



# NetScreen-Security Manager Release Notes

*Release 2005.3*  
*2-15-06*

## *Contents*

- 1 “Version Summary” on page 2
- 2 “New Features” on page 2
- 3 “System Requirements” on page 4
- 4 “Changes to Default Behavior” on page 4
- 5 “Addressed Issues” on page 4
- 6 “Known Issues” on page 12
  - 6.1 “Limitations of Features” on page 13
  - 6.2 “Compatibility Issues” on page 13
  - 6.3 “Known Issues” on page 13
  - 6.4 “Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager 2005.3” on page 17
- 7 “Getting Help” on page 19

## **Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

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

Part Number: 093-1747-000 Rev C

## 1 Version Summary

---

Juniper Networks NetScreen-Security Manager 2005.3 is a comprehensive security management solution designed to manage device, network, and security configuration for integrated firewall and virtual private network (VPN) appliances and systems.

## 2 New Features

---

The following is a partial list of new features and enhancements in this release:

- **Support for ScreenOS 5.3**—You can now manage Juniper Networks security devices running ScreenOS 5.3. This include the following new features:
  - QOS/Virtual Interface Enhancements
  - 10-VLAN on NS-5GT Trust-Untrust Mode Support
  - Dual-DMZ Port Mode on the NS-5GT
  - Source-Based Routing (SBR)/Source Interface-Based Routing (SIBR) with Next-Hop as Virtual Router Enhancements
  - Trial License Keys—Install a Trial License Key enabling you to install a key on a device running ScreenOS 5.3 to use subscription-based features on a trial basis.
  - Enhanced Deep Inspection—In ScreenOS 5.3.0, Deep Inspection (DI) signatures are optimized into four signature packs for specific threat coverage and desired network deployment. This approach is ideal because of the limited device memory and increased protocol support. Refer to the ScreenOS 5.3r1 Release Notes for more information.
  - Enhanced Certificate Support—Generated certificates now support Domain Component (DC =) entries.
  - Enhanced Antivirus Support—Antivirus settings can be created and applied at the template level. Scanning is configurable based on application protocol, file extension/mime type, and compression level. Email notifications of found viruses is supported.
  - Antispam Capabilities—Netscreen-Security Manager now supports whitelist/blacklist antispam capabilities. Emails can be blocked or tagged based on email ID, hostname, domain name, or IP address.
  - BGP Soft Reconfiguration—A dynamic inbound soft reset is used to generate inbound updates of a routing table from a peer. An outbound soft reset is used to send a new set of updates to a peer.

- Merge Dial Features—Added a new Route failover option. When the Route option is selected, NetScreen-Security Manager activates the Virtual Router IP Address and Network Mask fields to specify the route to be used for failover monitoring. In addition, a validation condition needs to be added to check that the entered IP/Mask corresponds to an actual route on the specified virtual router.
- ALG Enhancements for VoIP—Enhances SIP Settings for ALG configuration as well as adds H.323 settings and MGCP settings.
- Enhanced Certificate Support—Allows certificate with DC in certificate DN to be used for dialup user IKE ID selection.
- Juniper Networks Infranet Controller Support—A new setting called a “Infranet Settings” now appears in the Device Manager enabling you to configure security devices to work with Juniper Networks Infranet Controllers. You can use Infranet Controllers to segregate your network based on user privileges as well as the security level of the user’s system.
- **Forward Support of Future ScreenOS Releases**—Use NetScreen-Security Manager 2005.3 to install a schema patch enabling you to manage devices running future versions of ScreenOS. For some new ScreenOS commands, you can use the Supplemental CLI screen to configure security devices running future versions of ScreenOS. Supplemental CLI is supported for ScreenOS 5.1 and higher.
- **Rule-Based Log Actions**—You can now configure log actions (i.e., Run Script, Send Email, Syslog Messages, SNMP Trap, Write CSV, Write XML) on a per rule basis within a security policy.
- **Domain-Based Log Actions**—A new tree node called “Action Manager” appears in the UI enabling you to configure log actions and criteria for device logs on a per domain basis.
- **Simplified Logs**—Using the Log Viewer, you can now view specific log entries describing device connect and disconnect events.
- **Viewing and Monitoring Devices from the Global Domain**—A new column called “Domain” appears in the Realtime Monitor (Device Monitor, VPN Monitor and NSRP Monitor) enabling you to monitor security devices across all domains.
- **Enhanced Template Administration**—The Template Operations dialog provides sophisticated template administration capabilities. It has the following capabilities: assign one or more templates to one or more devices, remove one or more templates from one or more devices, validate one or more templates against one or more devices, either during an assignment or as a standalone action, override existing values on the device with values in the template, report template values that are irrelevant to the indicated devices and report values that conflict between two or more indicated templates.
- **Multiple MIP Support**—Multiple MIPs can be added to the Device Server. When a device is added, the NetScreen-Security Manager administrator has the choice of selecting the desired MIP for each device.

