Network and Security Manager Release Notes

February 19, 2018
Revision 37

Contents

Version Summary

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

New Appliances and Functionality

NSM introduces the following new appliances with the following specified components:

- **NSM4000** — A 2-U, rack-mountable chassis with an AC power supply module and an optional AC/DC power supply module; six 1-TB hard drives in a RAID 10 configuration; two externally accessible cooling fans; and four Gigabit Ethernet interfaces.

New Features in 2012.2

NSM release 2012.2 supports the following new features:

- NSM 2012.2R14: In Junos OS Release 12.1X46, Junos OS Release 12.3X48 and earlier, the **Destination Port** node format of source NAT and destination NAT is supported for both old and new node format. Also, you can now specify one or more destination port range (upper and lower limit) for rule matching. The destination port range is 1 to 65,535.
- Beginning in version v4 of CentOS 6.5 generic ZIP files, major RPM upgrades are listed inTable 1 on page 3.

Table 1: Major RPM Upgrades in Version v4 of CentOS 6.5 Generic ZIP Files

Packages	RPM Versions
GConf	GConf2-2.28.0-6.SCLC6_5.R1.0.1.i686
ORBit	ORBit2-2.14.17-3.2.SCLC6_5.R1.0.1.i686
libIDL	libIDL-0.8.13-2.1.SCLC6_5.R1.0.1.i686
sgml	sgml-common-0.6.3-32.SCLC6_5.R1.0.1.noarch

- Beginning in version v3 of CentOS 6.5 generic ZIP files, major RPM upgrades are listed in Table 2 on page 4.

Table 2: Major RPM Upgrades in Version v3 of CentOS 6.5 Generic ZIP Files

Packages	RPM Versions
Kernel	kernel-2.6.32-642.11.1.SCLC6_5.R3.10.1.el6.i686
Openssl	openssl-1.0.1e-48.SCLC6_5.R3.10.1.el6.i686
openssh	openssh-5.3p1-118.1.SCLC6_5.R3.10.1.el6.i686
Ntp	ntp-4.2.6p5-10.SCLC6_5.R3.10.1.el6.i686
Httpd	httpd-2.2.15-55.SCLC6_5.R3.10.1.el6.i686
Glibc	glibc-2.12-1.192.SCLC6_5.R3.10.1.el6.i686
Bash	bash-4.1.2-33.SCLC6_5.R3.10.1.el6.i686
Wget	wget-1.12-8.SCLC6_5.R3.10.1.el6.i686

- Beginning in NSM 2012.2R13a, NSM supports management of LN1000-cc devices with Junos OS Release 12.1X46-D55 and its successive maintenance releases.
- Beginning in NSM 2012.2R13a, NSM supports management of SRX550 devices.
- Beginning in NSM 2012.2R14, the OpenSSL version is upgraded to 1.0.2n.
- Beginning in version v2 of CentOS 6.5 generic ZIP files, major RPM upgrades are listed in Table 3 on page 4.

Table 3: Major RPM Upgrades in Version v2 of CentOS 6.5 Generic ZIP Files

Packages	RPM Versions
Kernel	kernel-2.6.32-573.3.1.SCLC6_5.R3.8.1.i686
Openssl	openssl-1.0.1e-30.SCLC6_5.11.R3.5.1.i686
Sudo	sudo-1.8.6p3-19.SCLC6_5.R3.6.1.i686
Ntp	ntp-4.2.6p5-5.SCLC6_5.2.R3.8.1.i686
Httpd	httpd-2.2.15-47.SCLC6_5.R3.7.1.i686
Bc	bc-1.06.95-1.SCLC6_5.R3.0.1.i686

- Beginning in version v1 of CentOS 6.5 generic ZIP files, major RPM upgrades are listed in Table 4 on page 5.

Table 4: Major RPM Upgrades in Version v1 of CentOS 6.5 Generic ZIP Files

Packages	RPM Versions
OpenSSL	openssl-1.0.1e-30.SCLC6_5.9.R3.5.1.i686
Nss	nss-3.16.2.3-3.SCLC6_5.R3.1.1.i686
Glibc	glibc-2.12-1.149.SCLC6_5.7.R3.5.1.i686
Bash	bash-4.1.2-15.SCLC6_5.2.R3.0.1.i686
Kernel	kernel-2.6.32-504.12.2.SCLC6_5.R3.3.1.i686
Ntp	ntp-4.2.6p5-2.SCLC6_5.R3.1.1.i686
Wget	wget-1.12-5.SCLC6_5.1.R3.1.1.i686

- Beginning in version v4 of CentOS 5.7 generic ZIP files, major RPM upgrades are listed in Table 5 on page 5.

Table 5: Major RPM Upgrades in Version v4 of CentOS 5.7 Generic ZIP Files

Packages	RPM Versions
Httpd	httpd-2.2.3-91.el5.centos
Syschecktrapd	syschecktrapd-1.1-10_5.x
Glibc	glibc-2.5-123.el5_11.1
	glibc-common-2.5-123.el5_11.1
Ntp	ntp-4.2.2p1-18.el5.centos
Bash	bash-3.2-33.el5_11.4
Nsmxwui	nsmxwui-2.6-9
Nss	nss-3.16.2.3-1.el5_11
Openssl	openssl-0.9.8e-33.el5_11

Table 5: Major RPM Upgrades in Version v4 of CentOS 5.7 Generic ZIP Files *(continued)*

Packages	RPM Versions
Kernel	kernel-2.6.18-400.1.1.el5
	kernel-xen-2.6.18-402.el5
	kernel-xen-devel-2.6.18-402.el5
	kernel-PAE-2.6.18-402.el5
Rsync	rsync-3.0.6-6.el5_11

- Beginning in the CentOS 6.5 upgrade ISO for NSMXpress/NSM3000 appliances, major RPM upgrades are listed in Table 6 on page 6.

Table 6: Major RPM Upgrades

Packages	RPM Versions
OpenSSL	openssl-1.0.1e-30.SCLC6_5.5.R3.2.1.i686
BASH	bash-4.1.2-15.SCLC6_5.2.R3.0.1.i686
httpd	httpd-2.2.15-39.SCLC6_5.R3.2.1.i686
NSS	nss-3.16.2.3-3.SCLC6_5.R3.1.1.i686
Glibc	glibc-common-2.12-1.149.SCLC6_5.5.R3.2.1.i686
	glibc-2.12-1.149.SCLC6_5.5.R3.2.1.i686
NTP	ntp-4.2.6p5-2.SCLC6_5.R3.1.1.i686
WGET	wget-1.12-5.SCLC6_5.1.R3.1.1.i686

- Beginning in NSM 2012.2R10, NSM supports to add security devices with IPv6 addresses when NSM server is configured with an IPv6 management address.

  Devices running ScreenOS and SRX Series high-end devices with IPv6 addresses, can also be added to NSM server with IPv4 management address when MIP address is configured with IPv6 address in NSM under Server Manager>Servers>Device Server>MIP.

  NSM supports RADIUS server authentication with IPv6 address for NSM users.

  NOTE: **Devices running ScreenOS and SRX Series high-end devices should have IPv6 support in nsm-agent and outbound-ssh respectively.**

For more details, see the *Installation Guide* and *Admin Guide*.

- Beginning in NSM 2012.2R10, the API is enhanced to support the following functions:
  - Manage VPN configuration in DeviceObj.junos-es container for SRX Series devices
  - Modification of management interface(Fxp0) for SRX Series devices
  - Assign SNMP name and SNMP contact SRX Series devices

  For more details, see the *API Guide* at the following location:

  http://www.juniper.net/techpubs/en_US/nsm2012.2/information-products/pathway-pages/nsmxpress/2012.2/index.html
- Beginning in version v3 of CentOS 5.7 generic ZIP files, the bash shell is upgraded to version 3.2-33.
- Beginning in version v3 of CentOS 5.7 generic ZIP files, network file system support is available for NSM appliances.
- Beginning in version v3 of CentOS 5.7 generic ZIP files, the open SSH package is upgraded to version 6.6.
- Beginning in version v3 of CentOS 5.7 generic ZIP files, the systaillogd package is upgraded to version 1.0-5.
- Beginning in NSM 2012.2R9, the JRE version is upgraded from 1.6.0 to 1.7.0_51. NSM 2012.2R9 can be installed only on RHEL version 5.5 or later, because the latest Java version support is available only from RHEL version 5.5 or later. In NSM appliances, NSM 2012.2R9 can be installed on CentOS version 5.7 or later. The NSM appliance OS upgrade package currently available is CentOS version 5.7.

  Existing users with RHEL servers need to upgrade their servers to RHEL version 5.5 or later, before installing or upgrading to NSM 2012.2R9 or later versions.

  Existing users of NSM appliances need to upgrade their servers to CentOS version 5.7 before installing or upgrading to NSM 2012.2R9 or later versions.

  

  NOTE: **To verify the latest Java version, run the following command:**

  /usr/netscreen/GuiSvr/lib/jre/bin/java –version
- Beginning in NSM 2012.2R12, the NSM client can be installed on Windows 10.
- Beginning in NSM 2012.2R9, the NSM client can be installed on Windows 8.1.
- Beginning in NSM 2012.2R9, NSM can be installed with minimal OS installation of RHEL 6.5.

  

  NOTE: **Install the system update packages available as a part of** 2012.2R9 software packages**, before installing NSM with the minimal installation of RHEL 6.5.**
- Beginning in NSM 2012.2R9, the OpenSSL version is upgraded to 1.0.1h.

- Beginning in NSM 2012.2R8, the option to create host and network objects is available under address group objects.
- Beginning in NSM 2012.2R8, alternating rows of policy rules are displayed in different colors.
- Beginning in NSM 2012.2R8, NSM provides the multi-schema support feature that lets you manage various Junos OS 12.1 Releases (12.1X44, 12.1X45, 12.1X46, and so on) separately.

  NSM versions 2012.2R7 and earlier with a schema version greater than 296 will not support managing X series of Junos OS Release 12.1 or later images for J and SRX Series devices.

  

  NOTE: We recommend upgrading NSM to the following versions for managing X versions of Junos OS Release 12.1 or later images for J and SRX Series devices:

  - NSM version 2012.2R8 or later
  - Schema version 297 or later

  While adding SRX Series and J Series devices in a cluster or as standalone devices in the unreachable and model work flow, select the appropriate OS version from the **Managed OS Version** drop-down list. For example, select 12.1X46 from the **Managed OS Version** drop-down list to add J Series and SRX Series devices with the 12.1X46 image in the unreachable and model work flow. The following changes affect NSM behavior:

  - In the model and unreachable workflow, the NSM GUI displays 12.1X images (12.1X44, 12.1X45, 12.1X46, and so on) in the **Managed OS Version** drop-down list separately.

    

    NOTE: This behavior is also observed in the earlier versions of NSM if the schema is upgraded to 297 or later versions.

  - You must perform an adjust OS version (single or bulk) operation to upgrade the managed device OS versions to the appropriate version for J Series and SRX Series devices with 12.1X images.
  - To support the multi-schema feature after upgrading the NSM version to 2012.2R8, the upgraded NSM schema version reverts to the default schema version (297) when the existing schema version is later than 297. The following output is an example displayed during the upgrading process:

    ----- LOADING DEFAULT SCHEMA VERSION 297 TO SUPPORT MULTIPLE SCHEMA VERSION FEATURE -----
    NOTE: User can upgrade schema version to 298, after NSM upgrade is successful

  After upgrading the Solaris build to 2012.2R8, you must immediately upgrade the schema version from 283 (default schema version) to 297 or later versions for the following reasons:

- To enable the multi-schema feature
- To manage the J Series and SRX Series devices with 12.1X images

NOTE: After upgrading the Solaris build to 2012.2R8, the device connection status remains down in the NSM GUI for J Series and SRX Series devices with 12.1X images unless the schema is upgraded to 297 or later versions.

- Beginning in NSM 2012.2R7, support for multiple proxy IDs is available for SRX Series devices running on Junos OS Release 12.1X46-D10 and later releases.

  To avail the multiple proxy ID support in VPN Manager, under **Device Manager** > **Devices**, right-click the SRX Series device running the 12.1X46-D10 image and select the **Use Multiple Proxy ID** check box.

- Beginning in NSM 2012.2R7, support for Web filtering in UTM is available for SRX Series high-end devices running on Junos OS Release 12.1X46-D10 and later releases.
- Beginning in NSM 2012.2R7, support for antivirus, antispam, and content filtering in UTM is available for SRX Series high-end devices running on Junos OS Release 12.1X46-D10 and later releases.
- Beginning in NSM 2012.2R7, SRX Series cluster devices are managed using either SSH keys or password authentication.
- Beginning in NSM 2012.2R7, when performing a search using copied text, NSM truncates the text by removing any spaces that appear before or after the text.
- Beginning in NSM 2012.2R7, right-clicking on an object in firewall policy rule brings up the **Find usage** option.
- Beginning in NSM 2012.2R7, installation is supported on Linux servers that run version RHEL 6.5. Before you can install NSM, you need to install the system update file corresponding to RHEL 6. The system update file for RHEL 6 is available as part of the Linux system update package for NSM 2012.2R7.
- Beginning in NSM 2012.2R6, support is provided for the configuration of the host name as gateway address for main mode in VPN Manager. Configuring the host name is optional. However, you need to configure the host name if the termination interfaces of at least two devices have dynamically assigned IP addresses and VPN is to be setup between them. In the previous versions of NSM, by default the VPN Manager selects **IP address** as the gateway address in the main mode.
- Beginning in NSM 2012.2R6, support is available for Junos devices running on Junos OS version 12.1X46. Previous versions of NSM will not support devices running on Junos OS version 12.1X46.
- Beginning in NSM 2012.2R6, NSM API has been enhanced with additional functionalities. For more details, see the *API Guide* at the following location: http://www.juniper.net/techpubs/en_US/nsm2012.2/information-products/pathway-pages/nsmxpress/2012.2/index.html.

- Beginning in NSM 2012.2R5, the PostgreSQL version is upgraded to 8.4.17 in Linux server. To upgrade the PostgreSQL version in Linux server, install the system update files provided with the release before installing 2012.2R5 Linux build.

  For NSM appliances, PostgreSQL upgrade is available with version v2 of CentOS 4.x and CentOS 5.7 generic zip files. To obtain the upgraded version of PostgreSQL in NSM appliances platform, upgrade to 2012.2R5 using Generic Zip file v2. For more details about the upgrade procedure, see the *Installation Guide*.

- Beginning in NSM 2012.2R5, the Apache Tomcat version is upgraded to 6.0.37.

- Beginning in NSM 2012.2R5, two new Kconsts are supported for ISG-IDP and standalone IDP, and three Kconsts are supported for SRX Series devices running on Junos OS Release 12.1X45-D10 and later releases.

  - Kconsts for ISG-IDP/standalone IDP are sc_tcp_action_on_reass_failure and sc_tcp_error_logging.

  - Kconsts for SRX series devices are action-on-reassembly-failure, tcp-error-logging, and no-tcp-error-logging.

- Beginning in NSM 2012.2R4 support for chained operation for device update is available.

- Beginning in NSM 2012.2R4 support for global search for NAT objects is available.

- Beginning in NSM 2012.2R4 support for negate-address is available for J and SRX Series devices running on Junos OS Release 12.1X45-D10 and later releases. With this feature, source and destination address can be excluded in zone base and global policy rulebases.

- Beginning in NSM 2012.2R4 support for crypto suite-B-GCM-128/256 predefined proposal sets and ECDSA-256/384 certificates is available for J and SRX Series devices running on Junos OS Release 12.1X45-D10 and later releases.

- Beginning in NSM 2012.2R4 in NAT rule base, additional match conditions source-address, source-address-name and source-port are supported in Static NAT rule. This feature is applicable for J and SRX series devices with Junos OS Release 12.1X45-D10 and later releases.

- Beginning in NSM 2012.2R4 in NAT rule base, additional match condition source-port is supported in source NAT rule. This feature is applicable for J and SRX series devices with Junos OS Release 12.1X45-D10 and later releases.

- Beginning in NSM 2012.2R4 in NAT rule base, as part of action Clear-threshold and Raise-threshold are additionally supported on Source, Destination and Static NAT rules. This feature is applicable for J and SRX series devices with Junos OS Release 12.1X45-D10 and later releases.

- Beginning in NSM 2012.2R4, while performing device upgrade through NSM, an option is provided to copy the image file into SRX Series devices without installing the package.

