the creation of policy versions automatically or as needed. You can find the difference between two versions of a policy and roll back to a previous version.
- **NSM API**—The NSM API provides programmatic access to NSM through a SOAP API and enables third-party developers to create applications that support a wide range of development tools. In this release, the NSM NBI provides the following features and functions:
 - Central policy management
 - NSM object management
 - Implement NSM Directives:
 - Import devices
 - Update devices
 - Summarize delta configuration
 - Get running configuration
 - Retrieve device list per domain
 - Retrieve high-level device status
 - Retrieve log packet data
- **Search for unused objects:** You can locate unused shared objects and delete them using the locate shared objects tool in the NSM UI.
- **Client support for Windows Vista:** You can install the NSM User Interface on client servers running Windows Vista.
- **User interface improvements:** Workflows for common tasks have been simplified and enhancements have been added. In addition, the navigation is divided into three major tasks- **Investigate**, **Configure**, and **Administer**, to improve navigation and increase the ease of use.

3 Before You Install

This section contains *important* information that you should consider before you install NSM.

Mandatory Steps for Preparing a Solaris 10 Server for NSM

Perform these steps if you plan to install NSM on a Solaris 10 server:

1. Install required locale files. Use the following command to check which locale files are currently installed:

```
/usr/bin/locale -a
```

Ensure that the following locales are installed. If you have all required locales, proceed to Step 2.

```
C
```

```
POSIX
```

```
en_CA
```

```
en_CA.ISO8859-1
```

```
en_CA.UTF-8
```

```
en_US
```

```
en_US.ISO8859-1
```

```
en_US.ISO8859-15
```

```
en_US.ISO8859-15@euro
```

```
en_US.UTF-8
```

```
es
```

```
es.UTF-8
```

```
es_MX
```

```
es_MX.ISO8859-1
```

```
es_MX.UTF-8
```

```
fr
```

```
fr.UTF-8
```

```
fr_CA
```

```
fr_CA.ISO8859-1
```

```
fr_CA.UTF-8
```

Use the Solaris 10 installation DVD to load any missing locales. The minimum supported Solaris 10 revision is 6/06. You can download the DVD from www.sun.com. Mount the DVD (in this example, /solaris) and issue the following commands:

- `/usr/sbin/pkgadd -d /solaris/Solaris_10/Product SUNWladm`
- `/usr/sbin/localeadm -a en_US -d /solaris/Solaris_10/Product`

2. Edit the `/etc/default/init` file to include the following lines:

- LC_COLLATE = en_US.UTF-8
- LC_CTYPE = en_US.UTF-8
- LC_MESSAGES = C
- LC_MONETARY = en_US.UTF-8
- LC_NUMERIC = en_US.UTF-8
- LC_TIME = en_US.UTF-8

3. Reboot the Solaris server.

```
/usr/sbin/reboot
```

For more information, see the 2008.1 *NSM Installation Guide*.

Installation Space Allocation

During the installation of NSM, the installer checks the default installation location to ensure that you have enough disk space allocated in order to install NSM. If you do not have enough disk space allocated, an error message is displayed warning that if you proceed with the installation, it will fail.

To avoid installation failures, you must have the following free space available prior to installing NSM:

- 5.3GB in the default NSM installation directory (/usr) or custom location
- 1.5GB in the NSM staging area (default /tmp, or specified by -niSTAGINGDIR)

Note that the installer does not check custom installation locations for disk space requirements and therefore, you will not receive an error message. Even so, you must follow the space recommendations in this section to avoid installation failures.

Job History and Audit log Migration

The migration of the job history and audit log data from previous NSM releases is not supported in this release of NSM. Before you perform the installation, follow these steps:

1. Make a backup of your existing data (by default /var/netscreen/GuiSvr and /var/netscreen/DevSvr).

2. On the NSM server command line, type

```
$> cd /usr/netscreen/GuiSvr/var/xdb/data
```

3. On the NSM server command line, type

```
$> rm -f directive auditlogDetails
```

4 Upgrade Considerations

This section contains information about upgrading NSM and deprecated operating systems. Be sure to check Known Issues on page 16 for additional upgrade information.

