



# NetScreen-Security Manager Release Notes

***Release 2006.1r2***  
***9-6-2006***

## ***Contents***

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Changes to Default Behavior on page 3
- 4 System Requirements on page 4
- 5 Upgrade Considerations on page 4
- 6 Addressed Issues on page 4
- 7 Known Issues on page 10
  - 7.1 Limitations of Features on page 10
  - 7.2 Known Issues on page 10
  - 7.3 Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager on page 18
- 8 Getting Help on page 20

## **Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 093-1825-000, Rev. C

## 1 Version Summary

---

Juniper Networks NetScreen-Security Manager is a comprehensive security management solution designed to manage device, network, and security configuration for integrated firewall, intrusion detection and prevention, and virtual private network (VPN) appliances, sensors, and systems.

## 2 New Features

---

The following is a list of new features and enhancements in the main release.

- **IDP Sensor Support**—Includes all IDP functions.
- **IDP Sensor/Cluster Monitoring**—NSM can now monitor the state and status of IDP Sensors and IDP Sensor clusters.
- **Standalone IDP Migration**—Migration of all configuration data and logs from IDP Manager to NSM. Upgrade of IDP Sensors to IDP 4.0.
- **Profiler**—Analyzes your network and automatically learns about the elements that comprise it, including hosts, peers (which host is talking to which other host), ports (non-IP protocols, TCP/UDP ports, RPC programs), and data from layer-7 that uniquely identifies hosts, applications, commands, users, and filenames.
- **Security Explorer**—The Security Explorer is a dynamic graphical tool that enables you to visualize network behavior based on profile, log, and report data. The main component is a touch graph that represents the relationships among data objects on multiple levels including hosts, services, and attacks. The Security Explorer also displays a Tool Area, Log Viewer, and Reports within contexts of the viewed graph.
- **IDP Policy Wizard**—Easily create a new IDP policy.
- **IDP Admin Role**—A new default role designed for IDP administrators, provides usability by showing IDP-relevant parts of UI only.
- **Audit Log Filtering and Sorting**—Provides a usable method for looking for changes made by a specific admin or changes made to a specific device.
- **View Logged in Admins**—Show name and contact information, idle time, and any locks currently held.
- **Enhanced RADIUS Support**—NSM role assignments via RADIUS now supported. NSM now supports two RADIUS servers.
- **Scalability**—100 IDP Sensors (20 of them running Profiler) with 2000 FW/VPN devices; or 6000 FW/VPN devices.

- **Recommended Attack Filter**—NSM now allows you to filter for Recommended attack objects when creating a custom group. Juniper Networks flags an attack as Recommended when it is currently circulating, represents a high risk of damage, or represents a common vulnerability. In addition, there is a new predefined attack group called Recommended which contains all attack objects with this flag on.

Custom attack objects may also be tagged as Recommended.

- **Out of Band Upgrade**—As part of the IDP Sensor migration process, you may upgrade IDP Sensors to 4.0 by loading the IDP 4.0 image directly on the Sensor. When the upgrade occurs, NSM will determine if the Sensor has already been upgraded. If it has not, the previous procedure will be followed, with NSM downloading the 4.0 image to the Sensor and having it execute the upgrade.
- **Dashboard**—Allows you to see your Destination Watchlist, Source WatchList, Top 10 Attacks all over past 1 hour, and device status.
- **New Predefined Log Views**—Under the Log Viewer node, you will now see three new sub-nodes: Backdoor, Scans, and Profiler. These predefined log views existed in IDP Manager and are convenient ways to view IDP-related logs.
- **New Attack Object Viewer/Editor**—The Attack Object viewer has been redesigned. Although predefined attack objects are still not editable, the Edit button in the viewer copies the object, then makes the copy editable in the view dialog. Use this same dialog to modify existing custom Attack Objects.
- **View Attacks by Service**—In the Policy Editor, see attacks within a rule grouped by their default service.
- **Policy Template Improvements**—IDP policy templates have been modified based on customer recommendations. Since IDP policies may be pushed to ISG or standalone IDP devices, the templates have a firewall rulebase by default. Standalone IDP Sensor ignore the firewall rulebase. Less commonly used rulebases are no longer part of the templates, but they can be easily added to any policy.
- **Audit Log Disk Space Management**—Logger can purge old entries before adding new ones to better manage disk space usage.
- **Block Logins**—Ability to block logins by IP address after specified number of consecutive failed attempts.