- **Policy Filter Tool**—This tool provides the ability to filter policy rules based on one or more filter conditions specified for rule attributes. One filter can contain several filter conditions for different attributes. The filter only applies to the currently selected rulebase and does not affect other open clients. The filter results are displayed in the same rulebase. Rules that do not match filter conditions are hidden. In the firewall rulebase only open rule groups are filtered. When a filter is set and a closed rule group is expanded, only rules that match the filter will be displayed in the group.
- **Red Hat Enterprise Linux (ES/AS) 3.0 and 4.0**—NetScreen-Security Manager 2005.3 is now supported on Red Hat Enterprise Linux (ES/AS) 3.0 and 4.0.

### 3 System Requirements

---

NetScreen-Security Manager 2005.3 no longer provides support for Red Hat Linux 8 or 9. If you want to install NetScreen-Security Manager 2005.3, you must install or upgrade the operating system to either Red Hat Enterprise Linux 3 or 4, before installing or upgrading to NetScreen-Security Manager 2005.3.

The NetScreen-Security Manager 2005.3 system update utility is compatible with Red Hat Enterprise Linux 3.0 Update 5 and Red Hat Enterprise Linux 4.0 Update 1.

### 4 Changes to Default Behavior

---

- The `rsynctimeout` value is changed. In previous releases of NetScreen-Security Manager, the timeout was calculated as follows:
  - for local backup, it was 1/10 of the value configured;
  - for HA replication and remote replication, it was 4/10 of the value configured

The NetScreen-Security Manager upgrade process from previous releases to NetScreen-Security Manager 2005.3 will modify the `rsynctimeout` to the correct value.

### 5 Addressed Issues

---

This section describes addressed issues in the current release:

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

The following are addressed issues with Import/Update in this release of NetScreen-Security Manager:

- **7351**—Re-import of a device failed to deduplicate objects that differed only in the comments field.
- **7281**—Import and update of cluster members was not allowed from the right click menu

- **7268**—Updates involving VPN policies sometimes failed if a device or address object was deleted that was referenced in the policy.
- **7191**—NetScreen-Security Manager attempted to set an incorrect zone name on a device in transparent mode causing an update failure.
- **7104**—Policy export sometimes did not include global rules.
- **6908**—The import menu available on right-clicking on a device was sometimes disabled when the device was in the UP and Import Needed state.
- **6701**—After importing a device the policy in an associated template was overwritten, even if it was identical to the policy on the device.
- **5343**—Updating a config to a device failed when a single policy has more than 1 MIP defined.

### ***Role-Based Administration***

The following are addressed issues with role-based administration in this release of NetScreen-Security Manager:

- **7522**—When you log in as a non-super user, and made changes to options under preferences, these values did not get saved after logging off and logging back in.
- **7066**—Admins other than super were not able to save their preferences.
- **6780**—The global zone should be mapped to global-VSYSNAME address setting functionality.
- **4071**—If a root device was defined in the global domain, admins with access only to a subdomain could not see shared interfaces in VSYS devices defined in the subdomain.