- Beginning in NSM 2012.2R3, when you start typing text to be searched, NSM displays the search text as blue until you press **Return** or **Enter** on the keyboard. The color of the text changes to black when a match is found and to red if no match is found. You can use the arrow keys to proceed to the next match item.

- Beginning in NSM 2012.2R3, the predefined and customized attack groups members match when the filter options are same in both attack groups.
- Beginning in NSM 2012.2R3, for J Series and SRX Series devices, multiple clients are supported in the firewall authentication pass-through and web authentication methods that can be configured in zone-based and global policies for Junos OS rulebases.
- Beginning in NSM 2012.2R3, for devices running ScreenOS, tables of DIP, MIP and VIP display the IP addresses with search options.
- Beginning in NSM 2012.2R3, in NSM for SRX Series devices, enable and disable options are included for NAT rules and rule sets.
- Beginning 2012.2R2, incremental attack update is enhanced for SRX Series branch devices. While performing incremental attack update, instead of sending the complete signature file, NSM trims **SignatureUpdate.xml.gz** file, specific to the attack version. This behavior is applicable only if the below conditions are satisfied :

  a. Attack version difference between NSM and SRX Series branch device is 1.

  b. Incremental difference of the file is not present in NSM.

- NSM supports automatic purging of database versions at configured intervals. When saved database files exceed the maximum threshold, only the configured minimum database version is retained.
- NSM supports loading of ScreenOS device and J Series and SRX Series devices schema based on the startup options provided in the installer script.
- NSM caching has been enhanced to clean up all objects in the cache, at configured interval to make conservative use of the available memory of the java process.
- On ISG and SRX Series devices, NSM provides the option to update only the firewall configuration without updating the IDP configuration. This option helps in reducing the total update time required for the devices.
- NSM supports software firmware upgrade for eight JUNOS devices concurrently.
- NSM provides nested service group support for J Series and SRX Series devices.
- Performance improvement on shared object, such as address, service and custom attack object loading in NSM.
- Performance of delta and update workflows in NSM has been enhanced.
- Performance of firewall policy loading in NSM GUI has been enhanced.
- Find usage-related changes to clean up non-existent rules and policies by checking for stale entries has been enhanced in NSM.

New or Changed Information

The following list provides new or changed information supported in this release:

- After migrating to NSM 2012.2R11, any VPN configuration changes saved in VPN Manager cause the existing proxy identity configuration to update from 0.0.0.0/32 to 0.0.0.0/0.

  NOTE: **NSM does not display proxy ID changes in the delta config window after a successful update.**

- Beginning in NSM release 2012.2R10, initiating an SSL connection to the NSM server using SSL version 3 is not supported.
- Beginning in NSM release 2012.2R10, NSM provides **Show Address Tree View** and **Show Shared Objects for policy view** checkboxes under Tools>Preferences>System Properties>Performance Options.

  When you uncheck these checkboxes, NSM does not display the following respective entities to enhance the GUI performance while loading address objects and policies:

  - The **Address Tree** tab under Object Manager>Address Objects and Policy Manager>Policies>*Device Policy Name*>Shared Objects for Policy
  - The **Shared Objects for policy view** box under Policy Manager>Policies>*Device Policy Name*

  NOTE: **By default, the Show Address Tree View and Show Shared Objects for policy view checkboxes are selected.**

- Beginning in NSM release 2012.2R6, NSM supports disabling the option Firewall Policy ID Validation.

  To disable the duplicate rule ID error message in firewall policy rules, navigate to **Tools** > **Preferences** > **System Properties**. Under System Properties, click **Performance Options** and select the **Firewall Policy ID Validation** check box. Even after selecting this option, if you want to perform a one-time validation to check for duplicate rule IDs for any specific policy, click **Show Warning** in Firewall Policy window.

- Beginning in NSM release 2012.1R1, NSM supports versioning for Junos OS attack download.
- Beginning in NSM release 2012.2, NSM supports importing of MIP groups from ScreenOS devices running release 6.2 or later.
- Beginning in NSM release 2012.2, support for import of device configuration from file for ScreenOS cluster.
- The Junos OS device schema handling has been enhanced in NSM.
- In NSM, per-policy TCP options like **syn-check-required** are available for J Series and SRX Series device policies.

- In NSM, validation option is enhanced for illegal character, character length of the address and service names, and limit on the count of the address group.
- NSM supports global address group in source, destination and static NAT rulebases.
- From 2012.1R2 release onwards, JRE version is upgraded to address security vulnerability issues that existed in the previous JRE used with NSM.

  CVE addressed with JRE 1.6.0_34 version upgrade are:

  - CVE-2011-0862
  - CVE-2011-0873
  - CVE-2011-0815
  - CVE-2011-0817
  - CVE-2011-0863
  - CVE-2011-0864
  - CVE-2011-0802
  - CVE-2011-0814
  - CVE-2011-0871
  - CVE-2011-0786
  - CVE-2011-0866
  - CVE-2011-0868
  - CVE-2011-0872
  - CVE-2011-0867
  - CVE-2011-0865
- From 2012.1R1 release onwards, downloading the Windows or Linux client package from the Solaris build using the web browser is not supported.
- If the *Auto Heap Size Adjustment* feature is being used, disable it before migrating to NSM 2012.1 version.

  To disable**Auto Heap Size Adjustment** option, navigate to **Tools** > **Preferences** > **System Properties** > **Options** .

  If the NSM 2012.1 version is migrated without disabling Auto Heap Size Adjustment, then the NSM client might fail to connect to the NSM server provided in a large DB case.

  To edit or modify the xdb content for systemprefs container:

  Edit the NSM server:

  1. Open xdb in write mode **sh /usr/netscreen/GuiSvr/utils/.xdbViewEdit.sh**.
  2. Select **option 7** (View/Edit record by domain-id.category.tuple-id).

3. Write **0.systemprefs.0** to enter into systemprefs container.
4. Modify true to false for **enableheapsizeadjustment** option.
5. Write and quit **(:wq!)**.

Edit the NSM client:

1. Open **NSM.lax** file at NSM installed directory.
2. Set the value for **lax.nl.java.option.java.heap.size.max=1280m** if it is 768 m.

Before You Install NSM

Windows 7 Support

NSM supports installation of the NSM client on the Windows 7 32-bit and 64-bit operating system. However, before installing the client or updating to the latest schema, ensure that Active Windows 7 user should have read and write permission for creating new directories and read, write and execute permission for creation and saving of new files under **NSM_Installed_Directory**.

By default, NSM client is installed under program files (x86) on Windows 7 where permissions are usually restrictive.

If the active Windows 7 user does not have permissions as mentioned above under program files (x86) , install NSM client under any other directory where sufficient read, write and execute permission is provided for the directories and files. For Example: **C:/Users/Public**.

NSM Client Installation for Solaris

From 2012.1R2 release onwards, to install Windows or Linux client for Solaris build download the client installer separately from the software download page.

Solaris Locales

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

NSM Appliance Installation

From 2012.2R1 release onwards, a separate downloadable zip package for appliances is discontinued for service releases. Instead, the Generic ZIP file will be provided. Use the latest Generic Upgrade package from the Software download site. NSM installer now has the capability to modify the version information on NSMXpress appliance.

NOTE: If you have already upgraded the NSM appliance to NSM 2012.2 version, and if you want to upgrade to any release between 2012.2R1 and 2012.2R4, you can upgrade using the Linux build of the respective service release. However, if you need to install the service releases 2012.2R5 or higher, use the version 2 of generic offline or online files.

Use the following files for Offline upgrade of NSM appliance to NSM 2012.2 service release:

The files required for the Offline upgrade of NSM appliance to NSM 2012.2 service release are listed in Table 7 on page 15. The files can be downloaded from http://www.juniper.net/customers/csc/software/.

Table 7: Files for Offline Upgrade

File Name	Download Link
nsm_generic_offline_upgrade_CentOS4.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 4.x (**X** in **vX** represents the latest version of the generic zip file).
nsm_generic_offline_upgrade_CentOS5.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 5.x (**X** in **vX** represents the latest version of the generic zip file).
Linux Server Installer for the required NSM version Example: nsm2012.2R1_servers_linux_x86.zip	Linux Server

To upgrade from previous NSM versions (versions below 2012.2) to service release of 2012.2, use the following procedure:

- Offline mode for CentOS 4.X—Unzip **nsm_generic_offline_upgrade_CentOS4.x.zip** using **unzip nsm_generic_offline_upgrade_CentOS4.x.zip**, in the NSM appliance. OR
- Offline mode for CentOS 5.7—Unzip **nsm_generic_offline_upgrade_CentOS5.x.zip** using **unzip nsm_generic_offline_upgrade_CentOS5.x.zip**, in the NSM appliance.

  NOTE: If the online mode is chosen, only the **upgrade-os.sh** file must be copied from the **NSM Appliance Generic Online Upgrade Script_vX** (X represents the version of the generic zip file) link on the Software Download site along with the 2012.2 Linux build to the NSM appliance either for CentOS 4.X or CentOS 5.7 platform.

- Extract the appropriate latest service release Linux build of 2012.2 using the command **unzip <Name_of_the_Linux_build_of_service_Release.zip>** in the NSM appliance.
- Start the installation in online or offline mode using the command **sh upgrade-os.sh<Name_of_the_Linux_build_of_service_Release.sh>Offline/Online**.

NOTE: For the successful upgrade of the system packages, make sure that the **nsm_generic_offline_upgrade_CentOS5.x.zip** file or the **nsm_generic_offline_upgrade_CentOS4.x.zip** file is present in the same directory where the **upgrade-os.sh** script is available.

You can choose Online or Offline mode of installation by specifying either offline or online as the last parameter in the command.

To know more about offline and online installations see, *NSM Installation Guide*.

Upgrade Considerations

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

Upgrading NSM on Linux/Solaris

You can upgrade to NSM 2012.2 from the following versions:

- 2012.1x
- 2011.4x
- 2010.3r2
- 2010.3s service release 1 onwards

NSM 2012.2 supports:

- 2500 low-end devices with 10 user connections; each device is loaded with configuration of size 57 KB.
- 300 high-end devices with 25 user connections; each device is loaded with configuration of size 1 MB.
- 100 high-end devices with 10 user connections; each device is loaded with configuration of size 4 MB.

NOTE: The system update packages published along with 2012.2 must be installed prior to the upgrade.

Upgrading NSM Appliance

Table 8 on page 17 summarizes the scenarios for upgrading NSM Appliance to 2012.2 version:

Table 8: NSM Appliance Upgrade Scenarios

NSM Appliance Version	CentOS Version	CentOS Version required after Upgrade	Procedure for Upgrading to 2012.2
2012.1x / 2011.4x / 2010.3R2 / 2010.3s1-s15	5.7	5.7	Upgrade using CentOS 5.7 packages provided on 2012.2 release web page.
2012.1x / 2011.4x / 2010.3R2 / 2010.3s1-s15	4.x	5.7	1. Upgrade to CentOS 5.7 using the CentOS 5.7 ISO available for the current release (2012.1x / 2011.4x / 2010.3s1-s15). 2. Upgrade to 2012.2 using NSM Appliance Upgrade CentOS 5.7 packages provided on the 2012.2 release web page.
2012.1x / 2011.4x / 2010.3R2 / 2010.3s1-s15	4.x	4.x	Upgrade using CentOS 4.x packages provided on 2012.2 release web page.
Versions prior to 2010.3s	4.x	4.x	1. Upgrade to 2010.3s or 2011.4 or 2012.1 from the current version. 2. Upgrade to 2012.2 from using CentOS 4.x packages provided on 2012.2 release web page.
Versions prior to 2010.3s	4.x	5.7	1. Upgrade to 2010.3s or 2011.4 or 2012.1 from the current version. 2. Upgrade to CentOS 5.7 using the CentOS 5.7 ISO available in 2010.3s. 3. Perform upgrade to 2012.2 using **NSM Appliance Upgrade CentOS 5.7** packages provided in 2012.2 web page.

Deprecated Operating System

NSM no longer supports ScreenOS version 4.X. You must upgrade your devices to ScreenOS version 5.0 or later. NSM no longer supports Junos OS Release 9.2 or earlier.

Vulnerabilities Addressed After NSMXpress OS Upgrade

The full list of Common Vulnerabilities and Exposures (CVEs) addressed for the Red Hat Enterprise Linux 5 server can be found at Red Hat Customer Portal.

NOTE: **These CVEs are addressed on NSMXpress appliance by upgrading the CentOS version to 5.7.**

The updated NSMXpress appliance operating system addresses the CVEs for the packages are listed in Table 9 on page 18. Details on individual CVEs fixed by Red Hat Linux in 5.x releases can be found at National Vulnerability Database.

Table 9: CVEs for NSM Packages

Packages	Addressed CVEs
NSM 2012.2 Release	
httpd-2.2.3-65.nsmx5.3	CVE-2011-3192, CVE-2011-3368, CVE-2012-0031, CVE-2011-4317, CVE-2012-0053 and CVE-2011-3607
openssh-5.8p1-1.i386.rpm	CVE-2011-3192, CVE-2008-5161 , CVE-2011-0539, CVE-2010-4478, CVE-2010-4755, CVE-2009-2904, and CVE-2008-3259
NSM 2012.1 Release	
acpid-1.0.4-9.el5_4.2	CVE-2009-0798; CVE-2009-4033
apr-1.2.7-11.el5_6.5	CVE-2009-2412; CVE-2011-0419
apr-util-1.2.7-11.el5_5.2	CVE-2009-0023; CVE-2009-1955; CVE-2009-1956; CVE-2010-1623
authconfig-5.3.21-7.el5	CVE-2006-2453; CVE-2006-2480
basesystem-8.0-5.1.1.el5.centos	CVE-2007-3996; CVE-2008-5374
bash-3.2-32.el5	CVE-2007-2926
bind-libs-9.3.6-16.P1.el5	CVE-2011-2464
binutils-2.17.50.0.6-14.el5	CVE-2010-0405
cpio-2.6-23.el5_4.1	CVE-2005-4268
curl-7.15.5-9.el5_6.3	CVE-2009-2417; CVE-2011-2192
dbus-1.1.2-15.el5_6	CVE-2010-4352
glib2-2.12.3-4.el5_3.1	CVE-2008-4316; CVE-2008-4316; CVE-2011-0536; CVE-2010-0296; CVE-2011-1071; CVE-2011-1095
glibc-2.5-65	CVE-2009-5029; CVE-2009-5064; CVE-2010-0830; CVE-2011-1089; CVE-2011-4609
kernel-PAE-2.6.18-274.el5	CVE-2011-1898; CVE-2011-3363; CVE-2011-4110; CVE-2011-1162; CVE-2011-2203; CVE-2011-2494; CVE-2011-2484; CVE-2011-2695; CVE-2011-2723; CVE-2011-3191; CVE-2011-3347
krb5-libs-1.6.1-62.el5	CVE-2009-0844; CVE-2009-0845; CVE-2009-0846; CVE-2011-0282; CVE-2011-0281
libpng-1.2.7-3.nsmx13.0	CVE-2008-1382; CVE-2009-0040
libuser-0.54.7-2.1.el5_5.2	CVE-2011-0002

Table 9: CVEs for NSM Packages *(continued)*

Packages	Addressed CVEs
libxml2-2.6.26-2.1.12	CVE-2007-6284; CVE-2009-2414; CVE-2009-2416; CVE-2010-4008; CVE-2011-1944; CVE-2011-2834; CVE-2011-3905; CVE-2011-3919
mailcap-2.1.23-1.fc6	CVE-2011-0707; CVE-2008-0564; CVE-2010-3089
nspr-4.8.6-1.el5_5	CVE-2009-2404
nss-3.12.8-4.el5_6	CVE-2009-2408; CVE-2009-2409
openldap-2.3.43-12.el5_6.7	CVE-2011-1024
openssl-0.9.8e-20.el5	CVE-2009-1377; CVE-2009-1378; CVE-2009-1379; CVE-2009-1386; CVE-2009-1387; CVE-2009-0590
pango-1.14.9-8.el5.centos.2	CVE-2009-1194; CVE-2011-0020
postgresql-8.1.23-1.el5_6.1	CVE-2007-0555; CVE-2006-5540; CVE-2010-4015
postgresql-devel-8.1.23-1.el5_6.1	CVE-2006-5540; CVE-2006-5541; CVE-2006-5542; CVE-2007-0556
python-2.4.3-44.el5	CVE-2007-2052; CVE-2007-4965; CVE-2008-1721; CVE-2008-1887; CVE-2008-2315; CVE-2008-3142; CVE-2008-3143; CVE-2008-3144; CVE-2008-4864; CVE-2008-5031; CVE-2009-3720; CVE-2010-3493; CVE-2011-1015; CVE-2011-1521

Deprecated Support

- Beginning in NSM 2012.2R8, bundled schema versions (schema version 295 or later) do not include support for the following versions of Junos OS devices (J Series, SRX Series, EX Series, M Series, and MX Series):
  - 9.3R1, 9.3R2, 9.3R3, 9.3R4
  - 10.1R1.8, 10.1R2.8, 10.1R3, 10.1R4.4
  - 10.2R2.11, 10.2R4.8
  - 10.3R1.9, 10.3R2.11, 10.3R3.7, 10.3R4.4
  - 11.1R1.14, 11.1R2.3, 11.1R3.5, 11.1R4.4, 11.1R6.4

  NOTE:
  - The NSM-supported OS versions for SA and IC devices are 6.3R7 or later and, 2.2R5 or later, respectively.