### 3 Changes to Default Behavior

---

- NetScreen-Security Manager now manages standalone IDP Sensors. The IDP Management Server and IDP UI cannot manage IDP 4.0 Sensors. See the IDP-NSM Migration Guide for a complete description of the changes.
- The Anomalies default log view is no longer available in NSM.

## 4 System Requirements

---

NetScreen-Security Manager 2006.1r2 requires one of the following operating systems:

- Red Hat ES/AS 3.0 with Update 5, 32-bit version only
- Red Hat ES/AS 4.0 with Update 1, 32-bit version only
- Solaris 8 or 9 with current recommended patches from Sun

Refer to the *NetScreen-Security Manager Installer Guide* for detailed installation requirements and procedures.

## 5 Upgrade Considerations

---

The follow items need to be taken into account when upgrading:

- If the Forward Support Schema update was applied to NSM 2006.1r1 to add support for ScreenOS 5.4, this Forward Support Schema update must be reapplied after upgrading to NSM 2006.1r2 release.

Reason: ScreenOS 5.4 introduced a new predefined service called SCTP. The Forward Support Schema update adds this new service definition in the NSM server configuration table called `service_table.nml`. After the upgrade to NSM 2006.1r2 this table is overwritten and this service is not part of the NSM 2006.1r2 default installation. This results in failure to start the NSM GUI server. Reapplying the Forward Support Schema update fixes this issue.

- If user “nsm” already exists, a shell needs to be defined for this user.

## 6 Addressed Issues

---

The following issues are addressed in this release:

### **Security Policies**

- **cs10416**—NSM added a trailing "/" to AV scan-mgr pattern-update-url, causing AV update failures.

### **Logs/Log Viewer/Log2Action**

- **cs7977/gl28440**—Max log count constraint appears not to work in Log Investigator. However, the number of logs shown on the Log Investigator result table includes the repeat count of every log that meets the filter criteria, even though only the number of logs traversed does not exceed the max log count.
- **cs9900**—log2action query limited to 100,000 records.
- **cs10546**—log2action --include-headers not aligned with CSV data.
- **cs10805**—Could not view packet data in logviewer for one subdomain.

- **cs11063**—Audit log did not display the difference in changes correctly. This release fixed the following issues in Audit log:
  - Audit log did not send a proper query when scrolling to the last entry.
  - Validation errors (red icons) appeared in the audit log display
  - Audit log did not display the difference when both the old and new values were explicitly set in the object (not as default)
  - Deleted items did not appear with a strikeout
- **gl28050**—SNMP logaction caused the other logactions (both rule- and domain-based) to get blocked if the /etc/hosts file didn't have an entry for the local NSM server host.
- **gl29112**—Documentation indicated incorrect path for log2action scripts.
- **gl29168**—Log-to-policy hyperlink does not work in migrated logs. Logs migrated from IDP lose the connection to the policy that generated them. Logs generated after the migration work as normal.

### **Management Servers**

- **cs9799**—GuiSvr crash with error Assertion...nsSetDbCache.c:4986.
- **cs9897**—NSM Add Many Devices did not work with split GUI and Device Servers
- **cs9985**—GUI Server failure when deleting a referring object.
- **cs10188**—tech-support.sh script added old files to archive, making archive unnecessarily large.
- **cs10313**—Status redirector issue caused Device Server to disconnect from GUI Server.
- **cs10341**—NSM DB locked for remote backup even after the backup is completed due to the number of open files that are still open.
- **cs10398**—GUI Server fails when the Job Manager output is corrupted.
- **cs10703**—Installation error when installing to HA combo boxes with shared disk.
- **cs10784**—In split server HA configuration, GUI Server failed over correctly but Device Server did not.
- **cs10791**—Running NSM as root and replication as a non-root user caused HA failover to fail due to incorrect permissions on PostgreSQL files.
- **cs10961**—GUI loses connection to GUI Server when running directives.

- **cs11051**—In a 4 server extended HA deployment on ES4, devSvr logWalker process core dumped a number of times, resulting in failure to connect to the SRS database.
- **gl29520**—Open PostgreSQL port (5432) on Device Server.

