



Network and Security Manager Release Notes

***Release 2008.2
15 January 2010***

Contents

- 1** Version Summary on page 2
- 2** New Features on page 2
- 3** Before You Install on page 7
- 4** Upgrade Considerations on page 7
- 5** Limitations on page 8
- 6** Important SSL VPN and Infranet Controller Instructions on page 8
- 7** Fixed Issues on page 13
- 8** Known Issues on page 15
- 9** Requesting Technical Support on page 25

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

1 Version Summary

Juniper Networks Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. With Network and Security Manager, Juniper Networks delivers integrated, policy-based security and network management for all security devices and other Juniper Networks devices in your networks. Network and Security Manager uses the technology developed for Juniper Networks ScreenOS to enable and simplify management support for previous and current versions of ScreenOS and now for JUNOS. 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 2008.2 release of NSM:

- **New device platforms:** NSM provides element management and application support for the following new platforms:
 - SRX-series gateways. Supported devices include Juniper Networks SRX5600 and SRX5800 running JUNOS 9.2 or 9.3.
 - M-series and MX-series routers. Supported devices include Juniper Networks M7i, M10i, M40e, M120, M320, MX240, MX480, and MX960 routers running JUNOS 9.3.
- **Element management for supported devices:** NSM provides the following enhancements to DMI-based element management of JUNOS-based platforms: Connectivity and Bootstrap, Configuration management, Configuration file management, Schema update, Inventory management, Software image management, and Status Monitoring.
 - **Enhanced configuration file management:** When enabled, NSM by default automatically deletes the oldest versions of config files to accommodate newer versions of the config files that are being imported. You can set a system preference for the maximum number of config file versions to be preserved. The default is 25 versions. The Config File Manager can automatically import config files from managed JUNOS-based devices when configuration changes are committed on these devices, enabling NSM to have different versions of the device configuration. You can enable or disable the auto import of config files and track those devices on which the feature is enabled. You can also see status of the config file versions.

- **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 all supported JUNOS devices can be configured with static IP addresses and added through reachable workflows. All supported device families can be configured with dynamic IP addresses and added through the nonreachable workflows.
 - **Dynamic configuration synchronization notification for SSL/IC devices:** NSM is notified when configuration settings on SSL/IC devices are changed.
- NSM 2008.2 supports both the 6.1 and 6.2 ScreenOS releases.
- **Support for NS-IDP-8200 with IDP 4.2:** The Add Device wizard in the NSM UI allows you to choose IDP 4.2 as an option in the OS-Version field, and offers NS-IDP-8200 among the hardware platform options. If you choose IDP 4.1 as the OS version, the Add Device Wizard offers you platforms NS-IDP-75, NS-IDP-250, and NS-IDP-800.
- **Unified Threat Management:** This feature incorporates the existing ScreenOS UTM features while also providing:
 - Read-only, predefined UTM profiles recommended by device implementation and user-customized profiles
 - Antivirus features (Full AV and Express AV)
 - Antispam features
 - URL filter features
 - Content filter features
 - Threat management for common objects in the NSM Object Manager
- **Network discovery and mapping:** You can use the Topology Manager feature in the NSM Device Manager to discover and map your network, and to discover both IDP and JUNOS-based devices. The Topology Manager displays devices and links information in graphical and tabular views. You can view the graphical topology within each of the groups in NSM. Topology Manager also provides a tabular view for end point devices and their connected switches. You can search for a device by its IP address, name, or system description. Topology Manager also provides a tabular view for viewing free ports. Device Discovery also supports mapping the host device name to the NSM device name.
- **Labeling static routes in ScreenOS devices:** NSM enables you to add a description or a comment to static routes in ScreenOS devices.
- **Edit auto-detected device host name:** You can edit or retain the detected device host name as the NSM device name.