- NSM 2012.2R8 is the last service release that includes the Solaris build.

Limitations

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

- Junos OS Release 10.4 support is deprecated on NSM schema versions 336 and later. When the NSM schema is upgraded to 336 or later, the configuration status of SRX Series and J Series devices running Junos OS Release 10.4 is displayed as "Down," and these devices cannot be managed by NSM. The NSM 2012.2R13a release default schema version is 341; for this reason, when the NSM server is upgraded to the NSM 2012.2R13a version, NSM can no longer manage existing devices running Junos OS Release 10.4. Before upgrading the NSM server to the NSM 2012.2R13a version, users should upgrade devices running Junos OS Release 10.4 to later versions of Junos OS Releases.
- Version v4 of CentOS 5.7 generic ZIP files is the last version that supports CentOS version 5.7.
- NSM does not support the Junos OS Release 15.1X49 or later schema for SRX Series devices.
- Beginning with the NSM 2012.2R12 release, the Central Manager build will be available on request. For more information, contact JTAC.
- In NSM, IPv6 addresses must be configured only in lowercase for interfaces in SRX Series devices. This is because NSM displays a delta configuration when an IPv6 address is configured in uppercase.
- Central Manager will not have IPv6 management address support.
- The following characters are not supported for NSM administrator names and passwords:
  - Period (.)
  - Number sign (#)
  - Dollar sign ($)
  - Asterisk (*)
  - Ampersand (&)
  - Circumflex (^)
  - Pipe symbol (|)
  - Double-quote (")
- Version v2 of CentOS 4.x generic ZIP files is the last version that supports CentOS version 4.x.
- NSM only supports Junos OS FIPS release 10.4R4 and earlier versions.
- Because of schema size issues, the NSM 2012.2R7 Solaris build is bundled with schema version 283. For Junos OS 12.1X46 support in the 2012.2R7 Solaris build, update schema to the latest version.

- When the installed schema version in the Solaris server is different from the schema version of the client, it may take about 30-40 minutes to establish the initial connection from client to the server. This is because the client downloads the schema packages from the server. This is a one-time limitation and the subsequent attempts for connection will be faster.

  Workaround: Follow the steps given below to reduce the delay in the initial connection:

  - Log in to Solaris server and run the following commands:

    cd /var/netscreen/GuiSvr/be/schemas/

    zip -r /var/tmp/nsm_schemas.zip dmi dmi-nsm CurrentSchemaVersion.txt

    chown nsm /var/tmp/nsm_schemas.zip

  - Connect the client to the server. The connection will be faster now.

  

  NOTE: **Follow this workaround only while connecting the client for the first time after installation. Subsequently, the client connection will be successful even without this workaround. For more information, refer to PR 929140 listed under** "NSM" on page 56 **in the section.**

- After upgrading from any previous version to NSM2012.1s1 and above, perform the NSM attack DB followed by the attack DB on the device. This is due to the change that has been introduced in the way NSM stores attack DB files.
- In NSM, if devSvrTFTP process is displayed as **off** after upgrading to the latest NSM version, the user is recommended to kill the tftp process that uses port 69 in Linux server manually, so that java tftp process of NSM can use the same port. After doing this, devSvrTFTP process may be restarted by the user. This devSvrTFTP process is used only for the NSM feature **config file management** in ScreenOS devices.
- On an NSM appliance, the recovery partition cannot be upgraded using the web interface of the appliance after the OS has been upgraded to CentOS 5.7. To upgrade the recovery partition using the CLI feature, see **Update Recovery Partition to a Factory Restore Version with CentOS 5.7** in the *CentOS Upgrade guide*.
- NSM does not support Junos OS downgrades. However, if you need to downgrade a device, follow these steps:

  1. From the device, use the CLI command to downgrade the image. For example:

     root> request system software add <package-name> reboot.

  2. After the downgrade, from NSM, delete the device and then add it again.

- For Junos OS J Series and EX Series devices—NSM Configuration Editor cannot completely validate the configuration that an NSM user has created before sending it to the device. The device validates the configuration when the configuration is pushed to the device as part of the Update Device job and may return validation errors to NSM.

- For SSL VPN SA and Infranet Controllers—Secure Virtual Workspace (SVW) settings on the SA device cannot be managed with NSM.
- For EX Series switches—EX Series switches running Junos OS do not support snapshots. Therefore, users should not select the "Backup the current filesystem(s) on the device" check box in the final page of the Install Device Software wizard.
- In the SA template, the network connection default value in the user role is not validated to its correct default value by NSM.

Important SSL VPN and Infranet Controller Instructions

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

NSM Server

- There is no limit to the number of devices that can be simultaneously updated in NSM, provided the configuration size on each device being updated is less than 5 MB. NSM can execute updates in parallel across a maximum of eight devices while the remaining update jobs are queued up.
- If the software version of SA/IC configurations exceeds 5 MB, we recommend a maximum of four devices per job for an appropriately sized Linux or Solaris server running NSM.
- Due to hardware limitations on NSMXpress, the recommended limit is two devices per job for SA/ICs running configurations more than 5 MB.
- The following files on the NSM software server must be edited as described below (no changes are needed for NSMXpress):
  - In **/usr/netscreen/GuiSvr/bin/.guiSvrDirectiveHandler**, change **Xmx10248000000** to **Xmx2048000000**:

    $LIB_DIR/jre/bin/java -DNSROOT=$NSROOT -DgproGDM=$DEST_DIR -DNSDIR=$DEST_DIR/var/be -DSTART_PATH=$DEST_DIR -DBE_CFG=${CFG_FILE} -DLOG4J_CFG=${LOG4J_CFG_FILE} -XX:PermSize=64M -XX:MaxPermSize=64M -Xms128000000 - Xmx2048000000 com.netscreen.devicecomm.GUIDirectiveManager -version -repo ${REPO_DEST_DIR} -conf ${SVC_CFG_FILE}
  - In **/usr/netscreen/GuiSvr/var/xdb/data/DB_CONFIG**, change the **set_cachesize** parameter from **0 256000000 1** to **0 1024000000 4**.

    NOTE: **Do not comment out the line /usr/netscreen/GuiSvr/var/xdb/data/DB_CONFIG in the configuration file; instead edit the existing path to avoid upgrade issues.**
  - Set the shared memory to a minimum of 1 GB (**kernel.shmmax = 1073741824**):
    - In **/etc/sysctl.conf**, for Linux systems

- In **/etc/system**, for Solaris systems

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

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

- In **/usr/netscreen/DevSvr/bin/.devSvrDirectiveHandler**, change **Xmx1024000000** to **Xmx2048000000**:

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

The servers 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:

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 1d.
   d. Click **OK**.
   e. Repeat Step 3b through Step 3d for all of the Infranet Enforcers.
   f. On the **Infranet Controller, select UAC > Infranet Enforcer > Connection** and check that all the Infranet Enforcers have been added.
4. On NSM, delete the Infranet Enforcer firewalls from the global domain:
   a. In the global domain, select **Device Manager > Devices** to list all the devices.
   b. Right-click each Infranet Enforcer firewall device and select **Delete** from the list.
5. On NSM, delete the $infranet instances from the Object Manager:
   a. Select **Object Manager > Authentication Servers**.
   b. Right-click each $infranet_n object and select **Delete** from the list.
   c. Select **VPN Manager > VPNs**, and check that you do not have any $infranet objects under VPN Manager. These objects are usually deleted automatically when you remove the firewall.
6. Create a new subdomain for the Infranet Enforcers:
   a. Select **Tools > Manage Administrators and Domains**.
   b. Select the **Subdomains** tab.
   c. Click the Add icon.
   d. In the New Subdomain dialog box, enter an appropriate name for the subdomain so you know what it will be used for, and then click **OK**.

e. From the drop-down list at the top left side, select your new domain. The new domain is empty, but it can use objects from the global domain. If you do not remove the $infranet instances from the main domain, you risk having duplicate $infranet names. In addition, add a Single Infranet Enforcer or Infranet Enforcer Cluster.

f. Repeat Step 5 and Step 6 for every Infranet Enforcer or Infranet Enforcer Cluster you need to add to NSM. When finished, you should see $infranet instead of $infranet_# in each of the domains except global.

7. In NSM, add the Infranet Enforcer objects to the new domain:

   a. Select **Device Manager > Devices**.

   b. Click the Add icon, and then select **Device** to start the Add Device Wizard.

   c. In the New Device window, provide a name for the device, a color for its icon in NSM, and check **Device is Reachable**.

   d. Follow the instructions in the wizard to add and import the device.

   e. Repeat Step 7b through 7d for each Infranet Enforcer device.

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

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

Usage Guidelines for Applying NSM Templates to SA and IC Clusters

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

Recommended

- Templates that are applied to cluster objects should only include CG data. Templates that are applied to cluster member objects should only include NS/NL data. These guidelines apply to templates that are created from scratch or through promotion.

- To replicate the configuration from one cluster (source) to another cluster (target) through templates, promote the configuration from the source cluster object to a cluster template, and then apply that template to the target cluster object.
- To replicate the configuration from one cluster member (source) to another cluster member (target), promote the configuration from the source cluster member object to a member template, and then apply that template to the target cluster member object.

Not Recommended

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

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

Node-Specific (NS) Configuration:

<nsm:path>/ive-sa:configuration/system/log/snmp</nsm:path>
<nsm:path>/ive-sa:configuration/system/log/events-log-settin gs/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-logsettings/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-port</nsm:path>
<nsm:path>/ive-sa:configuration/system/network/vlans</nsm:path>
<nsm:path>/ive-sa:configuration/system/network/network-hosts</nsm:path>
<nsm:path>/ive-sa:configuration/system/network
/network-connect/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/network-connect-policies/
network-connect-node-specific-configuration</nsm:path>
<nsm:path>/ive-sa:configuration/authentication/auth-servers/collection-of-auth-server/
union-of-ace/active-directory-winnt/
settings/advanced/computer-names/ive-name</nsm:path>

Node-Local (NL) Configuration:

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

/ive-sa:configuration/system/configuration/dmi-agent/deviceid
/ive-sa:configuration/system/configuration/dmi-agent/hmac-key
/ive-sa:configuration/system/maintenance/push-config/acceptpush

Best Practices

This section contains information about recommended practices when using NSM.

Maintaining the NSM GUI Server

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

On the NSM GUI client:

- Delete old entries from the Job Manager in each domain.
- Purge old database versions using **Tool > Database Versions**.

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

NOTE: **Beginning in NSM 2012.2, NSM supports automatic purging of database versions at configured intervals. When saved database files exceed the maximum threshold, only the configured minimum database version is retained.**

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

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

To create a self-signed certificate between an NSM server and an NSM client:

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

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

   #unzip createCerts.zip

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

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

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

NOTE: The script produces a certificate with a timestamp that is nearly 10 years beyond the current date.

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

```
root@nsm/]# sh createCerts.sh
Enter NSM installation path[/usr/netscreen]>
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Using configuration from cfg/openssl.cfg
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'State'
localityName :PRINTABLE:'City'
organizationName :PRINTABLE:'Name of the Organization'
commonName :PRINTABLE:'NSM'
emailAddress :IA5STRING:'user@example.com'
Certificate is to be certified until Aug 3 22:41:04 2019 GMT (3650 days)
Write out database with 1 new entries
Addressed Issues
Data Base Updated
Using configuration from cfg/openssl.cfg
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'State'
localityName :PRINTABLE:'City'
organizationName :PRINTABLE:'Name of the Organization'
commonName :PRINTABLE:'NSM'
emailAddress :IA5STRING:'user@example.com'
Certificate is to be certified until Aug 3 22:41:04 2019 GMT (3650 days)
Write out database with 1 new entries
Data Base Updated
Certificate was added to keystore
Certificate was added to keystore
[root@nsm/]#
```

This step creates four files: **root.pem**, **server.pem**, **truststore.ts**, and **keystore.ts**.

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

5. On the NSM GUI server, copy the files **root.pem** and **server.pem** to **/usr/netscreen/GuiSvr/var/certDB/TrustedCA/**.

6. On the NSM client, copy the file **trustedtore.ts** and **keystore.ts** to **NSM_GUI_INSTALLATION/security** directory. (The default directory is **C:\Program Files\Network & Security manager\security**.) Note that this must be executed on all systems where the client is installed.

7. Restart NSM GUI server services for a new certificate to be used: **#/etc/init.d/guiSvr restart**

   If using a high availability environment, execute: **#/etc/init.d/haSvr restart.**

Performance of NSM 2012.2

In 2012.2 release, due to memory optimizations and PR fixes, many policy operations and device operations are seeing performance gains. A few operations are seeing slight performance reductions. This is an expected behavior.

Configuration of clients used for testing:

1. **Windows XP Client:**
   - Processor: Intel ® Core ™ 2 Duo CPU E8400, 3.00 GHz
   - RAM: 2 GB
2. **Windows 7 Client:**
   - Processor: Core 2 duo CPU, E8400, 3.00 GHz
   - RAM: 3 GB

Configuration of Server:

- Processor: Intel(R) Xeon(R) CPU E5630, 2.53GHz
- RAM: 4 GB
- Linux: Red Hat Enterprise Linux ES release 4 (Nahant Update 6)

Configuration of Devices:

The contents of configuration for small configuration of size 1 MB is described as below:

Table 10: Small Configuration of Size 1MB

Category	Number
Address Objects	76
Address Group	3
Firewall Rules	51
Source NAT Rule Set	1
Destination NAT Rule Set	1
Custom Service Objects	50
Custom Service Group	3

The contents of configuration for large configuration of size 2 MB is described as below:

Table 11: Large Configuration of Size 2MB

Category	Number
Address Objects	3008
Address Group	54
Firewall Rules	3088
Source NAT Rule Set	42
Destination NAT Rule Set	65
Custom Service Objects	139
Custom Service Group	5

The performance values measured for some sample operations are described as in Table 12 on page 30.

Table 12: Performance Values

Action	Time taken (in seconds) in 2012.2					
	Large DB		**Medium Size DB**		**Small DB**	
	Windows 7 client	Windows XP client	Windows 7 client	Windows XP client	Windows 7 client	Windows XP client
Initial Login	54	60	104	104	108	90

Table 12: Performance Values *(continued)*

Action	Time taken (in seconds) in 2012.2					
Subsequent Login	50	47	100	76	103	87
In Object Manager						
Open Address Objects in the Object Manager (first time loading)	1	1	2	2	1	1
Open group object	1	1	2	9	1	1
Cancel out of group	1	1	1	1	1	1
Open host object	1	1	1	1	1	1
Cancel out of host	1	1	1	1	1	1
Create individual host	3	3	2	3	3	2
Delete object	2	2	2	2	7	2
Replacing Address Object	1	1	1	1	2	2
Service Objects						
Open Custom Service Objects (initial open only)	1	1	1	1	1	1
Open service group object	1	1	1	1	1	1
Cancel out of service group object	1	1	1	1	1	1
Open service object	1	1	1	1	1	1
Cancel out of service object	3	3	2	2	3	3
Search for service object	1	1	1	1	1	1
In Policy Manager						

Table 12: Performance Values *(continued)*

Action	Time taken (in seconds) in 2012.2					
Open FW Policy (initial open only)	1	1	1	1	1	1
Open individual FW policy (3088 rules)	55	45	58	47	65	46
Open individual FW policy (85-400 rules)	7 (100 rules)	6 (100 rules)	11 (100 rules)	9 (100 rules)	7(100 rules)	6(100 rules)
Open address group used in rule	1	1	1	5	2	1
Editing comments field	3	3	2	3	3	2
Saving FW policy (~3000 rules)	9	9	9	8	9	9
Saving FW policy (~85 - 400 rules)	6 (100 rules)	5(100 rules)	5 (100 rules)	4 (100 rules)	5(100 rules)	4 (100 rules)
In Device Manager						
Import Device (2 MB Config Device)	226	235	160	160	111	150
Edit Device (2 MB config Device)	9	9	7	8	7	8
Delete Device (2 MB config Device)	47	45	48	35	54	79
Summarize Delta Config (2 MB config Device)	81	82	50	55	52	58
Update device (2 MB config device, 1 rule add/delete)	129	125	80	97	80	80
Opening a policy with 5 rules	5	4	6	7	5	4
Import Device (1 MB config Device)	730	740	565	582	590	590

Table 12: Performance Values *(continued)*

Action	Time taken (in seconds) in 2012.2					
Delta Device (1 MB config Device)	150	147	133	125	140	140
Update Device (1 MB config Device)	310	290	260	160	285	310
Open a policy without source NAT rules (270 rules)	6	6	12	12	-	-
Summarize delta config and update device (2MB config)	150	147	135	129	88	110

NOTE: Many variables can affect performance. The above averages were observed in Juniper Networks QA labs.