#### *IDP/DI*

- **cs10137**—Incorrect detector.so version stored in NSM.
- **cs10345**—NSM not able to set flow table values high enough.
- **cs10736**—Policy validation failed for an ISG-IDP policy.
- **cs10994**—"Get running config" returns just one line of output for ISG-IDP ScreenOS 5.4.
- **gl29222**—Backdoor rulebase only supports IDP pre-defined services, not ScreenOS pre-defined services.

#### *IDP Migration*

- **cs10218**—importIdpLogs.sh displays usage even though correct syntax was entered initially.
- **gl28825**—The following attacks show up as unNamed in log viewer after migration. These attacks have been deprecated, and the relevant signatures incorporated into different attack objects.

```

HTTP:STC:IMG:JPEG-HEADER-UF
HTTP:STC:MOZILLA:HOST-MAL-IDN
HTTP:STC:OUTLOOK:MAILTO-QUOT
HTTP:STC:IE:ADOBE-ACTIVEX
HTTP:STC:MOZILLA:RSS-SCRIPT-INJ
HTTP:OMNI:SRC-DISC
HTTP:CGI:SQL-INJECT
HTTP:IIS:EXAIR-DOS-1
HTTP:IIS:CODEBRWS-ASP
HTTP:NOVELL:NETBASIC-TRVRS
SMTP:OVERFLOW:SQRLMAIL-HDR-INJ
SMTP:MAL:DSHOW-BIGCHUNK-SMTP
IMAP:OVERFLOW:NETMAIL-CONT-OF
APP:DSHOW-BIGCHUNK-SMB
WORM:NACHI:INFECTION-PING
SMB:OF:PNP-OF
SMB:EXPLOIT:SMB-OF-0045
    
```

- **gl28938**—Policy push fails when there is heavy traffic on the IDP Sensor and the policy is large. Policy push and compilation take longer than the timeout value.

#### *Clusters/High Availability/NSRP*

- **cs9663**—NSM failed to support VSD-less cluster.

- **cs9698**—After AdjustOS was performed on cluster members, the cluster object itself still showed the old ScreenOS version.
- **cs9770**—Import of Cluster Member unsets Secondary NSM server MIP address.
- **cs10286**—Unable to set the weight for NSRP monitor.
- **cs10412**—Faulty network connection caused failover instead of causing a reconnect.
- **cs10608**—Null value caused failover when adding additional cluster member.

### ***Reporting***

- **cs10377**—guiSvrCli.sh report generation failed for time-based shared reports.

### ***Upgrade***

- **cs10174**—Internal Code name used with an upgrade on Linux platform.
- **cs10175**—Solaris only. Upgrade script did not indicate what version of NSM was running previously, and did not indicate what version of NSM will be installed.
- **cs10263**—Migrating Audit Logs failed during upgrade to 2006.1r1.
- **cs10626**—Policy migrated from Global Pro to NSM on Solaris used too many resources.
- **cs10986**—Device update does not update the MIP address of the secondary Device server IP Address when used in an extended mode.

### ***User Interface***

- **cs8981**—Warning displayed when RIP is enabled on a virtual router. However, the RIP config did get generated correctly and pushed to the device.
- **cs9954**—After text entry, policy comment field did not resize correctly.
- **cs9986**—If custom services with the same name existed in global and sub domains, could not add only one of them to a policy. Adding one added both.
- **cs10087**—RegEx search function produced inconsistent results across sections of the UI.
- **cs10109**—Ethernet utilization graph displayed unclear data.
- **cs10205**—javaw spikes to 100% cpu when selecting lot of attacks in device.
- **cs10293**—Custom reports listed in no particular order in GUI.
- **cs10626**—NSM UI failed to respond when managing multiple group address objects due to a memory leak.
- **cs10919**—Spelling mistake in the text when a validation is performed on a bulk-add directive.

**Installation**

- **cs10270**—System Update failed to install 3 packages on Solaris 8.
- **gl29700**—After an extended install, when adding the Device Server, you are not able to configure the ports 7800 and 7803.

**Monitoring**

- **cs9726**—Device Monitor did not sort by device name alphabetically.
- **cs9808**—VPN Monitor view did not retain sort order after a refresh.

**Objects**

- **cs9409**—NSM allowed user to create a custom service that was not valid.
- **cs10028**—NSM predefined service NBDS was TCP/138 instead of UDP/138.
- **cs10450**—Domain Admin could not delete address objects in 2006.1r1.