Upgrading NSM

Consider the following when you upgrade to a new version of NSM:

- If you are upgrading to NSM 2008.1 from 2006.1rX or earlier or from 2007.1rX or earlier, you must install NSM 2007.2r2 first before you upgrade to NSM 2008.1.
- The Device Schema files loaded in NSM 2008.1r1 are not automatically upgraded when you upgrade the NSM release from 2008.1r1 to 2008.1r2. Before you upgrade NSM, you are required to run Juniper Update under the Server Manager. Warning: If you fail to run Juniper Update under the Server Manager before you upgrade NSM it will result in Juniper Update being disabled for future updates and you must perform the following steps to enable Juniper Update.

1. Stop the NSM server.
2. In a root shell, issue the following commands on the NSM GUI server. The User ID and password are the JTAC provided credentials that you used download the software:

```
cd /usr/netscreen/GuiSvr/var/dmi-schema-stage/nsm
/usr/netscreen/GuiSvr/Utils/subversion-1.4.4/bin/svn
update --username <user> --password <pass>
```

3. Start the NSM server.
4. Launch the NSM GUI client.
5. Log in and go to **Tools -> Preferences -> Juniper Update Settings** tab and enter the JTAC provided credentials.
6. Navigate to the **Administer -> Server Manager -> Schema Information** node to access Juniper update.
 - a. Click **Download Schema**
 - b. Click **Next** on the Source Selection screen
 - c. Click **Finish** on the Schema Update From Server screen
 - d. Click **Ok** when the job is 100% complete
 - e. Click **Apply Schema** on the Schema Information screen
 - f. Click **Yes** on the warning dialog
 - g. Click **Ok** when the job is 100% complete

7. Restart NSM. Usually this is automatically performed by default but you may have chosen to disable the restart during the installation.

Deprecated Operating System

- NSM no longer supports ScreenOS version 4.x. You must upgrade your devices to ScreenOS version 5.0 or later before upgrading to 2008.1.
- NSM 2008.1 no longer supports Solaris 8, Solaris 9 and Red Hat ES/AS 3.0. The operating system on the servers must be upgraded either to Solaris 10, Red Hat ES/AS 4.0 or Red Hat ES/AS 5.0 before upgrading to NSM 2008.1.

5 Limitations

The following items are known limitations:

- For JUNOS software with enhanced services for J-series, and EX-series switches running JUNOS only: 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 back to NSM.
- For NSM: NSM will only use the configuration schema that is made available through Juniper Update. Customers are advised to perform an update using Juniper Update to make sure the OS version running on the devices managed by NSM are supported.
- For SSL VPN SA and Infranet Controller:
 - Secure Virtual Workspace (SVW) settings on the SA device cannot be managed with NSM.
- For EX-series switches:
 - EX-series switches running JUNOS 9.0 or 9.1 software do not support snapshots (for example, request system snapshot). 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 scale limitation, tuning parameters, setup instructions, and template usage guidelines for SSL VPN SA (SA) or Infranet Controller (IC) devices.

NSM Scale Limitations and Tuning Parameters for SSL VPN and Infranet Controller

This section describes the NSM scale limitations and tuning parameters that customers need to consider and implement if they manage SSL VPN SA or Infranet Controller devices.

NSM Server

The NSM software server system must have 4 CPUs and at least 8 GB of RAM. There can be no more than 4 devices included in a single job (for example, Update and Import).