Addressed Issues

This section includes issues addressed for NSM, ScreenOS, SA Series SSL VPN Appliances, IC Series UAC Appliances, and SRX Series Services Gateways. 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.

Release 2012.2R14 Patch

- 1202528 - Delta configuration summary does not show that the **vlan group** command is unset.
- 1223201 - When you configure the target address, the Management interface is not listed under the source-interface for SNMPv3.
- 1229205 - DevSvr deviceservice process appears in the INFO level logging.
- 1263606 - 2012.2R13: When you try to import or export the database, it removes all policies from the nsmpolicy container.
- 1278693 - guilSvrcli.sh script does not pass some special characters used in the password for guiSvr authentication.
- 1290446 - 2012.2r12 objects and delta has summary issues.
- 1293367 - NSM continues to commit configuration after the SRX Series device configuration merge error occurs.

- 1294077 - SNMPv3 privacy and authentication passwords found in cleartext on ScreenOS.
- 1294563 - When you perform an export or import operation in a customer environment, it removes all addresses from the address container.
- 1282003 - SNMPv3 sha authentication-key encryption is incorrect when you update the SRX Series device.
- 1284764 - When you update the policy from NSM to SRX firewall, it shows the rcp error.
- 1195165 - When you modify the huge address group, some unexpected objects added and removed from the address group.
- 1260378 - NSM lock error is not displayed in Delta.
- 1266137 - Not able to run summarize delta configuration or update the device with 6.2FIPS version after the device is upgraded to NSM-2012.2R12.
- 1298431 - When you right click on the **install-on** column and select the target, the devices in the domain are not listed.
- 1306114 - NSM- 2012.2R13a: When you modify the huge address group, some unexpected objects are added and removed from the address group.
- 1208524 - NSM-2012.2R12: On SRX650 device, after you upgrade from Junos OS Release 12.1X44 to 12.3X48-D30, the destination NAT update fails when referring to a dst-port tag.
- 1299414 - NAT destination port coexists for Junos OS release versions 12.3X48 and 12.1X46.
- 1312210 - When you try to create a view for view definition, the following error message is displayed: **Could not create view for the view def java.lang.StringIndexOutOfBoundsException: String index out of range:2012.2R12**

Release 2012.2R13a Patch

- 1076250 - When the **guiSvr** and **devSvr** processes' memory utilization is high, the NSM update might fail.
- 1108474 - NSM deletes device configurations on SRX Series devices when the CA certificate is updated.
- 1113164 - NSM failed to export the audit log to a CSV file.
- 1127677 - NSM does not allow configuration of IKEv2 gateway parameters for SRX Series devices on VPN Manager.
- 1128203 - NSM update to multiple SRX Series devices fails frequently.
- 1131904 - Export and Import of the NSM database fails when the database size is greater than or equal to 50 GB.
- 1131935 - NSM does not update the **infranet-auth** configuration in a zone-based firewall policy on the NS5400 VSYS device.

- 1137500 - NSM does not support the **junos-icmp6-packet-too-big** service object on the Object Manager.
- 1147299 - NSM sends logs to the syslog server with the source IP address as 0.0.0.0 instead of the actual source IP address.
- 1163729 - NSM displays a delta configuration for the **unset service objects timeout** values on ScreenOS VSYS devices.
- 1165701 - On ScreenOS devices, when the **Delta and Update** operation is performed, the **Update Firewall Configuration Only** checkbox is unselected in **Tools -> Preferences -> Device Update -> Screen OS and IDP**.
- 1168018 - NSM allows dragging and dropping a cluster or VSYS member to another cluster or VSYS memer.
- 1168755 - When a time filter is configured, NSM fails to export **audit-log** files.
- 1170185 - NSM does not allow a device group to be deleted when **Load Screen OS Device Schema Only** schema is selected.
- 1172081 - When the user creates a policy rule on **Global firewall for JUNOS** without a policy name, the delta configuration does not display a warning of an overlapping rule. NSM deletes the user-created policy rule by automatically generating the new policy rule, parameters, and policy name.
- 1172089 - NSM displays the error message **unable to fetch the date for requested object** when audit log for the **Global firewall for JUNOS** rule base is edited.
- 1173561 - The **guiSvrManager** process generates a core file when the Standalone IDP cluster device is added to NSM.
- 1174740 - When the NSM server does not have the **xvfb** package, the **LogbasedReport** generation fails.
- 1175674 - NSM sends the **unset vlan group fnfg-s vsd-group** configuration at the next update of the VSYS device when the ScreenOS device runs in transparent mode.
- 1181533 - Radius authentication might not t work on NSM when the IPv6 address family is not supported on the NSM server.
- 1184473 - NSM unsets the **nsrp** secondary-path configuration on next update when the ScreenOS Cluster device **Name** is modified.
- 1194052 - NSM does not display address and service objects properly on zone-based firewall policies when more than 14 objects are added and Font Size is set to +3 in **Tools -> Preferences**.
- 1184119 - NSM supports the **SRX550** device.

Release 2012.2R12 Patch

- 1136564 - NSM failed to update the services offloading configuration on the SRX5400 device.
- 913382 - NSM does not provide the option to configure a source interface for SNMPv3 on ScreenOS devices.

- 1046303 - For standalone IDP devices, NSM does not allow you to change the value of the "Maximum length for NTPv3 and NTPv4" message from 72 to 120, the latest value.
- 1066016 - NSM might not update the access-profile configurations on SRX series devices.
- 1071188 - NSM report generation fails for a very large number of logs.
- 1071339 - When a service object that is replaced in the global domain is also referenced in the subdomains, NSM does not replace the service object in the subdomains. NSM replaces the service object only in the global domain.
- 1073164 - When both the interfaces eth0 and eth1 are configured with IP addresses, an NSM upgrade from release 2010.3S15 to 2012.2R10 fails.
- 1074134 - When an extranet device is added to the VPN manager, NSM might not change the config status of devices added under the VPN.
- 1078148 - NSM does not allow you to configure "none" in the "Maximum no. of group members" field under **Preference->Custom Validations**.
- 1082591 - NSM does not allow you to delete a description of an address-group object for an SRX Series
- 1085731 - When multiple groups are created for all policy rules and saved, NSM fails to display any policy rules under rule-groups in the NSM UI.
- 1088308 - When the "Valid Life Time" and "Preferred Life Time" values are configured under **Interface -> IPv6 -> Prefix List** on an ISG2000 device, the NSM update fails.
- 1097956 -NSM fails over to the secondary server when the disk-space computation encounters an error, such as failure to retrieve partition information **/usr/netscreen/GuiSvr/var**.
- 1100301 - When you update a policy without making any changes and then perform a storage manager cleanup operation, NSM does not forward syslog messages to the external syslog server. This issue applies only to rule-based log actions.
- 1106182 - NSM does not allow you to configure the **set di service http brute_search 32** option for an ISG1000 device.
- 1107669 - The "java null pointer exception" error message is displayed occasionally when a summarize delta config operation is performed on SRX Series devices in NSM.
- 1124254 - When the **CA Hash** value is configured under **Auth -> InfraneT**, the NSM upgrade fails for ScreenOS devices.
- 1128700 - SRX Series device hostnames are not parsed appropriately in logs by NSM.
- 1125256 - When the first rule in a rule base is configured with a higher number of objects than the other rules, NSM displays the first rule's row size for all rules in the Global Firewall for JUNOS rule base.

Release 2012.2R11 Patch

NOTE: NSM 2012.2R11 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see http://www.juniper.net/support/eol/nsm.html.

- 866236 - NSM did not provide the option to configure the DNS timeout value in seconds.

  NOTE: Configure the DNS timeout value in seconds in the Unit drop-down list under **Object Manager** > **Service Objects** > **Custom Service Objects**.

- 918919 - NSM did not prompt for the interface IP address after upgrading the CentOS version to 5.7 when the appliance was running only the DevSvr process.

  NOTE: The fix is available after CentOS is upgraded to version 6.5.

- 964962 - The NSM client took a long time to log in the first time when multiple cluster devices were being managed.
- 1006028 - VPN Manager assigned rule IDs that were already in use by firewall policies to policy-based VPN rules.
- 1010680 - The **Apply value** option did not function for selected rules under **Zone based policies** > **Rule groups**.
- 1011850 - NSM guiSvrManager memory increased when deleting bulk jobs from Job Manager.
- 1026477 - NSM displayed a blank page on the second attempt to view the policy distribution table under **Investigate** > **Realtime Monitor** > **Device Monitor** > right click on a device > **view statistics** > **Traffic**.
- 1028428 - After migrating to NSM 2012.2R11, any VPN configuration changes saved in VPN Manager cause the existing proxy identity configuration to update from 0.0.0.0/32 to 0.0.0.0/0.

  NOTE: NSM does not display proxy ID changes in the delta config window after a successful update.

- 1030576 - NSM displayed a validation error under **Event Options** > **Policy** > *Policy name* > **Policy** > **Then** > **Event Script** > **Execute commands** > **Destination**.
- 1031157 - NSM guiSvrManager crashed and generated a core file when a directive operation was running for multiple devices.
- 1032210 - NSM updates failed when the preshared key contained “tftp” in the combination of letters.

- 1034178 - NSM did not allow the management IP addresses of cluster VSYS members to be edited.
- 1035386 - When any redundant interface was deleted from a ScreenOS device, NSM deleted the syslog source interface configuration, if the source interface was also a redundant interface.
- 1043835 - NSM displayed an "The Address Specified for Secondary IP is already in use" error when configuring the secondary IP address for a subinterface in a VSYS cluster.
- 1047754 - NSM took a long time to create a source NAT rule set with a routing instance for SRX Series devices.
- 1049135 - NSM did not allow an interface name to be entered under **Routing Instances** > **Forwarding Options** > **DHCP Relay** > **Group** > **Interface** and returned a "Reference to undefined collection-of-interface" validation error when a similar configuration was imported from SRX Series devices.
- 1050060 - NSM failed to import the description value of custom application objects in SRX Series devices.
- 1052375 - While an address group object was being edited, NSM displayed its parent group object in the non-member list.
- 1052597 - NSM failed to display the hmac-sha-256-128 algorithm for the Authentication Header (AH) protocol under the **Authentication algorithm** menu.
- 1053970 - The local backup failed in an HA cluster when it was triggered while the delta config and update device directives were running.
- 1060800, 1042815, 1052026, 1061262, 1056593, 1045789 - NSM replaced existing policy rules with default rules when a delta config or an update device directive was running.

  NOTE: This error was not repeated in successive attempts.

- 1061199 - RADIUS authentication failed because NSM did not send the NAS IP attribute in the request to the RADIUS server.
- 1065249 - NSM failed to perform an attackdb update for version 2467.
- 1067344 - The XDB Orphan Tool failed to display a few orphan objects in the NSM database, when the appliance was running the **/usr/netscreen/GuiSvr/utils/.xdbOrphanRuleTool.sh -l** command.
- 1072175 - When performing a Summarize Delta Config operation for multiple devices, the operation failed for a few devices in SRX Series devices with Junos OS version 12.1X47-D10.

Release 2012.2R10 Patch

NOTE: NSM 2012.2R10 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see http://www.juniper.net/support/eol/nsm.html.

- 813958 – In the log viewer filter, NSM did not recognize the specified end date and therefore interpreted the start date as the end date when displaying results.
- 986347 – Device status was displayed as down on the NSM GUI after reboot.
- 989801 – NSM tried to delete the RADIUS server configuration under **Access Profiles** for the SRX240H2 cluster.
- 995546 – NSM did not support special characters in the one-time password during the upgrade.
- 997285 – Editing polymorphic objects took longer time for multiple edits.
- 999007 – Unable to create IKE gateways for the Auth server with external authentication.
- 999016 – NSM failed to copy a set of objects from one rule to another within a policy.
- 1004747 – NSM displayed the following error when SRX Series devices were opened under Config group list>Junos-defaults>Applications>Application for editing:

  invalid enum value
- 1005381 – NSM failed to update SRX Series devices when routing options with the as-path aggregator configuration were applied to the SRX firewall.
- 1006280 – NSM deleted the certificates on ISG Series devices after creating a VSYS from NSM.
- 1006786 – NSM failed to display tunnel information under *Policy based VPN*>Overrides>Policy Rules>Action.
- 1009620 – NSM failed to import the firewall rulebase from the database.
- 1019759 – NSM failed to display several jobs in Job Manager on the NSM GUI.
- 1020965 – NSM upgrade failed when the SELINUX option was set to "Enforcing".
- 1021921 – The firewall policy was deleted automatically after the updated configuration was applied to the firewall.
- 1022314 – IDP short names were unavailable in the system log.
- 1022923 – NSM does not allow interface values to be entered under **system-services-Dhcp Local Server-Group-Interface** for the Junos OS 12.1 release.

  Workaround: The fix is available in the schema version 307 or later.
- 1023418 – The output of the summarized delta config showed a mismatch in the preshared key for ScreenOS devices after an upgrade to the latest NSM version.

- 1028254 - NSM displayed the following error while launching the NSM client after an upgrade to 2012.2R9:

  Could not create Java Virtual Machine

- 1030257 – NSM does not have the option to add **et physical interface** to SRX Series devices.
- 1033290 - The DevSvr LogWalker process crashed every 10 minutes after an upgrade of NSM from 2012.2R5 to 2012.2R9.
- 1034846 - The DevSvr LogWalker process displayed the status as Off after an upgrade to 2012.2R9.
- 1035940 - The pop-ups displayed in the NSM GUI during device installation did not allow access to access other applications.
- 1037532 - Users required administrative permissions to download the latest schema version into NSM client after a schema upgrade in NSM.
- 1038162 - NSM displayed the following error while performing a device update:

  Failed to get the connection state from the device - Object not found

Release 2012.2R9 Patch

NOTE: **NSM 2012.2R9 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see** http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R9:

- 789226 - NSM did not allow an admin user to execute the permitted custom-role-based operations.
- 877083 - NSM did not allow the deletion of ScreenOS clusters.
- 895420 - In NSM, the configured password functioned correctly in a template but did not function correctly when pushed to SRX Series devices.
- 920274 - NSM did not have the latest version of Java.
- 945152 - NSM displayed duplicate policy ID warnings under **Policies** in the GUI.
- 955901 - RMA activate did not function when an IDP Series device was added to NSM in unreachable mode.
- 961477 - NSM did not provide the option to collapse/expand address group objects under **Object Manager**.
- 965645 - NSM deleted an IDP policy from an ISG-IDP device when a chained operation (summarize delta and update) was performed.
- 967959 - Even when another color was chosen during the creation of an administrator account, NSM displayed the administrator icon in grey (dimmed).

- 969827 - NSM did not allow the creation of multiple IKE gateways when remote gateways were the same.
- 976507 - NSM did not display a warning/error when more than eight objects were used in a NAT rule.
- 978951 - NSM displayed a delta config summary for the VLAN group in an NS5400 device even after performing an update.
- 983474 - NSM incorrectly displayed a red triangle error under **Config group list** > **Junos-defaults** > **Applications** > **Application** for high-end SRX Series device clusters.
- 983500 - After an SRX Series device was updated, NSM deleted the default value **any** from the from-zone and to-zone options in IDP policies.
- 985763 - NSM deleted VPN rules that had different tunnels but the same source address, destination address, and service.
- 990592 - NSM did not allow the selection of an SRX Series virtual chassis as a device under **Polymorphic Address Object**.
- 994035 - Server monitor calculated and displayed incorrect disk usage details.
- 995575 - The NSM upgrade failed while being upgraded to the latest version with a specific customer DB.
- 997132 - NSM did not provide the option to select an interface under **VLAN** > **Interface** for SRX Series devices.
- 998926 - NSM failed to display the outgoing interface under the BGP neighbor configuration.
- 1001464 - NSM displayed warning messages after updating an ISG-IDP Series device using a chained operation (Delta and update).
- 1001575 - NSM displayed a null point exception when a polymorphic address object in a destination address did not match with the device being updated.