**Device Management**

- **cs8024**—The direction for an attack object was set as "any" when it was copied to a custom attack object.
- **cs8449**—Interfaces that should be able to be set to 10/100/1000 Mbps can only be set to 1000 Mbps when in cluster.
- **cs8502**—NSM by default sets the tunnel interface to route mode.
- **cs8943**—NSM imported an address in multicast subnet range as multicast group.
- **cs8981**—Warning displayed while enable RIP on 5xp with ScreenOS 5.0.
- **cs9575**—Incorrect license mode detected on SSG5.
- **cs9821**—Delta showed "unset av http trickling" for devices that did not have an AV license.
- **cs10012**—Null interface in routing table was not being imported.
- **cs10189**—Error when setting interface speed on ISG1000 built-in interfaces.
- **cs10245**—Cannot create VIP same-as-untrust on NS25/50.
- **cs10280**—High CPU when applying multi-cell policy.
- **cs10387/10611**—L2TP / XAUTH / Local User option missing from individual device management dialog.
- **cs10484**—NSM doesn't allow firmware upgrades for ISG1K/2K from ScreenOS 5.0.0r9.2 (non-IDP) to 5.0.0r10a.4 (IDP).

- **cs10536**—Deleting an access list from a VR causes NSM to try to delete it from several devices.
- **cs10755**—Validation error displayed when IP pools were configured under the DHCP Server.
- **cs10930**—CLI not being generated for a Null route.
- **gl29533**—NSM does not allow selecting two Phase1 proposals when the P1 proposals are in two different groups.
- **cs11053**—Could not create VIP same-as-untrust on SSG 520.
- **cs11110**—Supplemental CLI for cluster members & Template Operations did not work properly.

### **SRS**

- **cs8916**—SRS VPN throughput statistics showed anomalous high spike.
- **cs10207**—SRS VPN reports does not work for a VPN in a VSYS.
- **cs10342**—Unable to import VSYS into SRS admin console.
- **gl29380**—NS5200 shown in SRS as standalone instead of cluster.

### **VSYS**

- **cs8762**—DIPs defined in VSYS did not appear in global DIP settings.
- **cs9684**—Import of device with VSYS doesn't set OSPF on shared interface.
- **cs9751**—NSM unset “int ip manageable” even if the checkbox is checked.
- **cs10285**—Incorrect routes were being generated with a metric 0 on a vsys.
- **cs10927**—Unable to set secondary IP on VSYS sub-interface.
- **cs11151**—When trying to create a destination route for a NS5400 vsys device running ScreenOS 5.4, you were not able to select an interface.

### **VPN**

- **cs10091**—VPN Monitor inaccurately displayed VPN as up.
- **cs10265**—Adding a VPN rule in the Policy Manager used to take a long time when too many address book entries are present.
- **cs10625**—Adding a VPN takes a very long time.
- **cs10717**—NSM did not allow setting different Diffie-Helman group for Phase 1 proposals.

## 7 Known Issues

---

This section describes known issues with the current release.

“Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

“Known Issues” describes deviations from intended product behavior in IDP as identified by Juniper Test Technologies through their verification procedures. Whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

### 7.1 *Limitations of Features*

- None.

### 7.2 *Known Issues*

The following are known deficiencies at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:”.

#### *Installation*

- **gl29683**—Install script prompts for the port number of GUI Server. The port number cannot be changed and should not be prompted.
- **gl30003**—During migration from NetScreen-Global Pro to NSM 2005.3r2, Rule IDs are duplicated.
- **gl30086**—Forward Support Install script should fail if no payload is found.
- **gl27621**—With 2005.3r1, after installing the SSG schema update, when a SSG device is added, warning/error messages appear that are misleading.
- **gl29580**—The archiveDomainVersions.sh will not work on Solaris because there is a bug in the script specific to the "find" command syntax on solaris.

#### *Upgrade*

- **cs11172**—Upgrade fails. Needed 2 GB in /tmp.
- **gl29704**—NSM 2006.1r1 Forward Support Schema update script is not HA aware.
- **cs6113**—If an upgrade from one release of NetScreen-Security Manager to another does not include version migration, it is impossible to migrate any versions in a future upgrade.