### ***Directives***

The following are addressed issues with Directives in this release of NetScreen-Security Manager:

- **7026/6702**—Some device directives would fail at due to NetScreen-Security Manager server processes starting before the configuration database was fully ready.
- **7017**—The Update Device directive did not push disabled rules to the device.
- **6954**—Directives including the Delta Config Summary, displayed errors if run on multiple devices at once.
- **5843**—Directives issued on clustered or grouped devices had incorrect percentage completion reported in the Job Manager.

### **Security Policies**

The following are addressed issues with security policies in this release of NetScreen-Security Manager:

- **7798**—A policy was created with zone exceptions for a specific device. When the policy was pushed, it was pushed with the default zones, not the zone exceptions.
- **7511**—The comments field for rule groups was mistakenly set as required. This prevented a name change to the rule group.
- **7415**—The UI reloaded data from the NetScreen-Security Manager configuration database when an IDP rulebase was viewed or modified. This resulted in an unnecessary increase in memory usage on the server.
- **7330**—Find usage did not display accurate policy rule numbers.
- **7317**—When a service object was added to a policy rule, a list of individual objects was not visible outside the object groups.
- **7243**—Use of the "Find Usage" command on an address object did not display the name of the rule group that the object is used in.
- **7022**—The find usage function did not clearly display the name and group of the referring rule.
- **6729**—Policy assignment through a template should not have been overridden by import.
- **6638**—When a policy was defined with an "SMTP" service object, an update to a ScreenOS 5.0 service failed. This service is available for ScreenOS 5.1 devices and above. Policy Manager should display a warning message when an SMTP service object is selected and the associated policy assigned to a ScreenOS 5.0 device.
- **6530**—When a rule was defined with Destination NAT, a warning was displayed as follows: "Destination NAT Options are not available on 4.0 devices. Will be trimmed before an Update Device". This should not be displayed for ScreenOS 5.x devices.
- **6135**—The sizing of policies in the Policy Manager was not consistent.
- **6100**—It was not possible to delete all rules in a rulebase with a single command or ungroup all rules in a rulebase with a single command.

### **Log Viewer**

The following are addressed issues with the Log Viewer in this release of NetScreen-Security Manager:

- **7977**—The time received filter in the Log Viewer did not function correctly.
- **7621**—Duplicate log entries existed in the exported CSV file from the Log Viewer.

- **7366**—Some data that was present in the Log Viewer failed to propagate correctly to reports.
- **6950**—Custom views and Preferences in the Log Viewer were not saved for users other than the super user.
- **5528**—The time received filter in the Log Investigator had an inconsistent behavior.

### **Logging**

The following are addressed issues with logging in this release of NetScreen-Security Manager:

- **7978**—Log database indexing did not function correctly for large log volumes.
- **7147**—The log database was in an inconsistent state due to an inaccurate count of number of logs per day.
- **7025**—Automated log purge was launched when sufficient disk space was still available.
- **6863**—When a device was activated, traffic logging was automatically enabled. Under a heavy traffic load, management connectivity to the device may be lost.
- **6906**—Incorrect use of angle brackets caused invalid XML output for XML log actions.
- **6926**—NetScreen-Security Manager did not push a loopback group assignment when the assigned interface was a VSI.
- **6235**—Log filters did not save netmask properly

### **Report Manager**

The following are addressed issues with the Report Manager in this release of NetScreen-Security Manager:

- **7148**—Report Manager display of time scale was inconsistent.
- **7008**—NetScreen-Security Manager gave a "Too many keys exceeded" error while generating reports.
- **6982**—Related options in report settings caused updates to fail on devices running ScreenOS 4.x.
- **5784**—The troubleshooting window should be in a more accessible location and have an admin activity associated with it.

### **Monitoring**

The following are addressed issues with monitoring in this release of NetScreen-Security Manager:

- **7699**—Default IKE Monitoring setting was "Please Select" instead of "None".

- **6975**—The device serial number sometimes was not saved correctly, causing the "To Hostname" field to be blank in the VPN Monitor.
- **6956**—The session utilization graph in the Realtime Monitor always showed zero.
- **6728**—In the Server Monitor, total memory used and physical memory used readings did not match the output of the top command on the server.
- **6769**—Using templates, it was possible to create a mgt-vr vrouter, but it was not possible to assign it to the management zone.
- **6860**—It was not possible to edit IP address fields for interfaces in the management zone.