Release 2012.2R8 Patch

NOTE: **NSM 2012.2R8 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see** http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R8:

- 847832 - NSM did not accept space characters while searching for attack objects.
- 860042 - NSM was unsetting BGP neighbor activate commands when a ScreenOS device was upgraded to version 6.3.
- 918747 - Unable to edit or delete the interfaces on VSYS devices in NSM.
- 922932 - In NSM, sorting the **Traffic Policy Distribution Table** under **Realtime Monitor** > **Device Monitor** > **Device Statistics** did not work.

- 924099 - NSM saved a new custom URL category under **UTM** > **Misc** > **URL Category**, even though the category was created with the **URL Filtering** profile.
- 932915 - NSM displayed the following error while editing a few target names in the audit log viewer: **Unable to fetch data for the requested object**.
- 940987 - NSM failed to update an SRX Series device and displayed the following error: **Insertion point not found**.
- 942801 - NSM was unable to send the predefined service **TRACEROUTE-UDP** to ScreenOS devices.
- 947348 - The IPv6 option was not enabled on the modeled VSYS device, although it is enabled on the root device.
- 947617 - Unable to enable the IPv6 option on the modeled VSYS cluster.
- 950257 - NSM did not provide the option to configure the outgoing interface value under **BGP neighbors**.
- 953356 - A failed update of a root ISG device detector displayed the incorrect detector version for the VSYS device.
- 958823 - NSM was unable to edit a subinterface under the VSYS cluster (member level).
- 959007 - NSM did not contain the predefined URL category **Games** under **UTM**.
- 959133 - The **Manage Port Template Association** screen did not display the list of EX Series switches loaded with Junos OS Release 12.
- 961475 - The option to hide the polymorphic object window was unavailable in the NSM GUI.
- 961505 - NSM failed to import SRX Series devices and displayed the following error: **Could not lookup record by name**.
- 963506 - In NSM, devSvrProfilerMgr crashed and generated core files.
- 965014 - When an interface for SRX Series devices was created under **Routing Instance**, NSM did not display the corresponding interface under **Routing Instance** >**System** > **Services** > **dhcp-local-server** > **Group** > **Interface**.
- 967469 - After performing a schema update in NSM, updating an SRX Series device failed because of RPC errors.
- 968737 - The bulk addition of J Series and SRX Series devices in unreachable mode did not generate CLI commands.
- 968988 - In NSM, devSvr crashed and generated core files while adding an ISG1000 device.

Release 2012.2R7 Patch

NOTE: NSM 2012.2R7 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R7:

- 885866 - In NSM, the **set env ipv6 enable** option was greyed out for the members of an ISG Series cluster.
- 895753 - NSM failed to automatically select the secondary source interface when the primary source interface was selected.
- 907769 - NSM displayed an error for IPv6 entries on the ISG Series device interface, even when no errors were present.
- 925209 - NSM did not support new categories of Juniper Networks' enhanced Web filtering functions.
- 925489 - NSM displayed a validation error for the duplicate rule ID in firewall policy rules.
- 927461- In NSM, exporting logs to csv using the **devSvrCli.sh** script did not populate the user column.
- 928859 - In NSM, SRX Series cluster devices were managed using password authentication instead of SSH keys.
- 930923 - NSM failed to display the hold-down time settings field for the SSG140 firewall.
- 932522 - While importing SRX Series devices, NSM changed the Web filtering local profile from **Permit** (the default value) to **Block**.
- 935300 - NSM failed to display the delta config summary even after the management zone for the management interface was changed.
- 936697 - Double-clicking in an address object group performed an add/remove operation.
- 936932 - In the NSM client, the work-in-progress symbol for the back-end process failed intermittently.
- 936936 - NSM took longer than usual time to add an object to an address group.
- 937243 - NSM sent the local IPv6 address to ScreenOS devices when dynamic VPN was configured using VPN Manager.
- 937710 - NSM failed to export the NAT rulebase policy to HTML.
- 939330 - NSM HA experienced a failover because NSM was unable to allocate memory for fragmented traffic.

- 939855 - The NSM database failed to fetch the container data of zone-based firewall rulebase, when the container data size was greater than 100 MB, using an API script.
- 940009 - While performing a Summarize Delta Config, NSM displayed the error **Cannot create device DM** when the **Use policy id in case policy name conflicts** option was enabled.
- 941173 - In NSM, **guiSvrManager** crashed and generated a core file.
- 942100 - After you scheduled the NSM attack database update using scripts, NSM updated the attack database only on a few devices.
- 943436 - For J Series and SRX Series devices, NSM displayed a validation error under **Configuration** > **Security** > **Dynamic VPN** > **Clients**.
- 943780 - After you pasted **any** in either the **Source Address** or the **Destination Address** field of a zone-based firewall policy rule, the field was empty.
- 943802 - The status of the delta config summary in the Job Manager was displayed as **Failed** for secondary SRX Series device when the **Skip Conversion of Shared Objects for Secondary Device** option was enabled.
- 944747 - A previously deleted SRX Series device cluster member reappeared in the GUI, when the user re-logged in to the GUI.
- 945170 - In NSM, VPN Manager did not configure a remote IKE ID for J Series and SRX Series devices.
- 945631 - The SSG5 device could not be updated in NSM while the AV scanner HTTP trickling settings were being configured.
- 946569 - NSM pushed and empty address group as a member of a nested address group to an SRX Series device.
- 946685 - On NS5200 device, the summarize delta operation failed with a Java null point exception after a VPN was modified under **VPN Manager** in NSM.
- 946850 - After upgrading NSM to the latest version, the interface configuration inherited from the template was always displayed in the delta config summary for an SSG Series device.
- 946909 - NSM VPN Manager displayed an error in the GUI when a Pre-Shared Key (PSK) was longer than 43 characters.
- 949889 - NSM did not list the redundant interfaces when the user attempted to create a new subinterface at the cluster level.
- 957190 - The NSM installation script failed to identify the postgresql package installed on a server.

Release 2012.2R6 Patch

NOTE: NSM 2012.2R6 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R6:

- 924999—In NSM, the IP Monitoring Policy Configuration window does not list the logical interfaces.
- 869791—In NSM, IDP policies are removed from the newly imported SRX650 cluster.
- 901898—In NSM, if all the rules in a specific zone direction (for example, trust to untrust) are disabled for a policy assigned to an SRX Series device and the device is updated, the update fails because of an incorrect NSM configuration.
- 907368—In NSM, device update fails for dial-up VPN when you use a RAS user group and an XAuth server that have special characters in the RADIUS secret.
- 915813—In NSM, View Statistics under the Device Manager fails occasionally.
- 920709—In NSM, integrated whitelist and blacklist URL filtering is not permitted without a license.
- 923578—In NSM, the extranet gateway parameters are not sent to the peer device routes.
- 925489—NSM displays warning messages about duplicate rule IDs in firewall policy rules.

  For more details, see "New or Changed Information" on page 12.
- 924205—After upgrading to the latest version of NSM, the admin privileges stored in RADIUS server for remote users fail.
- 927008—In an NSM high-availability setup, NSM self-monitoring alerts are not sent to all administrators.
- 915199—In NSM, template values persist even after the template has been removed.
- 875532—In NSM, the tunnel binding of an ACVPN is unset for ScreenOS cluster devices.
- 928903—In NSM, the DHCP client option does not appear for an interface on the SSG device.
- 932056—In NSM, if an extranet device is used in the VPN Manager, attempts to use a custom Phase 2 proposal with the authentication algorithm SHA2-256 fails.
- 934389—NSM fails to display the category and subcategory fields of logs that are coming from SA and MAG devices in the Log Viewer.

Release 2012.2R5 Patch

NOTE: **NSM 2012.2R5 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see** http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R5:

- 896272—In NSM, the NHTB entries are not displayed after a device is imported.
- 911064—In NSM, the daily backup fails.
- 910278—If there is an NSM HA failover, the devSvrMgr crashes and generates a core file.
- 909902—After updating the detector version in an SRX240H2 firewall from NSM, the device is updated with an incorrect detector version.
- 896929—In NSM, deleting an address object from an address group does not generate any delta configuration.
- 910627—Unable to create a VPN tunnel in NSM if the outgoing interface is configured with IPv4 and IPv6 addresses.
- 860241—NSM provides an option to set **security alg ftp ftps-extension trace options flag all** as inactive, causing device update failure.
- 909321—After NSM is upgraded to the current version, if the signature name is followed by a carriage return or any other interrupt character for log forwarding or exporting of IDP events, then a new syslog entry or a new line is created in a CSV export.
- 907351—In NSM, one routing instance disappears for devices running Junos OS when you click Devices and Topology links for a VPN under VPN Manager.
- 907144—For the current version of NSM, the options Save as and New View under Log viewer do not work.
- 913484—NSM changes the SNMP host original mask to /32 after ScreenOS is upgraded from 6.2 to 6.3.
- 862909—In NSM, the disk and log management fails when very large disk partitions are used.
- 884479—In NSM, the newLogWalker process fails randomly while generating the SNMP traps.
- 912208—In NSM, internal error messages are displayed when double clicking Log/Count is double-clicked in a policy.
- 901897—After updating ScreenOS devices from NSM, the update fails when an attempt is made to unset VIP from NSM.
- 896784—In NSM, the MIP option is not displayed in the management interface of an ISG1000 cluster.
- 894359—NSM fails to change the existing SNMPv3 USM user authentication and privacy passwords.
- 901007—NSM fails to create a custom-url-category for the enhanced feature profile.
- 879489—In NSM, after the deletion of the From Email Address in device_action_criteria, the address is retained in the database.
- 905129—NSM fails to resolve the IPv6 address to a domain name in an address object.
- 914590—NSM sends the CLI command **set pki authority default scep polling-int 15** to the device after ScreenOS version is upgraded from 6.2 to 6.3.

- 888944—NSM fails to send reports while running guiSvrCli.sh.
- 891138—NSM fails to import an SA6500 device.

Release 2012.2R4 Patch

NOTE: **NSM 2012.2R4 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see** http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R4:

- 866736—In NSM, while creating Protected Resource, the default values for Network Object or Service Object is displayed as **any**.
- 900556—In NSM, protocols cannot be configured in source NAT rule set.
- 901704—In NSM, updates to SRX Series device fail if interface port speed and link-mode is changed to none.
- 893446—In NSM, an application error is generated when log icon in the rule is selected.
- 886594—In NSM, importing a device configuration file from ScreenOS cluster fails.
- 888910—NSM reorders prefix list on every update on SRX Series devices.
- 874895—In NSM, using any interface that is not available under DHCP local server displays the following error:**Reference to undefined Collection of Interface.**
- 882342—NSM device update fails when ICMPv6 predefined service on zone-based policy is used.
- 890890—In NSM, unable to select JXM-1SFP interface as source interface.
- 873953—NSM API times out while retrieving address objects from a particular domain.
- 886883—In NSM, importing a device configuration from file for ScreenOS Cluster with cluster id 5 fails.
- 887428—In NSM, when the destination address is set to none, device update fails.
- 855287—In NSM, dragging zone into new rule does not update the new zone.
- 874044—In NSM, device validation fails with the following error: **$deviceobj .*:vsys_profile.sessions.max: Integer value must be between 0 and 500064.**
- 847633—NSM fails to send the appropriate CLI to remove route-filters from JUNOS devices.
- 870465—NSM does not delete the proxy id configuration from the device even after the option is disabled in the VPN Manager.
- 886882—In NSM, the options for chassis information cannot be edited or resized on ISG device cluster.
- 873390—In NSM after taking a daily local back up, start and complete tokens are missing.

- 894936—When NSM is upgraded, the limit for maximum number of client gets changed from 25 to 10.
- 893081—In NSM, ungrouping the copied policy from a rule group creates a duplicate policy entry.
- 891810—In NSM, rules are duplicated when ungrouped.
- 888025—In NSM, the warning message **log session init option is supported from Screenos 5.2 and above** is disabled.
- 883054—In NSM, search string appears in Red color even when the object is found.
- 882045—NSM does not display a warning message for policy name length when the length is greater than 31 characters.
- 882798—NSM device update fails when **Log on Session close** option is disabled and displays the following error message: **GenerateEditConfig Failed.**
- 884175—In NSM, when user defined proposals in phase 2 are used, update fails on SRX Series devices.
- 892412—After J and SRX series devices are imported, NSM sets incorrect destination-port value if destination port is not defined in the custom service object.
- 878794—NSM unsets the policy when the policy name is changed.
- 880878—NSM unsets the policy when the policy name is changed.
- 894234—In NSM, device update fails when the comment field in the address group already present in the policy is updated.
- 888690—NSM does not delete members from the global address group and does not display delta.
- 886200—NSM displays invalid data when the custom report is sent over FTP.
- 878831—In NSM, Summarize Delta Config operation takes a longer time after upgrading to the current release.
- 884291—Deletion of scheduler object from policy causes an update failure on SRX Series devices.
- 874715—In NSM, device update fails while performing chained operation with Junos OS Global rulebase policy.
- 890345—In NSM, device update fails while performing chained operation with the following error: **Failed while sending rule data to Config manager.**
- 880069—NSM considers multiple default routes as duplicates in SSG devices even though the gateways are different.
- 877826—In NSM, policy ID warning message is displayed for domain pre or post rules when ID is greater than 74999.
- 855482—In NSM, unauthorized local access is permitted for every local or root user to access SQL database.
- 896098—NSM generates incorrect CLI commands when IDP log options are enabled under syslog messages for ISG devices.

- 871274—In NSM, while performing attack update for multiple SRX-IDP devices, signature version is not updated as expected.
- 900156—NSM does not set **VPN NHTB** and **MTU** configuration on tunnel interfaces after the upgrade.
- 897793—Unable to modify tunnel interface on a ScreenOS cluster.
- 862715—In NSM, Sensor category under Device Log action criteria is not available.
- 899183—NSM upgrade fails during migration.

Release 2012.2R3 Patch

NOTE: **NSM 2012.2R3 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see** http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R3:

- 745721—SSL-TLS renegotiation DoS vulnerability CVE-2011-1473 is present in NSM.
- 837571—In NSM, the e-mail messages about IDP signatures, which are sent in response to Device Log Action Criteria (DLAC), do not contain the information the user needs to find signatures.
- 865706—In NSM, updating IDP policy on ISG2000 Series cluster device fails occasionally.
- 846408—In NSM, GuiSvr fails over displaying the following error: **Referee does not exist**.
- 856524—NSM in HA mode failed over generating core file.
- 872541—In NSM, devSvrManager crashes and restarts generating core file.
- 840001—In NSM, when an ADSL interface with a bound-in PPPoA+D2 instance is configured on a VPN tunnel interface, the ADSL interface is not displayed in the drop-down list.
- 861778—Updates to the SRX Series device fail when two firewall interfaces are changed from the disabled to the enabled state using NSM.
- 862536—In NSM, the syslog configuration is unset twice, which results in an update failure.
- 862941—In NSM, when a Summarized Delta Config operation is performed after the storage manager cleanup, policy/address objects are not displayed.
- 864527—In NSM, a Summarized Delta Config operation displays policy information that is already present on the ISG Series device.
- 865086—NSM is unable to create device a device mapper (DM) for an SSG 320M device during device update.

- 584794—In NSM, the option to disable or change a rule or a rule set on any NAT rulebase is not available.
- 865141—In NSM, the CSV report is generated with errors.
- 834129—In NSM, a zone-based firewall rulebase is validated, shadowing policies are displayed incorrectly.
- 857084—NSM deletes the wrong BGP neighbors when a peer group is deleted.
- 858892—In NSM, a string search for object and device lists does not work.
- 861685—Unable to drag and drop service objects into a rule that contains the option **any**, in NSM.
- 866395—In NSM, global DIP values are not available in NSM VPN manager.
- 866740—In NSM, the dialog box for creating a service or network object from the protected resource does not select the object automatically.
- 868763—When you run **guiSvrCli.sh** on Solaris, NSM displays the following error: **/usr/netscreen/GuiSvr/utils/guiSvrCli.sh: syntax error at line 251: `DATA=$' unexpected**.
- 867674—In NSM, when multiple clients are configured for firewall authentication pass-through clients in a policy rule, all clients in the policy except is inactive on every update.
- 821030—In NSM, the direction filter for dynamic attack groups does not work as expected for compound attacks.