W/A: You must delete domain versions after any upgrade where they are not migrated.

- **cs10177**—Upgrade changes the home directory for nsm user if /bin/sh is not default shell for user nsm.

- **cs11005**—Forward Support Install script is not HA-Shared Disk aware.
- **cs11172**—NSM upgrade 2005.3r2 -> 2006.1 failed due to lack of /tmp disk space.

W/A: Upgrade requires at least 2 GB of space in /tmp.

#### ***Import/Update/Export***

- **cs9836**—Global Pro export to NSM duplicates address groups.
- **cs10125**—Import of the device fails if keyword "admin" used in the config.
- **gl29790**—It is understood that multiple MIP's per rule is not a supported configuration for 5.0 devices, however once configured in the firewall policy, NSM fails during device update with cryptic job manager output.
- **gl30090**—While the policy update happens from NSM 2006.1 for ISG-1000 Screen OS 5.3.0en2.0, errorlog on the Device Server gproDDM.log appears: Error invoking function: CT\_LINK\_NEGOTIATION([Ljava.lang.Object;@11f23e5, however, the policy update happens fine.
- **gl29648**—If you update a device and the updated is unsuccessful, the Audit Log Viewer "device" value is NULL.
- **gl25885**—NSM errors when updating ISG to bring a link down.

#### ***Security Policies***

- **cs6937**—Rule grouping is only available for zone-based rulebases.
- **gl26972**—A predefined group with no members other than a custom attack generates a warning in a policy rule indicating it is empty.
- **gl27120**—Not all configured log actions appear enabled in the main rule view.  
W/A: Open Notification dialogs to see which log actions are configured.
- **gl30094**—Adding a rule after a filter is applied reverts to default zones.

#### ***IDP/DI***

- **cs10085**—Unable to set DI attack DB URL in NSM if user types in URL manually.
- **cs10190**—After upgrading from 2005.3r1 to 2006.1, could not create new dynamic attack groups for IDP.  
W/A: Download new attack DB, then create groups.
- **cs10259**—Last Modified Date Filter for Dynamic Group may be inaccurate.
- **cs10317**—UI prepends "file://" to any attack signature reference starting with "ftp://."
- **cs10762**—Attack DB update for SSG device displays warning.

- **cs10789**—NSM GUI errors when handling filtered custom IDP attack group.
- **gl28770**—Profiler permitted objects Apply button is not enabled after edit. After a permitted object used by the Violation Viewer is edited, the Apply button is not enabled.

W/A: Click on the Refresh icon button to refresh the Violation Viewer.

- **gl29021**—DI pack and detector versions not displayed correctly after attack object download. Sometimes after updating the attack object database, the UI does not show detector versions and DI signature pack versions correctly.

W/A: Log out and log back in.

- **gl29042**—IDP clusters in 3rd party HA configuration show status of Failed at all times. IDP clusters in stand-alone HA mode show correct status.
- **gl29051**—Policy push failed while during Profiler restart.

W/A: Do not push policies while Profiler is restarting

- **gl29074**—Retry Push feature doesn't work for IDP devices in NSM.
- **gl29223**—Secondary NSM server is not configured on the IDP Sensor when the device is added to NSM. Sensor disconnects from NSM if primary server fails over to backup.

W/A: Use ACM to specify secondary server for each Sensor.

- **gl29661**—idp4.0r2 not displayed in list of platforms after attack object database update.

W/A: Log out of NSM, and then log back in.

#### ***Log Viewer/Log Investigator/Audit Logs***

- **cs9900**—NSM log2action query can retrieve a maximum of 100k records.

W/A: Contact JTAC for workaround.

- **gl28807**—The log-to-policy jump is not disabled in the GUI for logs where it is not relevant, such as logs in the screen, config, and alarm categories.
- **gl28181**—Some audit logs for read-only events appear to be duplicates. In actuality, they are separate events because in some cases, the same command impacts more than one domain.
- **cs8075**—Log files became corrupted.
- **cs9990**—Audit Log does not show the action performed (modify/delete).
- **gl28698**—Depending on how the Log/Count configuration window is accessed, two different views can be displayed.