- **Device reboot:** You can now reboot all JUNOS-based devices from within the NSM UI.
- **Telnet /CLI window launch:** You can launch a Telnet/CLI window for all connected devices by selecting the option from the device right-click menu within the NSM UI.
- **Application Enhancements:** NSM 2008.2 provides the following enhancements:
 - **Application Policy Enforcement (APE) Rulebase:** NSM allows you to create an APE rulebase on IDP-enabled devices to detect network traffic based on application signatures and to take specified action. You can create APE rules from the Policy Manager or the Application Profiler, from which you can configure match conditions and actions that are based on your network traffic. All APE rules are terminal. NSM supports only predefined application signatures. Initially, the APE rulebase will only be supported on standalone IDP appliances running IDP 5.0.
 - **Integrated configuration of UAC and EX-series switches:** The new UAC Manager feature in the Configure module of the NSM UI enables you to view the associations between Infranet Controllers (IC) and Enforcement Points (EP) in a network. You can choose between IC views and EP views. The IC view provides a list of EPs associated with the IC and their location groups. You can associate or disassociate EPs from a particular IC. The EP view provides a list of associated ICs and their port details. You can use this feature to resolve configuration conflicts, and enable or disable 802.1X ports on enforcement points.
 - **Dynamic detector settings for IDP on SRX-series gateways:** NSM allows you to dynamically load the detector setting and detector version for IDP protocols on SRX-series gateways.
 - **Manage custom attack objects for SRX-series devices:** NSM enables you to import custom attacks and custom attack groups and display them as shared objects in Object Manager. You can also edit custom attacks and custom attack groups using Object Manager and update the device with these changes.
 - **Configuration enhancement for port-level templates in EX-series switches:** With the new port templates feature in the Device Manager, you can view a tabular listing of all port templates known to the system. You can also manage port template associations and add ports to be applied with a template. You can edit VLAN, native VLAN, and the IP address parameters on a port template association. Updating the device pushes all configuration changes to the devices. With the Port Template manager, you can detect and resolve conflicts between a port template and a device configuration.
 - **Inactive policy management:** NSM 2008.2 allows you to retain inactive policies on SRX-series devices. In previous versions, NSM automatically deleted inactive policies through an update action.

- **Cluster management:** Support for active/passive pairs for high availability, or active/active configurations. This feature is supported for the new SRX-series devices as well as for the existing 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:** NSM supports this JUNOS feature for all JUNOS devices, including the new SRX-series, M-series, and MX-series devices, in addition to existing J-series and EX-series devices. This feature allows replication of configuration data at multiple levels within a JUNOS device configuration.
- **Role-based administration:** Allow permissions to be set on all supported device types for new activities, including managing database snapshots that are used to identify the policy version, importing device inventories, and downloading and applying new device schemas from the Juniper Networks update server.
- The NSM Installer provides enhanced descriptions of preinstallation checks.
- NSM now runs with nonroot privileges following installation.
- **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.
- **NSM 2008.2 supports JUNOS 9.2 and JUNOS 9.3**
- The device configuration editor contains an additional Device Description field where you can provide text identifying the device. This device description will also appear in the Device List tab and in the tool tip for the device.
- **The NSMXpress appliance Web UI interface supports the following features:**
 - SNMP monitoring allows SNMP servers to selectively monitor the appliance for traps.
 - Reliable syslog forwarding—A TCP client can be configured to send logs to an external receiver.
- **Enhanced usability features:**
 - **Domain-based filtering for audit logs:** Audit log filters display views that are based on a user's working domain or the domains to which the user has access. For example, a user with access only to a specific subdomain can view only operations that occurred in the subdomain; a user with access to the global domain can view operations in all domains.
 - **Multicolumn filtering for audit logs:** You can configure audit log filters for multiple columns. For the Targets column and the Devices column, you can configure filters based on category, domain, and the complete domain/category/object row.

- **Enhanced drag and drop operations for Policy Manager and Object Manager:** From the main Address Tree and Service Tree, you can drag Address and Service objects into and out of groups. From the main Device tree, you can use drag and drop operations to modify device groups. Drag and drop support is also available in configuration dialogs for the following: Source and Destination columns of Zone-based and Global Firewall rulebases; Source, Destination, and Attacks columns of IDP rulebase; Source, Destination, and Attacks New Features 7 columns of Exempt rulebase; Source and Destination columns of Backdoor rulebase; Source and Destination columns of Network Honeypot rulebase; Source and Destination columns of Traffic Anomalies rulebase; Source and Destination columns of SYN Protector rulebase; and Source and Destination columns of Permitted Object entries.
- **Add global domain objects using Replace With in a Subdomain:** In Object Manager, if an NSM user has permission to view global domain objects in the selected category of address or service objects, then a Replace With operation displays all the objects for the selected category from the current domain and the global domain. However, the selected object to be replaced is not displayed.
- **Search for duplicate objects:** In Object Manager, the NSM user can search for duplicate objects from the Address, Service, Attack, and AV categories and delete the unused duplicate objects. The UI displays a report of all the used and unused duplicate objects; then the user can choose to delete the objects or cancel the operation.
- **Displaying objects that are members of an Object Group:** When a Policy Manager tree table view includes an address group or service group, you can view the object (leaf member) count for the address or service group by hovering over the group with the mouse. This feature is also supported for polymorphic objects in the address or service object category.
- **Applying the same object to multiple rules:** You can apply the same object (column value) to a selection of policy rules. Rule groups must be in an expanded state to apply the same object to the rules of a rule group. You cannot apply the same object to selected rules for columns that disallow duplicate values, such as the rule ID and No. columns.
- **Cut, Copy, and Paste support for fields in policy rules:** You can cut, copy, and paste a column field in a rule to other column fields that have the same context. When you cut or copy a field, you can perform multiple paste operations. Cut, copy, and paste operations are available for all column fields except rule ID column fields. The cut operation is not available for generic column fields such as Notification and Action.
- **Drag and drop enhancements for objects:** In Policy Manager, when you drag an object beyond the visible rows or columns in the security policy, the scroll bar moves horizontally or vertically if there are more rules or columns available into which an object can be dropped. Previously, objects could only be dragged and dropped within the visible rows or columns in the security policy.