The following files on the NSM software server must be edited:

- In `/usr/netscreen/GuiSvr/var/xdb/specs/jax.spec`, change **Xmx256m** to **Xmx512**.
- In `/usr/netscreen/GuiSvr/var/guiSvr.cfg` change `guiSvrDirectiveHandler.max.heap` from **102400000** to **204800000**.
- In `/usr/netscreen/DevSvr/var/devSvr.cfg` change `devSvrDirectiveHandler.max.heap` from **102400000** to **204800000**.
- 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`, change the shared memory of `kernel.shmmax` to **1GB**.

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

NSMXpress Server

For NSMXpress, there can be no more than 2 devices included in a single job. The following files on the NSMXpress server must be edited:

- 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`, change the shared memory of `kernel.shmmax` to **1GB**.

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 Steps 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 Steps 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 on 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 6e 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 Steps 7b through 7d for each Infranet Enforcer device.

When you are not using the Infranet Enforcer(s), it is important to reimport the configuration each time. 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 2008.1 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 only contains CG data and the cluster member object contains NS and NL data. Template promotion and application to clusters should be compliant with the cluster abstraction. The following describes the basic guidelines for using templates for clusters.

Recommended

1. Templates that are applied to cluster objects should only include CG data. NS and NL data should be excluded from such templates. Templates that are applied to cluster member objects should only include NS/NL data. These caveats apply to templates that are created from scratch or via promotion.
2. To replicate the configuration from one cluster (source) to another cluster (target) via templates, the recommended workflow is to promote the configuration from the source cluster object to a **cluster** template, and then apply the template to the target cluster object.
3. To replicate the configuration from one cluster member (source) to another cluster member (target), the recommended workflow is to promote the configuration from the source cluster member object to a 'member' template, and then apply the template to the target cluster member object.

Not Recommended

1. Do not apply any template, that contains NS/NL data (for example, promoted from cluster member or standalone device) to a cluster object. The usage of that template will result in unexpected UI behavior (NS/NL data in cluster object is not editable and invisible) and update result (NS/NL data from the template in cluster could be ignored).
2. 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 which of the configuration settings are NS, NL and CG.

Node-Specific Configuration (NS):

The following list contains the set of node-specific settings that occur in both SA and IC configuration schemas.

- configuration/system/log/snmp
- configuration/system/log/events-log-settings/syslog
- configuration/system/log/user-access-log-settings/syslog

- configuration/system/log/admin-access-log-settings/syslog
- configuration/system/log/sensors-log-settings/syslog
- configuration/system/network/network-overview/settings
- configuration/system/network/internal-port
- configuration/system/network/external-port
- configuration/system/network/management-port
- configuration/system/network/vlans
- configuration/system/network/network-hosts
- configuration/system/configuration/licensing
- configuration/system/clustering/properties/configuration-settings/network-settings

Node-Specific (NS)

The following additional settings in the SA configuration schema are node-specific. These settings do not exist in the IC configuration schema.

- configuration/system/network/network-connect/network-ip-filter
- configuration/users/resource-policies/network-connect-policies/network-connect-node-specific-configuration
- configuration/authentication/auth-servers/collection-of-auth-server/union-of-ace/active-directory-winnt/settings/advanced/computer-names/ive-name

Node-Local (NL)

The following settings in the SA and IC configuration schemas are node-local.

- configuration/system/configuration/dmi-agent/enabled
- configuration/system/configuration/dmi-agent/device-id
- configuration/system/configuration/dmi-agent/hmac-key
- configuration/system/maintenance/push-config/accept-push

The remaining settings in the SA and IC configuration schemas are cluster-global (CG).

7 Fixed Issues

The section includes the addressed issues for NSM, ScreenOS, Secure access SSL VPN SA series, and Unified Access Control (UAC) Infranet Controllers. 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.