- **gl29398**—When filtering by "device group" under Log Viewer for the devices column, no logs are returned from the filter.
- **gl30024**—When mouse over the "rule #" in LogViewer (on All Field window), it should showing the corresponding rule number. This works only for first one, the rest will be the same as the first one which is incorrect.
- **gl30391**—Some device UI nodes are missing in the audit log display.
- **gl30394**—Audit log does not display the difference in changes for VPNs and templates.
- **gl30397**—Some data values do not appear in the audit log.

### **Reporting**

- **cs9473**—devSvrCli.sh --log2action can take longer to filter and write out the file than it takes to run the command. So, it can appear that results of the command are inconsistent.
- **cs10663**—Devices not reporting Ethernet, flow, policy or protocol statistics.
- **gl28521**—Scheduled reports run on the global domain do not include logs from subdomains.
- **gl30205**—Report exported by email script shows incorrect dates (alternative days only).
- **gl30208**—Scheduled report did not work for reports filtered by cluster.

### **Clusters/NSRP**

- **cs8021**—Cluster objects do not show updated minor OS version running on a cluster that has been upgraded.
- **cs8219**—Incorrect Device Server IP shown in the configuration.
- **cs8448**—Error when setting speed/duplex for a mini-Gbit card on an ISG 1000 in a cluster.
- **cs9029**—NSM firmware upgrade of cluster should abort on failure to upgrade a member.
- **cs9664**—NSM does not support local sub interfaces in VSD-less cluster.
- **cs10692**—NSM not setting the primary interface of a redundant interface.
- **gl30207**—The sub-intf cli tag is not generated on VSD-less NSRP cluster.

### **VPN**

- **cs5353**—Config Sync does not report changes on VPN Manager.
- **cs7143**—The preshared key for a VPN is displayed in clear text. There should be a way to encrypt it.

- **cs8585**—VPN Monitor displays wrong information for A/P cluster. VPNs between passive devices in NSRP clusters appear as "down" in VPN Monitor.
- **cs10015**—NSM couldn't remove redundant sub-interface.
- **cs10108**—When logged in as a non-superuser, password masking code masks incorrect word. Instead of seeing:

```
set ike p1-proposal "kbc-phase1" preshare group2 esp aes128 sha-1 hour 24
```

the following appears:

```
set ike p1-proposal "kbc-phase1" preshare ***** esp aes128 sha-1 hour 24
```

- **cs10898**—Change in VPN unsets the complete VPN and recreates it.

### **SRS**

- **cs8643**—Some VPN statistics in SRS displays a list of devices instead of a list of device groups.
- **cs10344**—SRS install fails when using the option of an upgrade from HRS.

### **User Interface**

- **cs8015**—Custom service objects do not sort correctly in non-ICMP columns.
- **cs8215**—Static routes are displayed with additional blank lines.
- **cs8619**—search function in Security Policy "sticking."
- **cs8635**—Find IP function does not work in large subdomains.
- **cs8704**—After deleting a subdomain while logged in as a non-superuser, all other domains disappear until after new login.
- **cs9450**—NSM GUI hangs when viewing audit logs with rb\_firewall reference. When an audit logs entry contains the firewall rulebase, double-clicking on the entry hangs the GUI.
- **cs8344**—An "Internal Error Occurred" error message appeared during rule edit.
- **cs9158**—Rule groups do not get automatically expanded when filtered.
- **cs9648**—Objects no longer listed individually once they are added to a group.
- **cs10111**—Active Sessions does not list active sessions in a consistent manner due to 5-minute device polling interval.
- **cs10178**—If you view a policy in Audit Log Viewer, then add a new rule, the new rule does not display.
- **cs10390**—CLI not being generated when a route is defined to use a null interface.
- **cs10676**—Copy/Paste does not work in the Security Device List view.

- **gl29433**—The window title under device monitor for "device detail status" shows as \$deviceobjsvr.

### **Security Updates**

- **gl30163**—Update Attack DB not working in NSM 2006.1r2 for ISG with IDP devices running ScreenOS 5.0r10a.  
  
W/A: Upgrade ISG device to ScreenOS 5.0r10b or 5.4.
- **gl29045**—Attack db rollback to older version (from 577 to 575) failed.
- **gl29074**—Retry Push feature won't work for IDP devices in NSM.
- **gl28460**—GuiSvrCli Retry option does not work. If a Scheduled Security Update fails due to a device being offline, the retry update function (if used) does not attempt the update when the device reconnects.
- **gl29932**—After signature download some predefined groups do not show members.