Release 2012.2R2 Patch

NOTE: **NSM 2012.2R2 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see** http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R2:

- 738241—In NSM, exempt rule is not available as a right-click option in the log viewer.
- 562569—Unable to configure source NAT for VPN Manager policies in NSM.
- 611183—NSM incorrectly permits a global MIP and address object to be combined and pushed to a ScreenOS device.
- 677428—The support level column for SRX Series devices is not shown in the list view in NSM.
- 731762—In NSM, the add button for adding groups to a predefined attack group is not working.
- 736571—While adding an unnumbered tunnel interface, NSM displays the interface mode as NAT instead of Route.
- 739990—In NSM, a duplicate cluster member is created when a cluster member is dragged to a group.

- 825892—In NSM, chassis cluster failover was caused by a malformed syslog message in the SRX Series device log.
- 834763—After upgrading NSM to the latest version, data in an e-mail report is incorrect.
- 840273—NSM displays the following error while updating multiple devices: **java.lang.ArrayIndexOutOfBoundsException.**
- 840461—After upgrading a ScreenOS device to the latest version, NSM displays an error about the cluster members.
- 841228—In NSM, after the Topology Manager has discovered a device, the device status appears unmanaged.
- 841385—Unable to edit the static route gateway IP on the device editor to configure a route in NSM.
- 842498—In NSM, incorrect commands are generated for ScreenOS devices when the L2 region broadcast method for IPv6 traffic is set to NDP and ARP.
- 844547—NSM tries to remove IDP and UTM configuration from a newly imported SRX650 device cluster.
- 846701—NSM tries to send IPv6 BGP configuration to an IPv6-disabled device.
- 847932—NSM deletes an address description from the address book.
- 850106—Unable to assign a certificate from a subordinate CA to the Infranet Controller from NSM.
- 850499—In NSM, an SSG350M device fails when NHRP addresses are updated.
- 852814—NSM hangs when **save as** or **delete** options are applied to policy objects.
- 855845—In NSM, exporting the audit log in CSV format generates core files.
- 852461—Unable to create bridge group interface from NSM for SSG350 device.
- 856981—In NSM, if an imported address object comment is different from the existing comment, NSM does not unset the associated rules appropriately.
- 856823—NSM sends vsys configuration to the vsys devices on every update, even though the devices and vsys are in sync.
- 848967—In NSM, when more than four SRX Series devices are updated simultaneously, attack updates fail with the following error: **applyImageOnDevice failed Array index out of range.**
- 854318—NSM tries to remove UTM (AV profile) configuration from a newly imported SRX650 cluster.
- 837978—After RMA activate, attempts to update a device on NSM fail with the following error: **Fail to get the connection state from the device - Object Not Found.**
- 859341—In NSM, the vsys address object limit is displayed for devices that do not support virtual systems.
- 860811—When NSM is upgraded from a previous version to the current version, the ICMP echo reply object is changed.

- 860160—In NSM, **find usage** is not available as a right-click option in a custom service object.
- 595176—When NSM is upgraded from a previous version to the current version, device validation fails with the following error: **$deviceobj.*:vsys_profile.user_servs.max: Integer value must be between 0 and 2048**.
- 707848—NSM does not display a warning message when a colon (:) is used in the name field of the address object.
- 832285—NSM allows you to create a schedule object without specifying a start time and date.
- 857340—A Summarize Delta Config operation fails on NSM appliances in a cluster.
- 858539—When you perform a Summarize Delta Config operation an update on an SRX Series device, displays the following error: **java.lang.ArrayIndexOutOfBoundsException: -1**.
- 859295—In NSM, attempts to validate a policy on a standalone IDP Series device fail with the following error: **Failed to convert policy**.
- 855308—An NSM appliance installed on CentOS 5.7 fails with the following error: **haDoDirect returned FAILURE RSYNC_GUISVR_DEVSVR_FAILURE**.
- 859834—The NSM upgrade process fails when you attempt to install the GUI server using only the **-nIGNOREDISKSPACECHECK=y** flag, because permissions on the /tmp directory are set to 770.
- 852612—In NSM attempts to export audit logs with the **guiSvrCli.sh** utility fail with the following error: **Cannot allocate memory**.
- 859876—In NSM, the option of selecting the **JXU-1SFP-S** slot for an SSG140 device is not available.
- 846728—In NSM, all the interfaces configured on an ISG Series device are not displayed on the vsys device.
- 859366—While sending the service group object **trace route** from NSM to a standalone IDP Series device, the updates fail and NSM displays the following error: **Return value: -14**.
- 853297—In NSM, the TFTP process running on Solaris is not detected even though they it is enabled.
- 852078—In NSM, logging on the global firewall for Junos OS rulebase cannot be enabled when viewed in extended mode.
- 858683—The NSM policy update fails when the host IP and MIP IP are changed on a ScreenOS device.
- 839918—On NSM, the route is not displayed when an ISG Series Cluster device is opened for the first time.
- 777364—The cross-site scripting (XSS) vulnerability CVE-2010-2103 is present in NSM.
- 860632—NSM domain post rules for the **global firewall** for Junos rulebase do not work.

Release 2012.2R1 Patch

NOTE: NSM 2012.2R1 has reached End of Support (EOS). We recommend that you upgrade to a supported release. For EOS information, see http://www.juniper.net/support/eol/nsm.html.

This section describes the following addressed issues in NSM 2012.2R1:

- 678157—In NSM, while an ISG Series device is being edited, the NSM GUI defaults to a window size that does not display all the options.
- 682922—NSM read-only users cannot perform expand-all operation on policy groups.
- 701636—In NSM, a destination IP configured on a ScreenOS device for VPN monitoring is not imported.
- 705652—NSM incorrectly displays a validation error while a SNMPv3 group is configured.
- 707037—When SNMP IPv4 hosts are defined in a ScreenOS template at the IPv4 or IPv6 section of the SNMP host add window, the list of hosts associated with a given community are not displayed in the expected format.
- 809891—NSM adds duplicate policy entries for VPN Manager devices that are added to new topologies.
- 811665—While importing a ScreenOS cluster that does not include VSDs, NSM imports two separate policies for each cluster member.
- 812164—NSM does not display the ADSL interface under the VPN Manager tunnel interface list.
- 821359—In NSM, rolling back the configuration on a device using an older version of the configuration file in CFM fails with an error.
- 823845—After importing the device configuration, NSM unsets all BGP-related configuration information at the next update.
- 824923—In NSM, some valid policy rules are deleted after execution of the **xdbOrphanRuleTool.sh** script.
- 828095—In NSM, policy rules are merged when zone and policy names are the same.
- 828107—NSM displays SSG firewall error messages for NHRP settings on every update.
- 832609—When NSM is upgraded from a previous version to the current version, the delta config and update on a branch SRX Series device fails with an error.
- 834960—Unable to create custom object for SunRPC protocol with the value 1937339233 in NSM.
- 835522—When NSM is upgraded from a previous version to the current version, the VPN policy displays warning messages for devices with the tunnel.1 interface.
- 836531—When you perform a Summarized Delta Config operation on a vsys device, NSM displays the following error:**Config on Device but not on NSM:**

set password-policy user-type auth minimum-length 1.

- 675539—In NSM, predefined service objects in SRX Series devices do not display TCP destination port 445.
- 746016—While managing an EX4200-VC switch from NSM, the status of the switch is displayed as unmanaged, and the connection status as blank, in NSM Topology View.
- 753186—A family inet configuration is removed or not configured by NSM if it is imported to an interface using a configuration group.
- 795625—In NSM, unable to filter the Policy Name column on a Policy Manager.
- 836654—NSM is unable to update a source interface on the RADIUS authentication server.
- 838724—In NSM, the offline Junos OS attack database update fails.
- 839384—NSM incorrectly displays a validation error for security zones on an NS5400 device.
- 840069—Zone group options do not work in NSM.
- 840078—While a ScreenOS device is being edited device for the first time, OSPF parameters are not displayed in NSM.
- 840264—The NSM client hangs when the real-time monitor is opened.
- 842794—NSM displays large delta configurations when a device rule-ID is greater than 749999.
- 842887—When **infranet-auth** option is enabled on a Netscreen vsys policy, NSM tries to reset the policy without the **infranet-auth** option.
- 834848—In NSM, scheduled updates on the attack database fail on an ISG Series device.
- 842011—Unable to import subordinate CA certificate in NSM.
- 847587—In NSM, CLI-based attack database updates fail when the Junos OS attack database download is not enabled.

Release 2012.2

This section describes the following addressed issues in NSM 2012.2:

- 745634—In NSM policy view, when you add a new service to a rule that has the service option **any**, NSM adds the new service without removing the option.
- 465301—The OpenSSL library and apache web server using openssl library forcing security issues. This issue can be addressed in NSM appliance platform by upgrading the CentOS version to 5.7.
- 774262—Vulnerabilities reported via security scan. These issues can be addressed in NSM appliance platform by upgrading the CentOS version to 5.7.
- 803000—Security vulnerabilities found in NSM. This issue can be addressed in NSM appliance platform by upgrading the CentOS version to 5.7.

- 491817—Unable to create VSI interface higher than 7 in NSM.
- 769127—NSM does not import MIP groups from ScreenOS devices running 6.2 or later.
- 677433—NSM does not warn or limit the number of route map entries per route map on a ScreenOS device.
- 694066—In NSM, the option to set **syn-check-required** for a **per policy tcp** on an SRX Series device is not available.
- 734928—NSM incorrectly updates configuration files when an install is upgraded using a custom NSM installation path as the installation directory.
- 783791—NSM fails to install the regional server from the NSM GUI because of insufficient disk space.
- 787909—When NSM is upgraded from a previous version to the current version, entries such as super password, license type, and so on are deleted from **nsm_setup**.
- 795735—In NSM 3000, SNMP reports 100 percent CPU utilization. This issue is addressed by upgrading the CentOS version to 5.7.
- 797097—NSM deletes **tcp-options** and **apply-group-expect**from the firewall.
- 821112—Unable to access the information from the address objects fields in NSM.
- 824429—When you attempt to update a cluster that contains multiple device groups, NSM attempts to update all the devices in the cluster in addition to the intended device.
- 825900—When NSM attempts to perform a device update or summarized delta configuration, the operation fails with the following error: **object is locked out for this conn**.
- 826120—Unable to create an NHTB entry from NSM in a vsys using a shared untrust interface.
- 829580—In NSM, an attack update is displayed as 30 percent even though the attack update is pushed to the device successfully.
- 834328—NSM import and export operations fail, generating core files.
- 835033—The NSM devSvrManager process fails frequently, without generating core files.

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.

NSM

- 1313773 - NSM2012.2R14: NSM does not allow editing source and destination ports with low value on low-high pair in source and destination NAT rule base.
- 1312801- NSM2012.2R14: The configuration update to the device fails when you push the snmpv3 target configuration to the device.
- 1305667 - NSM2012.2R14: The rule group does not display rules when you expand the rule group.
- 1320572 - When you update ISG-IDP and predefined IDP policies, the update fails.
- 1153227 - When you update the IDP detector, the update fails.
- 1206482 - In NSM, the **java.lang.NullPointerException** error message is occasionally displayed when you create an exempt rule base on SRX Series devices and when the Global Firewall for Junos OS rule base is present in the same policy.
- 1198117 - NSM displays an **outbound-ssh secret** error when the RMA activate directive is performed on SRX Series devices.
- 1103634 - The CentOS 6.5 upgrade ISO is not compatible with the NSMXpress and NSM4000 appliances. However, it is supported on the NSMXpress-II and NSM3000 appliances.

  Update recovery partition and factory default features are not supported on CentOS 6.5 for the NSMXpress-II and NSM3000 appliances.
- 910894 - NSM does not display the correct information in the audit-log viewer's comparison window when a firewall policy is unassigned from the device.
- 1078345 - NSM deletes the NTP source address on the next update for SRX Series devices with Junos OS version 12.1X44-D45.2.
- 928788 - When SRX Series devices to be configured with BGP neighbor group authentication key are updated through NSM, NSM displays delta even after a successful update. This is because, although NSM sends the authentication key in plaintext, the key gets encrypted on the SRX Series devices. While performing a delta operation, NSM finds a mismatch in the authentication key and tries to reregister the authentication key in plaintext.

  Workaround: NSM synchronizes with SRX Series devices only when the encrypted authentication key is manually copied from the device CLI to NSM.
- 944384 - NSM continues to display the configuration status as in-sync, even after modification of the configuration in the IVE admin UI.
- 1030470 – The installation script displays an httpd warning message during a fresh installation of 2012.2R10 with an IPv6 management address.
- 1031314 – An NSM server with an IPv6 management address fails to authenticate NSM users through a Radius server in RHEL 6.5 running on a Linux server and CentOS 6.5 running on NSM4000 appliances.
- 1031317 – Unable to launch the WebUI of NSM appliances that are configured using an IPv6 address.

- 1032502 – An IDP250 device disconnects from NSM after an upgrade to the current version of NSM.

  Workaround: Perform an RMA activate to reconnect the IDP250 device to NSM.

- 1032972 – NSM displays a delta related to destination NAT after an upgrade of the device image from 12.2X45-D10 to 12.1X47-D15 engineering image.
- 1042293 - NSM intermittently fails to display SRX Series stream logs in Log Viewer when the devSvrManager process is restarted after the "devSvr.enableSyslogOverUdp" option is set as "true" in the devSvr.cfg file.
- 1033143 – NSM server restarts while performing 2-3 directive operations simultaneously.
- 1013997 - While verifying the devSvr version, NSM prints an additional message: **00cf47a4e755326056fb485b6ea553ab194401f2**.
- 1014287 - When an NSM HA failover occurs, the devSvrManager process in the secondary server starts after a delay of 3-4 minutes.
- 1010642 - In NSM on Windows 8.1, the Telnet client cannot be launched using the right-click function.

  Workaround:

  1. Enable the Telnet client through **Control Panel** > **Programs and Features** > **Turn windows features on or off**.
  2. Copy telnet.exe from **C:\Windows\System32** to **C:\Windows\SysWOW64**.

- 1008663 - Unable to add a FIPS enabled ScreenOS or SRX Series device to NSM, even when FIPS is enabled in the device and NSM.
- 980769 - NSM displays delta for the antivirus scan-options timeout value for high-end SRX Series devices with the 12.1X46 image.
- 952593 - NSM displays a delta configuration summary after an SRX Series device running Junos OS image 12.1X45 has been added.
- 952945 - The NSM update fails when the sessions-per-client limit value in UTM is configured as 2000.
- 954339 - NSM fails to provide the option to configure UTM Web filtering parameters such as **no-safe-search** and **quarantine-custom-message**.
- 958712 - In NSM, the newly added URL categories in Juniper Enhanced Web filtering are not listed in alphabetical order.
- 958740 - After upgrading NSM to the latest version, NSM fails to import the source port in the Source NAT rule.
- 958752 - NSM intermittently fails to populate pool information under the **Action** column for Source and Destination NAT rules.

  Workaround: Select the **Action** column in the UI.

- 959581 - NSM fails to copy and paste address objects for NAT rules.

- 940555 — NSM fails to update a policy in the device when the APE rule base in the policy has custom application object that has the match order value same as the value used in the pre-defined application object.
- 944996 — In NSM, warning messages appear during the installation of Solaris build.
- 944745—NSM unsets IKE gateway heartbeat parameters and VPN monitor for AC-VPN, when AC-VPN is configured with hub and spoke topology.
- 944744—In NSM API, object collision identification fails when adding a member to the existing address or service group.
- 929140—In NSM, the client is unable to connect to NSM Solaris server intermittently when the schema versions are different in the client and server packages. This issue is seen intermittently due to the increasing merged schema size.

  Workaround: The following workaround is recommended when schema version of the client does not match with the server schema and there is a problem during connection from the client to server.

  Server Side Modification

  1. Increase the heap size in jax.spec under **/var/netscreen/GuiSvr/xdb/specs/** on GuiSvr as follows:
     - **Original content**:

       :jvm-options (

       : ("-DEMBEDDED_JVM=true")

       : ("-Xms128m")

       : ("-Xmx256m")
     - **Need to modified to**:

       :jvm-options (

       : ("-DEMBEDDED_JVM=true")

       : ("-Xms128m")

       : ("-Xmx1280m")
  2. After modification, restart GuiSvr.