7.1 NSM

- 399270—When you create a VPN using NSM VPN Manager with extranet devices, it results in unsetting of NHTB entries for extranet devices.
- 227732—An error occurs when an NSM schedule object interval is set to start before 12 AM or PM and then end before 12 AM or PM on a Screen OS device since Screen OS is unable to read a 24 hour time period.
- 256891—While performing a policy device update or push to an IDP 4.1 device using the guiSvrcli.sh script, the attack platform version detail shown in the job manager is displayed incorrectly.
- 266488—The custom URL category cannot be managed within the custom virtual system (VSYs).
- 289933—There's a forward compatibility problem when a Secure Access SSL VPN SA device is upgraded to a future release in which the SA configuration schema is virtualized using DMI 1.2.
- 290656—The firmware is not listed in the firmware manager when you change the operating system on the device.
- 301848—You cannot assign a null zone to an interface in the NSM template.
- 305742—After applying a template and then deleting the template configuration on a device object, the result is an inconsistency in the NSM UI.
- 306672—The NSM installation script fails to check memory and prevent installation or migration if less than 2 GB of system memory is installed.
- 307266—The NSM installation script fails to verify if UTF locales are installed and therefore fails to stop the installation if these locales are missing.
- 307611—After you create two VIPs, one on self-IP and another on a new IP on the firewall, only one IP is displayed in the NSM UI after being imported.
- 308204—The expanded mode view doesn't show the configured DSCP marking value on a policy and the traffic shaping icon is not displayed in the NSM UI.
- 308481—When a device is configured with 2 default routes with each pointing to a different gateway and is subsequently imported into NSM, then the NSM delta configuration appears to be unsetting the default route.
- 308548—When a VPN tunnel interface is created using the VPN manager and is changed from unnumbered to a numbered interface, NSM sends the commands to unset the tunnel interface IP and then sends the commands to set the tunnel interface IP but misses the basic command of setting the tunnel interface and zone.

- 308801—The template operation does not remove all conflicting values in the device.
- 309635—NSM is not adding the device MIPs to the Global NAT MIP objects when the device is imported.
- 312383—Deletion of an entry from the NSM template leaves a stub entry in a device object.
- 312399—A modification in a template causes the configuration that is imported from a template to be lost in next update.
- 314398—Template settings are not being applied to a ScreenOS devices.
- 395607—When a HA fail-over occurs, the NSM UI is not able to connect to the running secondary server through the primary UI IP address.

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

- 400925—Upgrade from 2008.1r1 to 2008.1r2 may result in an empty attack update URL for JUNOS devices if the URL was not populated in 2008.1r1 release.
- 401535—An IDP policy rule with “All Attacks” *cannot* be updated to an IDP cluster.
- 396472—When you upgrade from NSM 2008.1 to NSM 2008.1r2 the schema on the device is not updated. To make sure the device schema is updated:
 1. Before you upgrade to NSM 2008.1r2, run Juniper Update on NSM 8.1.
 2. Upgrade to NSM 2008.1r2.
- 398611—When the peer VPN device is configured in NSM as FQDN and then re-imported, the device may unset the FQDN from the IKE gateway configuration.
- 398603—NSM unsets the VPN when you change the Interface IP address of a newly created device.
- 399496—Unsetting NSRP vsd group 0 breaks the connection between NSM and the device in question.
- 293392—When you change the address object on a policy, NSM erroneously un-seats and then sets the policy.
- 310341—The domain version comments are not saved in the current version but are saved for in a previous domain version.