### **NSRP**

The following are addressed issues with NSRP in this release of NetScreen-Security Manager:

- **8019**—Enabling OSPF on a cluster displayed a false error in a modeled device.
- **7934**—When adding a route on the trust-vr, a NullPointerException was displayed.
- **7547**—NetScreen-Security Manager only accepted 14 character NSRP encryption password when the ScreenOS limit is 15.
- **6927**—It was not possible to change the vr binding for a zone in a cluster.
- **6935**—Removal of a template with a RIP configuration from a device did not cause this configuration to be unset on an update to the device.

### **VPN**

The following are addressed issues with VPNs in this release of NetScreen-Security Manager:

- **7925**—A policy had a number of rule groups. The device cluster this policy was assigned to had manual VPNs configured. When any of the VPNs were deleted, all the rules within the rule groups were removed as well.
- **7706**—You could not create the tunnel.1 interface with VPN Manager for two VSYS on the same device.
- **7719**—When creating a VPN in VPN Manager with 1 main and 2 branches, creation of a different preshared key from the main to each branch failed.
- **7572**—When the preshared key is changed in VPN Manager, the change did not get sent to the device during an update.
- **6966**—The VPN Manager incorrectly generated dial-backup VPNs.

### **User Interface**

The following are addressed issues with the User Interface in this release of NetScreen-Security Manager:

- **7779**—The UI did not always display all services and addresses configured in a policy rule view.
- **7836**—When using the policy merge tool to merge a policy with a service group, the merge failed.
- **6318**—A preference to disable variable row height was needed for UI performance.
- **6123**—You could not enter some characters in the UI using a Japanese language keyboard.
- **6279**—It was not possible to run "Adjust OS Version" if the device username, ip address and password were not available

### **Installation**

The following are addressed issues with Installation in this release of NetScreen-Security Manager:

- **7307**—Permission settings in the /var/sadm/install/contents file in Solaris were inconsistent after installing NetScreen-Security Manager.
- **6771**—A fresh install removed the dbbackup directory without warning.
- **6648**—There was a memory leak in java processes on the management system server installed on Solaris.
- **6313**—The NetScreen-Security Manager installer should only check for the presence of a minimum version of rpm instead of an exact match.
- **6418**—The add device workflow led users to activate a device while the device was open for edit. This caused the serial number of the device to fail to be inserted into the configuration database.
- **6435**—Installing the management system failed if the installer file was copied in a directory that had a space as part of its filename.
- **6449**—The gzip path is hard coded in the management system installation script.

### **Upgrade**

The following are addressed issues with upgrading in this release of NetScreen-Security Manager:

- **7398**—NetScreen-Security Manager upgrade failed due to the presence of UTF-8 characters in the configuration database.

- **6952**—Upgrade from NetScreen-Security Manager 2004 FP3r1 to NetScreen-Security Manager 2005.1 introduced some inconsistencies in the attack tables in the database.
- **6792**—Upgrade performed some redundant backup functions which resulted in performance issues of the upgrade itself.
- **6134**—It was not possible to upgrade NS-HSC devices.
- **5557**—"Hello Interval", "Reconnect", "Threshold" for a VPN gateway were not set to nonzero values after upgrade from NetScreen-Security Manager 2004 FP2r3 to NetScreen-Security Manager 2004 FP3r2.

### **Management System**

The following are addressed issues with the management system in this release of NetScreen-Security Manager:

- **7938**—Minor database inconsistency caused the guiSvrManager process to stop.
- **7707**—GUI Server startup was sluggish due to redundant file checking.
- **6909**—The "replace with" feature caused inconsistencies in the database causing the guiSvrManager process to stop.
- **5364**—Memory issues found in the Data Collector process caused loss of connectivity to NetScreen-Security Manager.
- **5271**—An error was displayed indicating that you need to enter Server's IP address, otherwise NetScreen-Security Manager was not able to manage the device. This was true only for devices running ScreenOS 4.x, and was not true for devices running ScreenOS 5.x.
- **4999**—You could only run java processes with root as the owner on the NetScreen-Security Manager management system.