  Client Side Modification

  1. Delete <NSM_Installed_Dir>/ versions if any.
  2. Delete .nsm folder.

  After making the changes, connect the client to the server. It may take 30-40 minutes for the initial connection. But the subsequent attempts for connection will be faster.

  After the initial connection is established, revert the heap size modification in jax.spec back to the original value to avoid hampering other processes and to avoid system instability.

- 921760—NSM fails to push MIP configuration to the SoS device. However, NSM states that the update is successful.
- 676278—NSM changes the permitted IPs after the ScreenOS device is upgraded to 6.3.

  Workaround: Before upgrading ScreenOS device to 6.3, manually edit the IP address to the new IPv4 format in the template. After the firmware upgrade is successful and the device is edited, NSM displays the permitted IPs that are duplicated. Mouse over the permitted IP entries and delete the entries for which the tooltip **From object** appears.

  If ScreenOS device is already upgraded to 6.3, edit the IP address to the new IPv4 format in the template. The new IPv4 format is automatically reflected in the device. Mouse over the permitted IP entries and delete the entries for which the tooltip **From object** appears.
- 911718—In NSM, while performing attack update on ISG device with IDP support, if the option **All Attacks** is selected, device attack update fails. This is a device limitation.

  Workaround: Perform a selective attack update that works on the device.
- 905869—In NSM, after upgrading to the latest version, CLIs **unset flow route-cache** and, **unset flow icmp-ur-session-close** are displayed while performing delta summarize config.

  Workaround: Configure the above two CLIs again in associated device before subsequent update.
- 909151—In NSM, after importing NAT rules from device, Source address in the rule gets deleted if any modification is attempted on the same rule.
- 909160—In NSM, if the phase-2 proposal has aes-gcm but does not have authentication algorithm, and if configured on a device and imported, NSM shows delta for MD5 authentication algorithm.
- 910047—In destination and static NAT rule configurations in NSM, the destination address, address name, prefix and prefix name are not getting refreshed.

  Workaround: Delete the rule and create it again.
- 911480—NSM fails to show hardware inventory of EX series VC devices due to schema issue.
- 896784—In NSM, MIP cannot be configured on ISG1000 cluster member using management interface
- 885866—In NSM **set env ipv6 enable** option is greyed out on members for an ISG cluster.
- 854653—In NSM, zone group does not work as expected, when the policy rules contain set 800000 or more.
- 866394—NSM client shuts down occasionally with an exception while adding SOS software image to NSM using Software manager.
- 881680—NSM shuts down while saving larger configurations.
- 882556—In NSM, delta is seen after adding MAG-SM160

- 884599—In NSM, Unable enable or disable IPv6 environment variable at cluster level on ISG2000 cluster
- 884765—Export policy is not working in NSM
- 887712—Export Policy of VPN policy rules in VPN Manager does not work in NSM.
- 695371—When a service or application object is imported from a device without the source port range explicitly configured, NSM sets the source port to 1-65535 instead of 0-65535.

  Workaround: If port 0 needs to be included, the port range 0-65535 should be explicitly configured on device and imported to NSM or the source port range set to 0-65535 in NSM after import.
- 867444—**Launch Telnet** option for ScreenOS Series device does not work on Windows 7.

  Workaround: Copy the file **C:\Windows\System32\telnet.exe** to **C:\Windows\SysWOW64**.
- 838573—While deleting SRX cluster at Cluster level, NSM deletes only one member and error displays the following error message: **failed to remove cluster member references**.

  Workaround: Try removing the cluster again and in the second attempt, the members will be removed successfully.
- 839824—NSM device update configuration fail when, **to-zone** or **from-zone** is selected as **junos-host** under policy.
- 858892—String search in object or device listing does not work in NSM.
- 816397—In NSM, after a schema upgrade, configuring a routing-instance with destination NAT on SRX Series devices display a validation error.
- 842327—Disabling services offload option on SRX high-end device is not working in NSM.
- 842381—NSM does not display extended applications while creating application group.
- 747830—In NSM, the configuration status changes to **NSM Changed** while you are editing, deleting or importing ScreenOS configuration file management settings.
- 749590—When the find usage option is used on an address object in the Policies view, the view hangs.
- 749654—NSM does not support address group when IPv4 and IPv6 addresses are used, even though address groups might be supported on SRX Series devices.
- 770004—In NSM, custom DI objects are created under Custom IDP attacks, and are not available to be selected for DI attack groups.
- 776436—On upgrading NSM 2012.1, with previous releases of Junos OS 11.2 release, a warning message is not displayed when you select the destination address name.
- 777029—The search options for source, destination and service are not working in the global policy rulebase.

- 778840—When the **Diff running config file** workflow in ScreenOS configuration file management is used, the NSM GUI colors change. To resolve this issue, restart the client.
- 781664—When SRX Series, or ScreenOS devices are added using the blade server workflow, a warning message is not displayed.
- 785654—NSM is unable to deactivate all rules in the IDP rulebase.
- 785668—The rule number is incorrectly displayed the log viewer after the policy has been reordered.
- 786723—NSM tries to delete existing and create new configurations related to UTM antivirus settings.
- 788314—In NSM, when an IC Series UAC Appliance is added, a duplicate entry is created occasionally. This can be resolved when the services are restarted.
- 775422—In Static NAT, Inet node is not displayed in the action field.
- 789260—In NSM, attack updates fail occasionally. For information see http://kb.juniper.net/KB14181.
- 779355—Topology discovery do not detect WAN links, if dynamic routing is used on WAN interfaces.
- 771769—In NSM, after generating IDP profiler logs, source and destination IP address is transposed in log viewer.
- 266865—If the startup information for a device is updated from **Use Device Server Through MIP** to **Use Default Device Server IP Address and Port**, NSM cannot push any change to the device.
- 277604—2008.1: **In-device** Policy Node is shown even while logged in through **No View**permission of Security Policy and View Permission of device in NSM.
- 277997—2008.1-VPN: Address objects naming constraint for Voyager devices cause issues with pre-defined ScreenOS device VPNs.
- 284698—Interface configuration screens may show more settings than supported by the actual interface.
- 286643—Creating virtual system devices with (dot) "." in the name will cause firmware upgrade to fail. The root device will reflect the change, but the virtual system will not.
- 287814—IDP subdomain administrator able to modify global address objects.
- 288309—For J Series routers in an NSM cluster, the failover triggers hardware inventory **out-of-sync** when device connects back to NSM.
- 292369—When a policy-based VPN is created and updated device and imported back to 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 it are removed from the VPN Manager, but not the Policy Manager policy. Before the devices can be successfully updated, the VPN rules need to be manually deleted in the policy under Policy Manager.

- 292522—Update to host value in an already existing terminal service resource profile, does not update the host value in the bookmarks.
- 295156—Modifying an existing SAM policy results in reshuffling the policies.
- 295314—Database version created by column is unknown for import device.
- 299504—Promotion to template is empty if opened fast.
- 299014—During an upgrade installation of NSM, license information is required to complete the installation, though the license is present in NSM server.
- 302289—The virtual chassis with **me 0** interface causing device disconnect after inventory import.
- 302500—If you perform a firmware upgrade from Junos OS Release 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 operating system (OS) version of the device. To adjust the OS version in NSM, open Device Manager and right-click the device. Select either View/Reconcile Inventory or Adjust-OS Version. Ensure that the OS version running on the device matches the one recorded in the NSM database.
- In NSM 2008.2, the NSM UI connects with the GUI server through port 7808, which is FIPS compliant. When installation is complete, you see the following message: **Please note that TCP port 7808 is being used for server-UI communication**. Earlier versions of NSM connected through port 7801, which was not FIPS compliant.
- 303308—In case of Platform mismatch, NSM should not send get-syslog-events RPC.
- 304406—In a HA environment, when performing a refresh with the NSM installer or NSMXpress UI, an error exists which may cause the HA peers not to initialize communication properly. The most common scenario where this error occurs is when trying to migrate from a single NSM server to a HA configuration. This error does not occur when performing a clean install or an upgrade using the NSM installer.
- 312509—NAT rule set configured on SRX5800 devices are not imported properly into NSM.
- If you add a Junos OS device to the NSM database through the reachable device workflow, you must enable netconf for SSH (specific to system services) by running the following command in the device CLI: **set system services netconf ssh**.
- 388578—NSM 2008.1r1 does not support SSL-VPN security devices.
- 394543—Update device operation for more than 30 devices hangs for 5 to 10 minutes when configuration updated is large (> 50k).
- 396285—Rebooting NSM servers fails in a Solaris 10 environment. The workaround to start or stop an NSM server is one of the following:
  - 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. Do not use this script as the root user.
- 400850—The physical interfaces bound to security zone similar to the redundant interface, is not displayed in non-members list of PBR policy.

- 404479—The interfaces configured in a Shared-Vr on a virtual system or cluster-virtual system device is not listed under the next-hop entry in SIBR routes.
- If you add a Junos OS device to NSM through the unreachable workflow, execute the following commands on the device CLI to enable logging on it:
  set system syslog file default-log-messages any
  set system syslog file default-log-messages structured-data
- 404943—In Policy Based VPN, NSM pushes invalid CLI for services.
- 406791—NHTB reference error on the migrated setup from 2008.1R1 to 2008.2.
- 409350—NSM does not support automatic ADM transformation for DMI devices.
- 410009—Overlapping of unconnected devices with connected devices and links needs to be avoided in topology map. The workaround is to manually drag unconnected device icons to free areas in the topology map, or view connected and unconnected devices separately.
- 422422—With every action, memory usage continue to increase.
- 426324—**guiSvrManager** crashed and cored with 17 clients on 2kFW+100IDP+1NS5400with 2k VPNs.
- 434863—VPN Manager auto fills local and remote proxy IDs for a route-based tunnel with outgoing interface IP, which is incorrect; when the VPN is in between a third-party device and a Netsctreen device
- 436587—In 2008: After migration from 2008.1R2 to 2008.2R1, NSM unsets NHRP, routerid, and auto route export.
- 437109—If backup is disabled during a high availability installation of NSM, manual backups using the script **replicateDb** present in the **/usr/netscreen/HaSvr/utils/** directory are not allowed too.
- 437457—For virtual systems, updating device with an ICAP profile fails with an exception.
- 438631—Packet capture configurations are not imported from devices, after upgrade from 4.1r3 to 5.0.
- 439567—Update fails on SRX devices when the service filed is changed in IDP policy and is pushed to the device.
- 439909—NSM API cannot login using a user-defined inside a sub-domain.
- 443271—"When device disconnects and reconnects back to NSM due to a reboot, the hardware-inventory status may be set to out-of-sync in NSM even when there is no change in the device hardware. Workaround: Perform inventory refresh. The status is set back to in-synch in NSM."
- 449502—NSM not able to login to SA device using the provided valid credentials. Workaround: Perform inventory refresh. The status is set back to in-synch in NSM.
- 446392—When migrating from 2007.3R1 to 2008.2R2, NSM is unsetting and setting to different configurations (belongs to loopback and sub interfaces) after migrating from 2007.3R1. Migration from 2007.3R4 to 2008.2R2 succeeds.

- 450863—NSM should through an error when an IPv4 address is added to an IPv6 address group on using "replace with" option.
- 450964—First time log in to the Web UI should point the user to the Install page.
- 452182—While searching IPs there is no option to search all IPs for a subnet.
- 452960—NSM should not allow the user to configure DIP in a subnet when the extended IP is set in some other subnet.
- 452898—Binding an interface to a zone makes the order of the options change.
- 453968—Search option in IPv6 and IPv4 policies are not working as expected.
- 454983—CFM Auto import is not working for NSMXpress box. The workaround is to run the **passwd cfmuser** command as root on the NSMXpress device and enter the same password configured during install.
- 455944—Route-map field entries are not correctly displayed at the template.
- 457072—Node specific entries cannot be created from NSM for cluster.
- 457242—Myreport graph displays 0.0.0.0 along with IPv6 addresses.
- 457557—Java null pointer error shown for IPv6 rule created by custom admin with custom role (Create Security Policies).
- 458585—NSM should display a validation error for Attack Database Server, if an invalid server path is provided.
- 459052—While creating gateway VPN settings, the NSM update often sends the following commands:
  set ike gateway g1 dpd-liveness interval 0
  set ike gateway g1 dpd-liveness retry 5
  unset ike gateway g1 dpd-liveness always-send
  unset ike gateway g1 dpd-liveness reconnect
  unset ike gateway g1 nat-traversal
- 459323—NSM does not display validation message for Destination or Source port Low or High Values under Extended Access-lists.
- 459330—NSM fails to update PBR match-group and action-group names if the name string has spaces.
- 459949—Profiler does not get enabled in device on restarting when AVT is enabled. The workaround is to right-click on the device and select Start profiler.
- 460492—Warning for SELinux package when installing system update on RHEL 4.6. However, the installation works.
- 460645—GUI display is not proper for **Update device config** options. The workaround is to extend the length of the window to view all the options.
- 460894—The NSM Object Manager does not display Zone object details.
- 461192—At route-map Interface List NSM should display only the configured interfaces not all the interfaces.
- 461266—Standard icons are not showing in topology for few device platforms.

- 463254—The order of the nodes within the Network tab change when the transparent mode is turned on for a template.
- 463738—The mode displayed under **Device config** for interfaces of a device in transparent mode shows as route mode where as it should be transparent mode.
- 463788—NSM UI displays a validation error for route-map entries, but the device accepts it.
- 464029—NSM shows validation for IPv4 addresses even though the VPN terminates on an IPv6 address.
- 464071—SCTP, UTM and GTP Objects when deleted from the policy shows up in expanded mode.
- 464094—NSM allows to create IPv6 based DIP when the IPv6 mode is set to none under any interface.
- 464145—When VPN monitor displays status about an active VPN, the "Local address" and "Peer address" fields are left blank.
- 464404—Configuring a custom-vr using a template shows an override near the custom-vr created and also an option to revert to the default or template value near the virtual router name.
- 464834—Unable to map predefined users "nsm" and "cfmuser" while creating WebUI users and setting authentication to Unix. Recommendation is, do not map predefined users to WebUI users through UNIX authentication.
- 465023—The quick configuration editor Interfaces page is not refreshed when an interface is edited from a regular config editor. Functional zone tables are not validated when any node under functional zones is configured.
- 465407—NSM allows to configure IPv6 options on an IPv6 disabled device (device running 6.3 OS).
- 465748—Auto Download of NSM Client from NSM appliance fails. A workaround is to download the client directly from the NSM server (https://*ApplianceIP*) or change the **guiSvrWebProxy.port** value to **443** in **/var/netscreen/GuiSvr/guiSvr.cfg**.
- 466039—The Interface Quick Configuration landing page usually shows **"Could not Create View"** for EX Series, MX Series, and SRX Series devices.
- 466233—IPv6 address does not display under routing table entries (Network > vr > vsys1-vr > Routing table), for modeled virtual system devices. A workaround is to import the vsys device.
- 466335—Super user password cannot be changed from the Web UI for an NSMXpress box.
- 466349—NSM does not filter IPv6 policy rules from the Central Manager during an update to a ScreenOS device that does not support IPv6.
- 467745—The NSM 2008.2r2 client often displays an empty device list.
- 468189—When migrating from 2008.2r2 to 2009.1r1 installer script does not show old versions correctly.

- 472185—NSM monitor slow to detect state changes.
- 473963—NSM3000: hared disk installation reports Password is too short, minimum length is 8 characters for one-time password for device server.
- 474008—NSMXpress: Getting a **Stopping NFS statd: [FAILED]** message while installing the RS. However, the installation is successful.
- 474518—Check box missing for NTP on redundant interfaces within NSM.
- 475084—NSMXpress: Unable to create a user with password option "Unix authentication" under user management "NSMXpress User list".
- 477352—Screen refresh after creating an object is poor.
- 477355—Junos does not do any validation of configuration from NSM.
- 478484—During a regional server installation on an NSMXpress appliance, the following error message at the post-installation tasks stage is displayed:
  "No such file or directory" (/bin/cp: cannot stat `/usr/netscreen/GuiSvr/var/metadata_table.nml': "var/install/NSM-RS)
  However, the installation is successful.
- 479859—NSM should not allow creation of ANY-IPv4 or ANY-IPv6 objects in Object Manager.
- 481088—SMTP Protocol Anomaly attack object does not contain Recommended Action.
- 481124—A DI signature is shown as member of IDP dynamic attack group.
- 485787—NSMXpress - Online recovery partitioning from 2009.1r1 does not happen to 2009.1r1a.
- 484205—Community-list command for BGP is not same in job information and in device.
- 484701—NSM 2009.1r1 client response time is slower than 2007.3r4.
- 486191—2009.1r1a:Reconfiguration of NSMXpress standalone fails using nsm_setup. Reconfigure NSMXpress through nsm_setup.
- 489761—In an extended high availability setup, NSM reports improper DMI device connection status upon **GuiSvr** failover. The workaround is to restart the Device server.
- 493491—In 2010.1, the **Random-port** option is not available while configuring DIP on ScreenOS device interface.
- 495927—2010.1: In a policy, when right click on source or destination address of an IPv6 rule, NSM does not give the "Add Address" and "Filter" options. The workaround is to directly right-click on the rule without first selecting it.
- 496118—2010.1: NSM fails to update, while pushing "Manage-IP of redundant IP" on ISG2000 cluster.
- 496177—2010.1: Update of IPv6 prefix list on physical interface fails with ISG2000.
- 496395—2010.1: (TEMPLATE) NSM UI does not display a validation error at **VR -> Virtual router id**, when OSPF and BGP are enabled.