- 298146—The NSM audit logs indicate changes that are not actually performed.
- 311632—An error occurs when you set the system log filters on Secure Access SSL VPN SA and United Access Control (UAC) Infranet Controller device templates.
- 266981—The device sub-interfaces are not correctly imported into NSM for a cluster if the VSD is not defined.
- 250830—When using an SSG-500 device and an SSG-500M Series device in an NSRP environment, both devices must be running ScreenOS 5.4r2 or later. Both devices must be one of the following clusters: SSG 520 and SSG 520M NSRP cluster or SSG 550 and SSG 550M NSRP cluster.
- 283064—The DSCP value does not get exported when the policy is exported into an HTML format.
- 306735—After installation, NSM has open ports and processes that are listening to 11122 NACN and 15400 NSP. The work-around is to stop the processes that are listening to these ports since NSM does not support Screen O/S 4.x.
- 314260—The NSM NBI SOAP interface does not work when the schema is installed. After installing the schema update, the NBI and the server report a different version leading to a potential validation error of a valid condition.
- 306197—When installing (fresh or upgrade) the NSM management servers into a location other than the default (/usr/netscreen), the required available disk space in the custom location is not checked, possibly causing the installation to fail if insufficient space is available. To avoid this, confirm that at least 5.3GB free space is available in the custom location prior to starting the installation.
- 306199—The installation (fresh or upgrade) may halt due to insufficient space in /usr. A warning message is generated at such an event. This behavior is needed to ensure that sufficient disk space is available for the install process. To avoid this, confirm that /usr has at least 5.3GB and the staging area (default /tmp, or specified by -niSTAGINGDIR) has at least 1.5GB free space prior to starting the installation.
- 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.

- 299775—Currently, only the NSM GUI enforces uniqueness of object names. The NSM Server does not enforce uniqueness of object names. Consequently, an NBI client could potentially create multiple objects with the same object name on the NSM server. To avoid duplicate object names, developers of NBI client applications must ensure that NBI client application code enforces uniqueness for object names. Object names can be address objects, NAT objects, services, schedules, DI profiles, AV profiles, user objects, authentication servers, group expressions, certificates, and policy objects.
- 283258, 289220—NSM does not display the correct IP address of NBI client applications that are running on a different computer from NSM. For example, if a system administrator attempts to view the IP address of an NBI client connected to NSM from the Logged In Administrators feature or from the Miscellaneous column in Audit Log Viewer, the IP address displayed for the NBI client shows 127.0.0.1, which is the address of the Web server that NSM uses. As a workaround, you can access NBI client IP addresses from the log file, `web_access.*.log`, which is located in the `$/NSROOT/GuiSvr/var/errorLog` directory.
- 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.
- 295314—After the initial import of a device, the database version feature shows the user who performed the import as *unknown*.
- 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.
- 274821—During the initial creation of a device template, you must save the template and edit it again to ensure that the changes are saved.
- 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.
- 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.
- 290847—When a comma-separated value (.csv) formatted file is used for rapid deployment, static IP addresses are not imported to NSM for the device. If you create a configlet that models many devices (for example, using the workflow "Modeling and Activating Many Devices using csv files"), the system allows you to specify the device IP, device root user, and password in the.csv file. However, after modeling, the device IP does not appear in the NSM GUI.
- 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.

- 292523—In NSM, you may not be able to delete a virtual system (vsys) from within a subdomain. If you have a problem deleting the virtual system, delete it from the domain level.

- 294623—In NSM, you can accidentally create a firewall policy with a Policy ID (ID) 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 ID in the policy list. This can lead to inconsistencies such as a mismatch between policies and IDs.
- 304550—After migration from previous releases, the administrator needs to uncheck the 'Enable attack downloads for JUNOS Devices' option in the Tools, Preferences, Attack Object.

8.2 *Devices Running JUNOS Software with Enhanced Services for J-series Devices*

- 288309—For J-series devices 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**. You must adjust the OS version to ensure that the OS version running on the device and the one recorded in the NSM database are the same.

8.3 *EX-series Switches*

- 293292—Device connectivity ends in NSM when JUNOS is downgraded from 9.1 to 9.0.
- 271590—JUNOS-based devices remain connected to NSM even after the outbound-ssh session is deleted and committed using the CLI on the device. The CLI command **restart service-deployment** will drop the connections. The connection will also be dropped after the device is rebooted.

8.4 *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 in order for it to complete. The update will fail if insufficient RAM is available.
- 300818—Update of vsys devices from NSM that has a name greater than 11 characters fails. To prevent the failure, create vsys device names with less than 11 characters.

- 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.