### **IDP Migration**

- **gl29701**—Negated objects in Traffic Anomalies do not migrate to NSM properly.
- **gl29141**—IDP Migration fails on NSM GUI Server due to permission issues.  
  
W/A: Change the permissions of the /var files on both GUI Servers to rwxrwxrwx before migrating, then change the permissions back after migrating. Refer to the *IDP-NetScreen-Security Manager Migration Guide* for complete procedures.
- **gl28186**—IDP sensor does not appear after IDP migration. Sometimes a sensor does not show up in the device list after it has been migrated.  
  
W/A: Log out of the GUI, then log back in. The sensor will appear.
- **gl29695**—After migration, custom attack groups have "CS:" appended to them.

### **VSYS**

- **cs9585**—NSM VSYS cluster doesn't show all static routes in the GUI. When VSYS are in different subdomains and have their local routes in the same shared vrouter, some of the local routes do not show in subdomains.  
  
W/A: Call JTAC for assistance.
- **cs10393**—IP address overlap error after importing two vsys using same subnet. Two different virtual routes are in use, so the overlap is OK. However, error message appears anyway because both are using the same vr.
- **cs10669**—Though tunnel interfaces are never shared, and so not included in the root template for VSYS, routes that use tunnel interface *are* included in the root template and can show in VSYS. This causes validation errors.

- **cs10964**—Cannot unset netmask from VSYS interface.
- **gl30211**—OSPF should not be available in VSYS when interface is in shared untrust-vr with ospf enabled.
- **gl24654**—"Auto-export route to untrust-vr" option on Untrust-VR should not appear.

#### **Management Servers**

- **cs9499**—archiveDomainVersions.sh is not valid for HA environment.
- **gl24664**—Version number for haSvr version is not consistent.

#### **Device Configuration/Management**

- **cs2589**—Service objects can be sent to devices that do not support them.
- **cs3723**—Unable to create a configlet for a device in transparent mode.
- **cs8015**—Custom service objects do not sort correctly based on the non-ICMP column.
- **cs8345**—ssh authentication is checked by default even when disabled in template.
- **cs8411**—NSM cannot move zone untrust in untrust-vr if using DHCP or PPPOE. When modeling or RMA/activating a firewall that has the untrust zone into the untrust-vr and the untrust interface has a dynamic ip address with DHCP or PPPOE, it will fail to update the device after first connection with NSM.

W/A: From NSM, disable DHCP client on untrust interface, then update the device. Once it's done, enable DHCP client on untrust interface, update device again.

- **cs8537**—NSM should display a warning for IKE dn user with all wildcards.
- **cs8766**—Unable to use a custom service object in the filter when creating a dynamic group.
- **cs8785**—Failed to upgrade firmware from 4.0.x to 5.x via NSM.
- **cs8852**—Statistics fail when an incorrect serial is used with bulk-add.
- **cs9178**—NSM does not send needed unset commands for adjusting access list.
- **cs9327**—NSM failed to connect to firewall for interface using untrust-vr.
- **cs9664**—NSM does not support local sub interfaces in vsd-less cluster.
- **cs10012**—The option for null interface in the Routing Table is missing in NSM.

W/A: Configure the null interface via CLI on the device. Import the device, edit the imported route, and uncheck the "Gateway Tracking On" check box. Then select "null" as the interface. Save. After that, device and server are in sync and device update will not change this route.

- **cs10014**—Setting a custom pre-defined service timeout at the device level generates a failure when updating the device in NSM.
- **cs10483**—SNMP sysname overrides hostname in device templates.
- **cs10716**—NSM directive doesn't set RIP advertise default route option.
- **cs10725**—If you configure a route map in NSM then when inside the dynamic routing protocols section when you go to select a route map the "none" option is no longer available in the drop-down menu.
- **cs10988**—Unable to define a route to null interface using a template.
- **cs11017**—Delta config shows some differences in AV settings after upgrade to 5.4.
- **gl25190**—If an aggregate interface with a single member has that member replaced, an update failure will occur.

W/A: First add the second member and update the device. Then you can remove the first member without issues.

- **gl26079**—There is an issue with enabling PIM-SM and IGMP together on an interface. In some cases, when you enable IGMP, PIM-SM settings will be disabled.