- **VPN filtering:** You can configure, save, and modify a VPN filter to control the information that is provided in the VPN Monitor. VPN filters are saved per user and are used to monitor VPN information related to the type, status, or the specific security device or virtual system associated with the VPN tunnel that you want to view.
- **Application volume tracking (AVT):** AVT allows network administrators to monitor network traffic volume at the application and application-group level. You can view application and application group level traffic from the Application Profiler view, which is divided into two panels. On the left side, the hierarchical application view displays a tree of the application categories with volume information displayed in bytes and packets. On the right side, the application session view displays the application name and the aggregated bytes and packets by application. By default, this view contains only the data collected during the configured time interval. You can also configure filters from the Application Profiler to display only the network traffic data that you want to monitor.
- **New Shared Objects:**
 - **Access Profile:** Access profile objects can be shared across security policies that are assigned to J-series routers and SRX-series gateways managed by NSM. The access profiles shared object is not supported on ScreenOS devices. When a security policy using access profiles is assigned to a ScreenOS device, the access profile settings are removed before the security policy is updated.
 - **Routing Instance Objects:** A routing instance object allows you to share routing instances in the RADIUS server and LDAP server configurations within the access profile object. A routing instance object is a polymorphic object (similar to zone objects) that maintains the mapping between the actual routing instance and the device in which it is created. The routing instance shared object is not supported on ScreenOS devices.

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

Solaris Locales

Before installing NSM on a Solaris server, a specific set of locales must be installed, and appropriate edits made 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 2008.2 from versions 2007.2rX, 2007.3rX, and 2008.1rX.

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 for J-series and EX-series devices 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 to NSM.
- For SSL VPN SA and Infranet Controller:
 - NSM 2008.2 manages Secure Access SSL VPN SA series devices. The management for Secure Access family of devices will be available with SSL release 6.3.
 - 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 (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 setup instructions and template usage guidelines for SSL VPN SA (SA) and Infranet Controller (IC) 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). For NSM*Xpress*, there can be no more than 2 devices included in a single job. The following files on the NSM software server must be edited as described below (no changes are needed for NSM*Xpress*):

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

- 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
- In `/usr/netscreen/GuiSvr/var/xdb/specs/jax.spec`, change **Xmx512** to **Xmx1024m**
- In `/usr/netscreen/DevSvr/bin/.devSvrDirectiveHandler`, change **Xmx102400000** to **Xmx204800000**

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.

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 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 guidelines apply to templates that are created from scratch or through promotion.
2. To replicate the configuration from one cluster (source) to another cluster (target) through 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):

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Node-Local Configuration (NL):

```
/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
```

All other settings are CG.