### **Performance**

The following are addressed issues with performance in this release of NetScreen-Security Manager:

- **6603**—There were performance issues when dismissing the "find usage" dialog.
- **6609**—"Get License Key" output displayed DI where it should display IDP.
- **6616**—SNMP alerts contained commas making it difficult to parse
- **6698**—Deleting an address object from a policy rule sometimes caused only one rule to remain in the associated rule group.

### **Migration**

The following are addressed issues with migration in this release of NetScreen-Security Manager:

- **7554**—Migration from NetScreen-Security Manager 2004 FP2r3 or NetScreen-Security Manager 2004 FP3r2 to NetScreen-Security Manager 2005.2 unset the keepalive value for BGP causing the BGP neighbors to be unset/set on first update to the device.
- **7362**—The migrateDomainVersion.sh script did not check for correct usage.

### **VSYS**

The following are addressed issues with VSYS in this release of NetScreen-Security Manager:

- **7853**—Routes defined in shared virtual routers did not appear correctly in a VSYS.
- **7891**—Service object timeouts were not pushed to VSYS devices. This issue is now resolved for ScreenOS 5.3 devices.
- **7381**—NetScreen-Security Manager failed to completely delete a VSYS device from its root. This caused the addition of a new VSYS to fail even though sufficient licenses were present.
- **7255**—Changing a VSYS name caused inconsistencies in the configuration database.

### **Device Configuration**

The following are addressed issues with device configuration in this release of NetScreen-Security Manager:

- **8020**—Address objects imported from different zones were not correctly deduplicated.
- **7947**—It was not possible to define a DIP with an IP address in the range of the Secondary IP Address of an Interface.
- **7923**—The following pre-defined service objects were missing from NetScreen-Security Manager: ECHO, SCCP and MS-SQL.
- **7858**—It was not possible to unset the syslog src-interface parameter.
- **7769**—ScreenOS devices failed to send bulk CLI update confirmation within the timeout period. This resulted in NetScreen-Security Manager not sending a save command and the update was not successful. NetScreen-Security Manager implemented the following workaround: NetScreen-Security Manager will send a save command when this timeout occurs.
- **7700**—The "set user-group < name > location external" command was not displayed in "config summary".

- **7631**—NetScreen-Security Manager did not push custom IKE Phase1 proposals in an update causing the update to fail.
- **7628**—NetScreen-Security Manager did not display the interface pull down menu in the template while creating a route.
- **7626**—NetScreen-Security Manager did not display a warning on routes if the gateway ip was set same as interface IP.
- **7615**—It was not possible to configure source address for SNMP traps being sent from NetScreen-Security Manager. The source address is hard-coded to loopback.
- **7598**—You could not set route preferences on ScreenOS to values from 0 to 255. NetScreen-Security Manager allows values from 1 to 255 only.
- **7550**—ScreenOS supports the selection of source interface for authentication server traffic. This feature did not function properly with an NS5GT device.
- **7477**—Template override was displayed for VPN setting when no template setting was present.
- **7476/7369**—Adding modeled devices using "Bulk Add" configlets failed to generate correctly.
- **7371**—Device status on different instances of the UI were inconsistent.
- **7374**—It was not possible to disable a wireless interface on a Wireless NS5GT through a template.
- **7320**—Device Configuration State did not correctly display differences between the configuration on the device and configuration in NetScreen-Security Manager.
- **7310**—Bulk add of 3400 devices failed.
- **7309**—Two CLIs available on ScreenOS wireless 5GT devices to reactivate the wireless settings were not supported.
- **6984**—Duplicate fields were displayed in the activate device wizard.

## 6 Known Issues

---

This section describes known issues with the current release.

Section 6.1 “Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

Section 6.2 “Compatibility Issues” describes known compatibility issues with other products, including but not limited to specific Juniper Networks’ appliances, versions of ScreenOS, Internet browsers, and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.