- 496431—2010.1: NSM pushes redunt interface configuration on each update for an ISG2000 device.
- 496701—2010.1: Update fails (set cpu-protection threshold 0), after upgrading ISG2000 from 6.2 to 6.3 through NSM.
- 496705—2010.1: Wizard to configure DIP for an interface in ScreenOS template is not displayed completely. The workaround is to drag the wizard open completely. On subsequent edits, the wizard opens to the same size as dragged earlier.
- 496721—2010.1: Removing peer-group member from a peer-group in BGP and updating it to the device does not delete the same from device.
- 497112—2010.1: Update and Delta is failed on SRX3600 devices, if IDP policy with dynamic attack group, which has all filters enabled.
- 497949—2010.1: New user role tab in a user role group creates new user role by checking only members and hence duplicate members are created.
- 498731—2010.1 (IPv6): NSM displays the IPv6 tab at VSI interface, even if there is no support for ScreenOS 6.0 OS versions.
- 498733—2010.1: NSM UI display is not proper for enabling **Track IP** at Cluster Members VSD Group Monitoring.
- 499146—2010.1: Delta seen after RMA/Activate of NS204 device with MS DB.
- 499174—2010.1: Update fails when configuring Service-applications at policy and updating to Junos (J6350) devices through NSM.
- 499181—2010.1: NSM UI display the **Gateway Tracking On** option for IPv6 destination based routes, which is not supported by IPv6 destination based route.
- 501774—2010.1: Device connectivity in NSM goes down and comes up, when trying to push port template configuration to device through NSM.
- 502716—2010.1: Unable to push IDP policy on MX960 device from NSM.
- 503701—**Select Cluster Member** option is not shown in UAC Manager -> Infranet Controller to select EP to associate with ICs.
- 504876—2010.1: EX8216 devices are not getting connected to NSM with Junos OS 10.0R1.8.
- 504886—2010.1: NSM UI does not display the **Advanced > Predefined Service Session cache > Predefined Services** option, when a ScreenOS device is modeled and activated.
- 506135—Query Expression variables are not displayed for log monitoring/filters for SA device. The workaround is, create a query expression in a template where these variables are visible and successfully update a device in NSM with the template.
- 514022—2010.1a (IPv6): It is unable to delete the IPv6 node under interface, through NSM. The workaround is to delete an IPv6 address configured on an interface using the CLI.
- 514848—2010.1a (IPv6): Duplicate host and network names gets created in Object Manager when the IP is changed.

- 515487—The loopback interface belonging to a shared zone in a vsys is incorrectly imported into NSM.
- 516415—2010.1a (IPv6): Changing the domain-name of an IPv6 address object in the device and importing it to NSM imports it as an IPv4 address object.
- 516420—2010.1a: Device Monitor does not update the modified device polling time, automatically.
- 517719—NSM - Pulse: Unable to add pulse binary package to NSM. However, the pulse binary package size is 70 MB and requires 2048 MB of heap memory.
- 521704—2010.2: Same users cannot be deleted when logged in.
- 521930—2010.2: Junos applications node in template shows extra options which are not present in actual device for both pre-defined and custom applications.
- 523092—2010.2: When creating log reports, NSM does not allow to select the dates March 29, 30 and 31 in time period.
- 523099—2010.2: NSM UI displays the deleted virtual system information.
- 523176—2010.2 (Reports): If **Columns for Report** is selected with either source, destination, NAT source or NAT destination IPv6 address, report displays an **0.0.0.0** also.
- 523190—UAC-Interop: Username and Password text boxes gets displayed only on selecting Authentication Type to **Certificate** and then back to **Basic**.
- 523484—2010.2: Version number is wrongly displayed for Junos devices after a firmware upgrade through NSM.
- 524124—2010.2: After importing an exported configuration file successfully, NSM should not show the configuration status as **Managed,Insync**. The workaround is to update the device after importing the configuration file.
- 524216—Predefined Junos OS service objects **junos-persistent-nat** and **junos-stun** are not available in NSM.
- 526007—NSM3000: Factory Defaults option with Offline Update Recovery Partition from 2009.1r1a to 2010.1 fails on NSM3000 appliances. The workaround is to re-install the image through USB.
- 526499—2010.2: After upgrade to LGB13z1bb, NSM shows old versions of haAvailSvr as well.
- 532855—The NSM application will not discover all end point devices if complete address forwarding tables (AFT) information is not available.
- 562393—When SRX low-end family devices (which have been renamed from 10.2) are added through model or unreachable workflow, the Managed OS version support drop down list in NSM must display operating systems only up to 10.1. However, the list displays 10.2 and 10.3 too.
- 572667—NSM allows manual grouping of a standalone IVE device or blade server members that belong to a different blade server. However, NSM must validate the manually added members belong to the Junos Pulse gateway blade server. The

workaround is not to manually group members belong to different Junos Pulse gateway blade servers or to use automatic grouping workflow.

- 580279—When you delete a blade server after adding a blade server member or an IVE device, a **Reference cluster owner removed** message is displayed even though there is no cluster grouped under the blade server. This message can be ignored.
- 582020—When the **policy-options** command is configured on a Junos OS device and imported to NSM, the **next-hop** and the **load-balance** options are not available on NSM. The NSM UI needs to be synchronized with the Junos OS device.
- 583241—Update device operation fails when an IVE device OS is upgraded from the NSM UI. We recommend that you import the device configuration first, make the required changes, and then update the device configuration from NSM.
- 591145—When you change the FPC power configuration from Off to On, a **Hardware inventory out of sync** error is displayed. As a workaround, execute the **View/Reconcile** operation to reconcile the hardware inventory of the Junos Pulse gateway blade server, and then update the configuration.
- 597263—When you perform an import operation on the blade server after changing the FPC power configuration from Off to On, the application blade is removed from the chassis and added to the device tree root node. The workaround is to delete the application blade from the NSM UI, add it again, and then perform an import device config operation on the Junos Pulse gateway blade server.
- 608293—The NSM UI displays a validation error when 11.1R1.14 JPG device images are added to NSM. This is a one time issue and once **OK** is clicked after adding the device image, the error gets disappeared.
- 666486—The SLE parameters are visible even when the attack version selected is not IDP 5.1. (By default, the SLE parameters should be visible only when IDP 5.1 is selected.)
- 720916—Occasionally, validation error occurs on Predefined Attacks after attack update, when incremental update option is selected. However, this will not affect the functionality.

  Workaround: On seeing this issue, select a different node (for example, **Device Manager**), and then select **IDP Objects** node again, the validation error will disappear.
- 721782—The option **Update IDP Rulebase Only** should update only the IDP, Exempt, and Backdoor rulebases. But currently NSM is updating both APE and SYN Protector rulebases along with the above mentioned rulebases when the **Update IDP Rulebase Only** option is selected.
- 725530—Duplicate IDs are shown under **Zone Based Firewall** after importing SRX virtual chassis device. For J/SRX Series devices, this error applies only in case of two rules having the same zone directions.

EX Series Switches

- 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 OS Releases 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 in to 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 OS Release 9.2R3 or 9.3R2.
- 398860—If you use LLDP, IP phones connected to 9.2R1.10 EX Series switches are not discovered. You need to upgrade to EX Series 9.2R2.15 or later.
- 402243—On a virtual chassis, if there is a physical link through the vme0 interface to an adjacent EX Series switch, topology discovery records two links, one from the vme interface and another from the me0 interface.
- 406887—Topology discovery commits data in small chunks to the database. If one of many such transactions fails, the remaining data is not committed. This could create inconsistent data in the database.
- 427855—When both master and backup router engines in a grande device are reachable by SNMP, topology discovery displays them as two separate devices in the topology map.
- 444091—Wrong links are discovered with EX8200 devices with only STP/RSTP. Enable LLDP on all the switches to ensure that links are discovered properly.
- 446950—Because of a UI issue, NSM incorrectly allows you to create virtual chassis with EX3200-24P. Virtual chassis should be created with EX4200 platforms only.

Devices Running ScreenOS and IDP

- 294030—On an ISG device, sufficient device memory is required to compile the policy during an update from NSM. A policy that specifies **All attacks** needs 600 MB or more RAM on the device. The update fails if the amount of RAM is insufficient. Contact JTAC for a workaround.
- 450906—When IPv6 is enabled on an interface in host mode, NSM does not generate any interface ID unless configured by the user whereas ScreenOS does, causing a mismatch. A workaround is to import the device into NSM after you update the IPv6 settings.
- 454755—ScreenOS does not treat DI profiles as standard shared objects. Hence NSM does not reflect changes in the profiles after you import a device.

- 458945—NSM cannot manage a device running a ScreenOS version earlier than 6.3 with an IPv6 configuration. For NSM to effectively manage the device, it must be upgraded to ScreenOS 6.3 and added or imported into NSM.
- 461167—You cannot export device logs using the syslog option from the NSMXpress WebUI.
- 461181—Updating fails when a policy with web filtering enabled is pushed to a vsys device from NSM.
- 461986—You cannot generate reports and e-mail them using the email.sh option in the NSMXpress appliance.
- 464396—On a modeled ScreenOS root device with a modeled vsys device, NSM does not display the IPv6 option on the modeled vsys.
- 464517—When a rule is added to a policy and the Notify Closed Session option is enabled, NSM shows the 'unset IDP' command in the delta configuration. If IDP is enabled on the device, IDP does not get unset.
- 465144—NSM does not display the option to monitor the IDP security module under the VSD group monitoring section.
- 479370—NSM does not generate dead peer detection configuration for IKE gateways on SRX Series devices.
- 497120—Updating an SRX3600 device with an IDP policy fails, displaying a "Previous commit is in progress" error message. The workaround is to wait for several minutes until the back-end commit process is completed.
- 518101—Validating a device fails after adjusting the OS version or updating the software through NSM.
- 521642—NSM displays delta configuration for ISG devices after the OS version is adjusted from 6.1 to 6.3.
- 522885—While adding SOS devices on an NSM HA server, a **DB_EVENT_PANIC** error message is displayed, and the HA server fails over to the secondary server. This issue is seen occasionally.
- 522890—Editing a ScreenOS cluster device, with a device configuration of 275 KB, takes approximately 5 minutes.
- 523203—ISG-1000 devices running ScreenOS 6.3r3 display a validation error under the root profile.

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

- 436750—NSM cannot import an IC if the IC has more than 5100 resource access policies. The import operation does not complete.
- 455844—Deleting an SA device object from NSM does not remove the object until services are restarted. This is seen intermittently.
- 460586—When a Junos OS SA/IC template is removed from a device, the template values are not retained even if the **Retain Template values on removal** option is checked.

- 465450—While creating a new custom expression under Role mapping, if you choose Directory/Attribute: as any LDAP server on NSM when you configure the User/Admin/MAC Realm General settings, the update to an SA/IC device fails.
- 519756—Creating a new Kerberos Intermediation on an SA device running SA 7.0R1 without assigning a realm will display an error. The workaround is to create a realm and assign it to the default Kerberos Intermediation.

SRX Series Services Gateways

- 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.
- 439305—An SRX Series device update fails because NSM does not drop the invalid IDP policy rule, **IP-action** with **Block** option selected. Although NSM displays a warning when you create this particular policy rule, it does not prevent its creation.
- 449045—When deleting the SRX family of devices, certain Java exception errors are logged into the file gproGDM.log of the GuiSvr error log directory.
- 452275—VLAN configurations are not applicable for SRX3400, SRX3600, SRX5600, and SRX5800 devices. However, the configuration editor and the quick configuration editor list the VLAN configurations.
- 458973—NSM displays validation errors under all occurrences of 'isis' node when the Junos OS Release 9.6 schema is applied. This issue is seen on all J Series and SRX Series devices.
- 460593—The system services RSH and Rlogin are not configurable from NSM.
- 461264—At times, an update on an SRX Series device fails with the error message **"Previous commit in progress**." This may happen when a previous commit is still being executed on the device in the background; for example, during an IDP policy compilation. For a workaround, see http://kb.juniper.net/KB16548. If the error is not due to an IDP policy compilation, the workaround is to add the device again.
- 477359—The private edit mode used in SRX Series clusters does not block NSM.
- 517276— NSM does not display logs for the backup device in an SRX Series virtual chassis in the Log viewer.
- 517284—IDP Detector Engine update does not work for both devices in an SRX Series virtual cluster.
- 519796—NSM does not display SRX Series virtual chassis details in Device Monitor.

Errata and Changes in Documentation for NSM Release 2012.2

The following section provides the documentation errata for this release.

Errata

- In the *Network and Security Manager Security Administration Guide*, the section on Viewing Additional Device Detail and Statistics is missing, including the information that this feature is supported only on ScreenOS devices.
- In the *Network and Security Manager API Guide*, the **Predefined Service Object and Customer Service Object** timeout formats are missing. While retrieving the timeout value of these objects using NSM API, the following format is displayed:
  - Predefined Service Object –**<timeout>7560</timeout>**
  - Customer Service Object –**<timeout><val>7560</val></timeout>**

NSM Documentation and Release Notes

For a list of related NSM documentation, see http://www.juniper.net/techpubs/software/management/security-manager/ .

If the information in the latest release notes differs from the information in the documentation, follow the *NSM Release Notes.*

To obtain the most current version of all Juniper Networks technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

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 https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

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.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service

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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://www2.juniper.net/kb/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

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 https://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 https://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**. 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 https://www.juniper.net/documentation/feedback/.

Revision History

January 14, 2013—Revision 1, NSM 2012.2

February 21, 2013—Revision 2, NSM 2012.2

April 16, 2013—Revision 3, NSM 2012.2

May 14, 2013—Revision 4, NSM 2012.2

June 20, 2013—Revision 5, NSM 2012.2

July 15, 2013—Revision 6, NSM 2012.2

August 12, 2013—Revision 7, NSM 2012.2

August 23, 2013—Revision 8, NSM 2012.2

September 13, 2013—Revision 9, NSM 2012.2

October 10, 2013—Revision 10, NSM 2012.2

November 13, 2013—Revision 11, NSM 2012.2

November 29, 2013—Revision 12, NSM 2012.2

December 12, 2013—Revision 13, NSM 2012.2

December 19, 2013—Revision 14, NSM 2012.2

February 4, 2014—Revision 15, NSM 2012.2

March 28, 2014—Revision 16, NSM 2012.2

April 9, 2014—Revision 17, NSM 2012.2

August 11, 2014—Revision 18, NSM 2012.2

September 30, 2014—Revision 19, NSM 2012.2

October 30, 2014—Revision 20, NSM 2012.2

November 20, 2014—Revision 21, NSM 2012.2

January 23, 2015—Revision 22, NSM 2012.2

March 17, 2015—Revision 23, NSM 2012.2

March 26, 2015—Revision 23, NSM 2012.2

April 27, 2015—Revision 24, NSM 2012.2

May 20, 2015—Revision 25, NSM 2012.2

July 01, 2015—Revision 26, NSM 2012.2

July 21, 2015—Revision 27, NSM 2012.2

October 07, 2015—Revision 28, NSM 2012.2

December 10, 2015—Revision 29, NSM 2012.2

January 14, 2016—Revision 30, NSM 2012.2

February 16, 2016—Revision 31, NSM 2012.2

June 16, 2016—Revision 32, NSM 2012.2

October 12, 2016—Revision 33, NSM 2012.2

January 12, 2017—Revision 34, NSM 2012.2

February 08, 2017—Revision 35, NSM 2012.2

November 07, 2017—Revision 36, NSM 2012.2

February 19, 2018—Revision 37, NSM 2012.2