7 Fixed Issues

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

- 289866— The NSM UI address object length validation does not match the address object maximum length supported in ScreenOS.
- 298203— **Bgroup** is unavailable as a source interface for NSM communication on SSG5 devices.
- 305005—The change of ports in the NSM device server is not reflected in the device commands generated by NSM.
- 310634—Recreating route-based VPNs through the VPN Manager generates override errors.
- 312350—The NSM database loses the settings made on redundant interfaces.
- 314020—The User Service Group default value (256) in the NSM device root profile does not match the value allowed (1024) in ScreenOS.
- 387078—The "attack DB" update through a proxy with password authentication does not work in NSM 2008.1r1. Update through a proxy without password authentication works. As documented in 410288, you need to restart the GUI client for the proxy settings to take effect.
- 387843—The SCCP algorithm is incorrectly set to true for vsys devices running ScreenOS 5.4. When the firewall is upgraded to ScreenOS 6.1, an exception is generated on update for "set alg sccp enable."
- 389147—Gateway Tracking-enabled routes created on cluster members are not pushed to the device.
- 392461—NSM incorrectly handles "permitted IP" in nested templates.
- 393713—The communications NSRP config sync is wrongly enabled on vsys cluster Vrouters.
- 395678—NSM allows the dhcp server to be configured on a subinterface in a cluster.
- 395918—NSM does not have an option to bring down an HA interface.
- 396223—NSM displays incorrect ScreenOS software versions when the same ScreenOS version is loaded for multiple platforms.
- 396457—The maximum number of security zones allowed in an SSG-5 device is low.
- 398080—Enabling OSPF on cluster members causes an error in the cluster.
- 399832—If an interface IP is used as a VIP, you cannot create any more VIPs.
- 399845—If two interfaces are in the same zone, you cannot add a VIP on the second interface.

- 399966—NSM removes ethernet interface associations from bgroup0 after they are imported.
- 401239—If the NSM base directory is not /usr/netscreen, you cannot upgrade firmware.
- 402744—When new ScreenOS images are uploaded after a migration to NSM 2008.1R2, platform information for existing ScreenOS images is lost.
- 405980—The device server fills all 25 device Daemon logs within two minutes, with the error message that the domain version is outdated.
- 408851—Performance issues on some NSMXPRESS environments caused by a spelling mistake "catgory".
- 306199—The error message for insufficient disk space during a default installation provides two solutions of which solution 2 is wrong.
- 398611— When you import a device configuration, the FQDN peer ID is disassociated from the IKE gateway in NSM and this change is not reflected in the delta config summary.
- 401535—IDP policy with 'All Attacks' is not pushed to an IDP cluster.

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

- 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.
- 303308— Excessive retry operations can cause a DMI device to malfunction if NSM closes the connection to the device while the device is trying to connect to NSM. When you add a DMI device through the NSM UI, you first add an unreachable device and then use the generated key to configure the device so that the device can initiate the connection to the NSM server. The connection will fail, however, if NSM closes the connection because:
 - The device is in the modeled RMA state.
 - The device shares a duplicate sequence number with another managed device.
 - The platform or device type (cluster member, virtual chassis, and so on) you specified while adding the device does not match the device itself.

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

- 304406—During an NSM installation in a HA environment, when performing a refresh with the NSM installer or NSMXpress UI, the HA peers may not initialize communication properly. This problem commonly occurs when you migrate from a single NSM server to a HA configuration. The error does not occur when you perform a clean install or an upgrade using the NSM installer.
- 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.
- 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.
- 293292—When a JUNOS-based device managed by NSM 2008.1 is downgraded to JUNOS 9.0, the connectivity between the device and NSM is lost. To reestablish a connection, the device should be reconfigured through the CLI. Alternatively, you can also delete the device from NSM and then add it again.
- 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.
- 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.

- 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.
- 296323—The NBI incorrectly allows objects with duplicate names to be added. Application writers need to check for duplicate names before calling the NBI to add objects.
- 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.
- 283069—Significant delays (up to 30 hours) may occur between the time that NSM receives logs from firewalls and sends them to the syslog server. This situation arises when the logwalker process is hung. When this happens, NSM stops processing the syslog logs.
- 284373—If you update a regional server to the Central Manager with a newly created rule and then remove the Central Manager from the network, the rule remains on the regional server. The rule can only be removed by editing the backend database.
- 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.
- 291820-1—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 (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.
- 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.
- 397158—NSM does not allow you to turn off an IF-MAP server. As a workaround, click on Client. NSM then enables the OK button. Click on No IF-MAP. NSM leaves the OK button enabled and allows you to save the change.
- 398045—Some localization options that are present in the NSM UI are not available in the Web UI.
- 398094—When the RADIUS client template is removed from NSM, the update device operation fails.
- 312498—The upgrade from NSM 2008.1 to 2008.2 takes significantly longer than the upgrade time for 2007.3 to 2008.1 because of the increase in installer size and the quantity of data in 2008.1. Both backing up the old software and data, and installing the new software take longer.
- 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.
- 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.
- 401197—NSM fails to update the ISDN Dialer interface settings with the PPP profile.
- 401811—NSM disables the edit option on the Shared-DMZ Vrouter on vsys devices.
- 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.
- 405579—NSM does not allow you to configure more than one VIP entry with "Same as Interface IP" settings on NS5GT devices running ScreenOS 6.2.
- 406557—When you create a global MIP, DIP or VIP object on a ScreenOS device and then update it in NSM, some detailed information such as NHTB and Ping entries are lost.
- 407558—Devices with Shared-DMZ zones and their corresponding Vrouters are not imported to cluster-vsys devices. They are imported correctly in a single vsys device.
- 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.
- 410288—When you change the proxy settings in NSM, they take effect only after you restart the GUI server.
- 410797—After a migration to NSM 2008.2, the Juniper update credentials are lost. You need to re-enter the credentials.