Section 6.3 “Known Issues” describes deviations from intended product behavior in NetScreen-Security Manager as identified by Juniper Networks Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

Section 6.4 “Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2005.2” describes deviations in ScreenOS 5.0 that affect this release of NetScreen-Security Manager as identified by Juniper Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

## **6.1 Limitations of Features**

None.

## **6.2 Compatibility Issues**

None.

## **6.3 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:”

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

The following are known issues with import/update/export functionality in this release of NetScreen-Security Manager:

- **8006**—You can not import a security device running ScreenOS 4.0 using NACN if telnet is not enabled.
- **7774**—Import of a device config larger than 2 Megabytes may fail. The device will truncate the output.
- **7701**—Device Update fails if the Address Object name has multiple interior adjacent white spaces. i.e.: "abc < sp > < sp > 123".
- **6879/6185**—NetScreen-Security Manager cannot distinguish which devices contain which DI signatures. Updates may fail if unsupported signatures are included in a policy rule.
- **26363**—Import of device configurations larger than 2 MB fails (ScreenOS limitation).

### ***Security Policies***

The following are known issues with security policies in this release of NetScreen-Security Manager:

- **8017**—NetScreen-Security Manager will not generate correct CLI to create a multi-cell policy rule using a MIP with ScreenOS 4.0.
- **7889**—Application errors appear when selecting attacks in some IDP rulebases.

- **7617**—Currently the UI displays only changes to a policy (i.e. adding/removing of rulebases from policy). Changes to rulebases (adding/removing/modifying rules) are logged in audit log but can not be displayed using the Policy Editor.
- **6937**—Rule grouping is only available for zone-based rulebases.
- **6013**—When a policy rule is cut, it disappears until it is pasted.
- **26972**—A predefined group with no members other than a custom attack generates a warning in a policy rule indicating it is empty.
- **26627**—Permissions to create and delete security policies do not automatically select permissions to the following:
  - create/edit Backdoor rulebase
  - create/edit Firewall rulebase
  - create/edit IDP rulebase
  - create/edit Multicast rulebase

### **Device Configuration**

The following are known issues with device configuration in this release of NetScreen-Security Manager:

- **8036**—Routing table default metric that appears in NetScreen-Security Manager does not match the ScreenOS default.
- **8024**—The direction for an attack object is set as "any" when it is copied to a custom attack object.
 

W/A: Set the direction as "client to server" or "server to client".
- **8015**—Custom service objects do not sort correctly based on the non-ICMP column.
- **7984**—NetScreen-Security Manager sometimes displays an incorrect attack database version.
- **8025**—The domain path for the guiSvrCli.sh script should be specified as: global[. < subdomain-name > ].
- **8012**—Columns do not size correctly in the table view of the Anti-Spam screen.
- **8093**—The Device Server IP address may show as missing in the "Startup" screen if the system has been migrated from NetScreen-Global Pro.
 

W/A: Open the device editor, select the server under Report Settings -> Events and choose the Device Server under the startup section.
- **7744**—NetScreen-Security Manager does not set webauth on a ScreenOS 4.0 transparent device interface.

- **5425**—NetScreen-Security Manager unsets dynamically learned DNS settings.
- **26079**—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.

- **25190**—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.

### **VPN**

The following are known issues with VPNs in this release of NetScreen-Security Manager:

- **8189**—If a Route Based VPN is created at the device level without using a VPN abstraction and the related tunnel interface has the same name in two or more devices, deletion of this tunnel on a single device results in the deletion of the reference to this tunnel on all devices that use the same tunnel interface name.

W/A: Delete all the routes that utilize this specific tunnel interface. Alternatively, contact JTAC to assist in manually deleting this tunnel interface from the NetScreen-Security Manager database.

- **7143**—The preshared key for a VPN is displayed in clear text. There should be a way to encrypt it.
- **5353**—Config Sync does not report changes on VPN Manager.

### **NSRP**

The following are known issues with NSRP in this release of NetScreen-Security Manager:

- **8041**—NSRP cluster member names are not updated in the NSRP monitor when the devices are deleted and re-added.
- **8021**—Cluster objects do not show updated minor OS version running on a cluster that has been upgraded.
- **7820**—NetScreen-Security Manager with VSYS cluster members may experience performance issues at login time.