W/A: Unset IGMP (Uncheck "Enable", Select IGMP type "None"), save and then return to configure PIM-SM settings.

- **gl28681**—Update fails if you unset multilink interface encapsulation from NSM.

W/A: When changing the encap setting to none, change the previous WAN fields to default values. This will prevent device update failure.

- **gl28734**—When changing encapsulation type, NSM does not unset settings configured for earlier encapsulation type.
- **gl29110**—Firmware must be loaded in subdomain in order to perform firmware update in subdomain.
- **gl30095**—NSM 2006.1 service\_table.nml lists two services for smtp: SMTP (black) and smtp (red).
- **gl29900**—The definition of DNS services under predefined services in NSM2006r1 is incorrect. The source port range for both dns tcp and dns udp is given as 53 to 53. When using any of these services in a policy created in NSM and updating the device, the result is a non-working policy due to wrong definition of source port range.

- **gl30002**—MIP validation error for a 5GT-WLAN "nsm will not let me set mip same as untrust ip on 5gt". It works with home/work mode, but fails with trust/untrust mode.
- **cs11154**—In both NSM 2005.3r2 and NSM 2006.1 you are not able to modify the predefined service timeout objects.

#### **RADIUS**

- **cs5014**—Initial RADIUS configuration stores password in cleartext, does not allow timeout or port value change.

### **7.3 Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager**

The following are known issue in ScreenOS 5.x that specifically affects this release of NetScreen-Security Manager:

- **os55015**—While using NetScreen-Security Manager with DI enabled on an NS-500 device running ScreenOS 5.3, you may experience issues when downloading configurations larger than 1.7MB.
- **cs7488**—NetScreen-Security Manager reports an error when trying to set link-down an interface on an ISG 2000 device.
- **cs3723**—It is not possible to create a configlet for a device in transparent mode.
- **os53891**—When upgrading a device from ScreenOS 5.0r10 and lower to ScreenOS 5.3, devices crash.
- **os53871**—Devices running ScreenOS 5.3 may crash when generating Deep Inspection logs.
- **os53854**—Wireless interface zone settings on devices running ScreenOS 5.3 are always displayed as "none" in the NetScreen-Security Manager UI.
- **os53710**—It is not possible to set the bandwidth on interfaces for a VSYS in ScreenOS 5.3.
- **os53595**—If you change the Device Server IP address, devices running ScreenOS 5.3 are not able to connect.

W/A: Perform an "RMA Device" and "Activate Device" workflow to continue managing the device.

- **os53312**—You can not nest local user groups in ScreenOS 5.3.
- **os53035**—NSRD in transparent mode is not functional in ScreenOS 5.3.
- **os48987**—Using NetScreen-Security Manager to upgrade security devices running ScreenOS 5.0.0 over a slow network connection (if the image download takes over 5 minutes), occasionally causes updates to time out.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **os45418/48460**—Devices are not able to save the key used to connect to the NetScreen-Security Manager Device Server. This causes the NSM agent on the security device to have to re-negotiate the key every time the security device restarts. The key re-negotiation process can take up to 15 seconds. One side effect of this issue is that when you restart the Device Server, this will also cause key renegotiation for all other security devices running it manages. This may cause system performance degradation that then affects the management of all security devices.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **os43001**—If you use NetScreen-Security Manager to upgrade the firmware on a device from ScreenOS 5.0.0 to ScreenOS 5.1, the security device crashes.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

The table below describes specific releases of ScreenOS that resolve the issues referenced above, or provides other workaround information:

<b>Issue</b>	<b>5.0.0</b>	<b>5.0.0 r9 for 5000 M2</b>	<b>5.0.0-GPRS.r8.5</b>	<b>5.0.0 WLAN</b>	<b>5.0.0 r9 for ISG 1000/ISG 2000</b>	<b>5.0.0IDP1</b>
48987	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2
45418/ 48460	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2
43001	5.0.0 r10	5.2	5.2	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2

## 8 Getting Help

---

For more assistance with Juniper Networks products, visit:

[www.juniper.net/support](http://www.juniper.net/support)

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your NetScreen device with Juniper Networks at the above web address.

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.  
ATTN: General Counsel  
1194 N. Mathilda Ave.  
Sunnyvale, CA 94089  
U.S.A.

[www.juniper.net](http://www.juniper.net)

**Writer:** Mark Schlagenhauf