8.2 *J-series Devices Running JUNOS Software*

- 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.
- 402298— When a firewall policy with network address objects is applied to JUNOS devices, the device update operation in NSM fails, because DMI devices do not support network address objects.

8.3 *EX-series Switches*

- 293292—Device connectivity ends in NSM when JUNOS is downgraded from 9.1 to 9.0.
- 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.
- LAG links are discovered as multiple, separate links and not as a bundled link because the discovery of LAGs is not explicitly supported by Topology Discovery.

- 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 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.

- Topology discovery does not support clusters.
- 405316—Wrong RSTP/STP information fetched from EX-series devices causes Topology Discovery to find wrong bridge-to-bridge links. To work around this issue, enable only LLDP.
- 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.
- 403380—In the Topology Manager, when a very broad subnet is included, the large number of IP addresses causes the topology discovery to remain incomplete. The workaround is to include subnets narrower than 255.255.240.0.
- 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.

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. The update will fail if insufficient RAM is available. You can contact JTAC for a workaround.

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

Controller

- 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.
- 283276—The model-activate workflow is not supported for SSL VPN SA and Infranet Controller devices.
- 55674—In the NSM UI, the group selector panels titled "Members/Non-Members" map to the panels titled "Available/Selected" or "Available List/Selected List" in the SSL VPN SA or Infranet Controller administration UI.
- 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.

- 55933—SSL VPN SA device configuration can be promoted to an SSL VPN SA template and applied to other SSL VPN SA device objects. Likewise, Infranet Controller device configuration can be promoted to an Infranet Controller template and applied to other Infranet Controller device objects. However, promotion of SSL VPN SA device configuration to an Infranet Controller template (or vice versa) is not supported.
- 56704—When SSL VPN SA and Infranet Controller device objects are promoted to templates, default values in the device object are not promoted to the template. This behavior is working as designed and is not a defect.
- 57104—Identifier names (names of key fields) in the SSL VPN SA and Infranet Controller configuration, such as the names or realms, roles, sign-in URLs, sign-in pages and so on, **cannot** be changed through the NSM UI. This is established NSM behavior and is not a defect. However, identifier names can be changed through the SSL VPN SA and Infranet Controller Web UI.
- 57190—Selection of multiple objects is not available through the NSM UI, even though this capability is available on the SSL VPN SA and Infranet Controller Web UI in multiple places, for example, resource profiles, admin roles, and user realms.
- 55527—The SSL VPN SA and Infranet Controller admin UI allows duplication of objects such as roles or resource profiles. This capability does not exist in the NSM UI.
- 399744—After a device update, the "Set device attributes specified below" option in a Secure Access device is disabled, if this option was selected during the creation of a session export policy in NSM.
- 399740—Tabs inapplicable to Secure Access devices, such as "this server" and "session import policy," are visible in NSM when an IF-MAP configuration is performed.
- 399743—NSM does not have a field for specifying identity when an administrator creates a session export policy. The administrator can, however, select different identity types.
- 394241—After a promote template operation on a device configuration, there is no indication whether the promotion was successful.
- 398436—Updating any log on the Web UI causes NSM to wrongly display a changed device configuration status.
- 399802—NSM does not display identity options for Federation server session export policies and does not display IF-MAP device attributes.
- 400551—The NSM UI wrongly displays IF-MAP-Federation as IF-MAP-Fed.

8.6 SRX-series Devices

- 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.

9 Requesting Technical Support

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

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

9.1 Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

9.2 Opening a Case with JTAC

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

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

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

Documentation Feedback

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

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

- Document name
- Document part number
- Page number

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

Copyright © 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.