8.5 Secure Access SSL VPN SA series and United Access Control (UAC) Infranet Controllers

- 394318—Even though the device's configuration status in NSM is shown as **Managed, insync**, the summarize delta configuration operation returns a difference in the <summary> fields within the HostChecker Patch Assessment bulletin configuration. The reason for this discrepancy is in the backend device configuration. The <summary> fields contain a pair of strings framed by double quotes with a space between them, such as: "Persistent Mail Browser Link," "Cache Bypass," whereas on NSM, the space between the two double-quoted strings is incorrectly stripped off. This difference is displayed in the delta config. However, this is harmless since this configuration is immutable on the device, and so does not get altered when pushed down from NSM as part of the configuration update operation.
- 305746—When a template is deleted from a device object, validation errors are displayed when navigating to elements within the device object which previously referred to configuration inherited from the template.
- 284840—The adding of modeled Secure Access SSL VPN SA series and United Access Control (UAC) Infranet Controller devices is not supported, but the add device wizard still shows Secure Access SSL VPN SA series and United Access Control (UAC) Infranet Controller devices as possible choices.
- 59214—In NSM, while an active-passive cluster is updated, the wrong node name is displayed in the message when an automatic reimport of configuration is initiated.
- 58637—When NSM imports a file containing base64-encoded binary data from the device, it does not display the name of the file in the GUI. The NSM user needs to explicitly enter the file name via the GUI.
- 56845—If new node members are enabled in the SSL VPN SA administrator UI (Web UI), but not added to NSM through the Add Cluster Member workflow, a cluster-level update from NSM fails with an error message, "Update fails Update Device Results GenerateEditConfig Failed". To avoid this issue, cluster updates from NSM should not be performed unless the NSM cluster and the device-side cluster have an identical set of members, and the DMI connection between each cluster node and NSM is up.

- 56508—Creating or deleting SVW policies, third-party policies, Connection Control policies, and Advanced Endpoint Defense policies through NSM is not supported. However, they can be imported from the IVE into NSM and modified using NSM.
- 58572—When an SSL VPN SA/ Infranet Controller cluster comes up after a reboot, wait about 5 minutes before attempting configuration imports or updates to the cluster.
- 56509—When a cluster node is deleted from the device side, the corresponding cluster member object must be deleted from NSM. Otherwise, an unexpected error occurs.
- 56298—In the NSM UI, under System->Configuration->DMI Agent screen, do not change the state of the DMI agent setting from Enabled to Disabled. If you change this setting, the DMI connection between NSM and the device will fail.
- 56705—As part of SSL VPN SA configuration promotion to templates, device-hardware specific configuration such as licenses get promoted as well. When this template is associated with a different SA device and the target device is updated, the configuration update will result in an error since the licenses in the template cannot be applied to the target device.
- 56980—On an SSL VPN SA or Infranet Controller device cluster, you cannot have the same administrator simultaneously logged into two cluster nodes through the Web UI. When an administrator who is logged into one cluster node attempts to log into another cluster node, an “access denied” message is displayed on the second node. This behavior is working as designed.

When an SSL VPN SA or Infranet Controller cluster node is first added to NSM through the “Add Cluster Member” workflow, you must use a unique admin user name for the member. Do not use an admin user name that has already been used for the Add Cluster Member workflow for any other node in the same cluster.

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 postsales 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. 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 Manager: <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/>.

Opening a Case with JTAC

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

- Use the Case Manager 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).

For international or direct-dial options in countries without toll-free numbers, visit us at

<http://www.juniper.net/support/requesting-support.html>. If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the gzip utility, rename the file to include your company name, and copy it to [ftp.juniper.net:pub/incoming](ftp://ftp.juniper.net:pub/incoming). Then send the filename, along with software version information (the output of the show version command) and the configuration, to support@juniper.net. For documentation issues, fill out the bug report form located at <http://www.juniper.net/techpubs/docbug/docbugreport.html>.

Documentation Feedback

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

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

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks 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