W/A (Partial): Open and save VSYS cluster objects to remove some redundant data.

- **7792**—NSRP Status is not updated correctly.
- **7291**—A "No Serial Number for Device" message appears which prevents access to device statistics in a cluster member.

- **26796/22489**—Connection status for VSYS cluster members is inconsistent.

### **Monitoring**

The following are known issues with monitoring in this release of NetScreen-Security Manager:

- **6477**—Get tech output for ScreenOS 4.0 devices may be truncated when retrieved through the NetScreen-Security Manager troubleshooting window.
- **5470**—The Realtime Monitor is not properly enabled after migration from NetScreen-Global PRO.

### **Installation**

The following are known issues with installation in this release of NetScreen-Security Manager:

- **8353**—While upgrading NetScreen-Security Manager from previous releases to NetScreen-Security Manager 2005.3 on Solaris, backup of your current GUI Server fails if the filenames are greater than 100 characters.

W/A: Download the latest tar from [www.sunfreeware.com](http://www.sunfreeware.com) (version 1.15.1) - this package gets installed in the /usr/local/bin directory. Create a soft link to the /usr/sbin directory as follows:

```
cd /usr/sbin
mv tar tar.org
ln -s /usr/local/bin/tar tar
```

- **8198**—If path is not set to include /usr/ucb, then NACN cert generation fails at server install time. This will make it impossible to manage NACN enabled ScreenOS 4.0.x devices with NetScreen-Security Manager.
- **7892**—You must run setsyncuser for replicateddb to function correctly
- **7906**—The HA Server install does not provide a graceful shutdown script in the /etc directory.
- **7939**—The restoreDbFromBackup.sh requires the /var/netscreen/GuiSvr directory to be present. If this directory is not present, then the restore script reports success output but nothing is restored.
- **7996**—rsync may not work correctly if some NetScreen-Security Manager processes are not running.
- **26915**—Repair install option with reconfigure option selected as true will fail with an error.

W/A: You must manually edit the guiSvr.cfg file while server processes are shut down.

### **Upgrade**

The following are known issues with upgrades in this release of NetScreen-Security Manager:

- **6113**—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.

- **26668**—Firmware Upgrades from ScreenOS 4.0 to ScreenOS 5.1/5.2/5.3 should be blocked.

### **Migration**

The following is a known issue with migration in this release of NetScreen-Security Manager:

- **26596**—Migration from a previous release of NetScreen-Security Manager may result in inconsistencies in the device UP or DOWN status.

### **Statistical Report Server**

The following are known issues with the Statistical Report Server in this release of NetScreen-Security Manager:

- **7315**—The Statistical Report Server fails to save the IP address for a second GUI Server.
- **6883**—The Statistical Report Server does not report device downtime accurately.

### **Management System**

The following are known issues with the management system in this release of NetScreen-Security Manager:

- **7035**—The GUI Server directive handler process stops under heavy load.
- **7233**—If the GUI Server is not configured in HA mode, then the Device Server will not failover if it is configured in HA mode.

## **6.4 Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager 2005.3**

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

- **55015**—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.
- **7488**—NetScreen-Security Manager reports an error when trying to set link-down an interface on an ISG 2000 device.

- **3723**—It is not possible to create a configlet for a device in transparent mode.
- **53891**—When upgrading a device from ScreenOS 5.0r10 and lower to ScreenOS 5.3, devices crash.
- **53871**—Devices running ScreenOS 5.3 may crash when generating Deep Inspection logs.
- **53854**—Wireless interface zone settings on devices running ScreenOS 5.3 are always displayed as "none" in the NetScreen-Security Manager UI.
- **53710**—It is not possible to set the bandwidth on interfaces for a VSYS in ScreenOS 5.3.
- **53595**—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.

- **53312**—You can not nest local user groups in ScreenOS 5.3.
- **53035**—NSRD in transparent mode is not functional in ScreenOS 5.3.
- **48987**—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.

- **45418/48460**—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.

- **43001**—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

## 7 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 © 2005 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.

