



NetScreen-Security Manager Release Notes

***Release 2005.1
9-1-05***

Contents

- 1 “Version Summary” on page 2
- 2 “New Features” on page 2
- 3 “Changes to Default Behavior” on page 3
- 4 “Upgrade Considerations” on page 4
- 5 “Addressed Issues” on page 4
- 6 “Known Issues” on page 13
 - 6.1 “Limitations of Features” on page 13
 - 6.2 “Compatibility Issues” on page 13
 - 6.3 “Known Issues” on page 14
 - 6.4 “Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2005.1” on page 18
- 7 “Getting Help” on page 19

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1621-000

1 Version Summary

Juniper Networks NetScreen-Security Manager 2005.1 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:

- **Scheduled Security Updates**—You can now schedule attack object updates for the GUI Server and your managed devices. Using the command line utility `guiSvrCli.sh` and a scheduling program (such as `crontab`), you can configure NetScreen-Security Manager to perform regular attack object updates.
- **Scheduled Reports**—You can now schedule reports. Using the command line utility `guiSvrCli.sh` and a scheduling program (such as `crontab`), you can configure NetScreen-Security Manager to generate reports.
- **Supported Security Devices and ScreenOS versions**—This release of NetScreen-Security Manager adds support for the following:
 - *NetScreen-5GT Wireless*. This security device can act as a wireless access point (WAP), enabling it to handle wireless and wired traffic.
 - *5000-2XGE SPM*. This secure port module (SPM) provides two 10-Gigabit Ethernet ports using hot-swappable 10-Gigabit Small Form Factor Pluggable Module for PHY transceiver. The 5000-2XGE SPM delivers up to 10 Gigabits-per-second (Gbps) of firewall and up to 5 Gbps of Virtual Private Network (VPN) capacity.
 - *ScreenOS 5.2.0*. This version of ScreenOS contains many new features. For details, refer to the *ScreenOS 5.2.0 Release Notes*.
 - *ScreenOS 5.0 L2V*. This version of ScreenOS supports transparent vsys. You can create vsys devices for a NetScreen-5000 series device running 5.0 L2V. Using Layer 2 zones, you can import VLAN IDS (tags) from the root device, group the IDs, and assign to an interface on the root or vsys.
 - *ScreenOS 5.0-FIPS*. This version of ScreenOS is FIPS compliant. Refer to the FIPS documentation for details on how to manage devices in FIPS mode.
 - *NetScreen-Hardware Security Client Plus Key*. You can now configure a NetScreen-HSC security device with a plus key when adding or modeling the device in the NetScreen-Security Manager UI.
- **Configlet Support for ADSL**—You now use Rapid Deployment (RD) to create a configlet for a NetScreen-5GT security device using ADSL. Two new options now appear in a configlet: 1484 protocol mode and the ADSL operating mode.

- **Retry for Failed Update**—You can now configure NetScreen-Security Manager to retry a device update that failed because the device was not connected to the management system; when the device reconnects, NetScreen-Security Manager attempts the update again. (To specify retry and other update settings, from the menu bar, select Tools > Preferences; in the Preferences navigation tree, select Update, then configure the update settings as desired.)
- **Log2Action Option**—You can now export logs to CSV, email, script, SNMP, syslog, and XML using the command line utility devSvrCli.sh and the log2action option. Prior to NetScreen-Security Manager 2005.1, you could configure real-time log forwarding (in the GUI server settings) as well as exporting from the Log Viewer; this new feature enables you to also export logs on demand from the Device Server.
- **Run Scripts**—You can now configure the GUI server to forward log records to a custom script.
- **Policy Printing and Exporting**—You can now export rulebases in a Security Policy to HTML for viewing and printing.
- **Preferred (Policy) ID Enhancements**—Firewall rulebases now contain a column for Preferred ID when viewing a Security Policy in extended mode. Additionally, Preferred ID now appears as an separate option in the Rule Options column (was previously configured in Miscellaneous rule options).
- **Rule Titles (ScreenOS Policy Name)**—The Comments column of a rulebase now displays the ScreenOS policy name, known as the “rule title” within the NetScreen-Security Manager UI.
- **Support for 4000 Devices**—The NetScreen-Security Manager management system now supports up to 4000 security devices.
- **Service Object Port Column**—The service object dialog box now displays a Port column, which lists the port numbers associated with the service.
- **Address Object Selection Within Group**—You can now select an individual address object from within an address object group.
- **Enhanced Search**—You can now search within rulebase columns.

3 Changes to Default Behavior

Please note the following changes in the default behavior of NetScreen-Security Manager:

- For devices running ScreenOS 5.2 and later, you can now configure logging to occur when a session is either initialized, closed or both on a security device. To configure logging, right-click on the Rule Options column for the appropriate rule, and select Log/Count. In the Logging Options section, you must then select either or both the Log on Session-Close or Log on Session-Init. For devices running a version of ScreenOS previous to ScreenOS 5.2, you must select the Log on Session-Close option.
- In Report Manager, “Custom Reports” is now called “My Reports”.

- The Job Information window for Update Device and Summarize Delta Config contains additional sections for CA Certificate to be removed from Device, and CRL to be removed from Device.
- Preferred ID is moved to a separate column from the “Miscellaneous” column in Security Policies.
- The Address Selection dialog in Security Policies has been changed to improve usability.
- During installation of the GUI Server, the message “.Xvfb doesn’t exist, ...” appears if you do not have the Xvfb library.
- A new confirmation message appears when you invoke the Import Device action.

4 Upgrade Considerations

If you upgrade from NetScreen-Security Manager FP2 and below to NetScreen-Security Manager FP3 and later, you will notice changes in rule ID numbers for some policy rules. Rules that contain more than one service object are affected by this. This is caused by a change in the hashing algorithm that generates the rule ID. Performing an update on the device resolves this condition. During the update, policy rules are unset and then set again with the new ID.

As an alternate, you can also set the preferred ID field in the policy rule to match the rule ID on the device. In this case, you do not need to unset your rules. You can do this manually or by running the import directive on the device.

5 Addressed Issues

This section describes addressed issues in the current release:

Role-Based Administration

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

- **5937**—Admins could not delete security devices due to reference resolution issues with VPN Manager.
- **5825**—Admins could not configure a Start Time or Stop Time within a schedule object.
- **5805**—Admins could not bind an interface to management zone in a device template.
- **5763**—Admins could not set email reporting options for a device template.
- **5762**—Admins could not configure the syslog reporting option in a device template, but the option was not recognized by devices that use the template.

- **5717**—NetScreen-Security Manager did not enable admins to configure more than 200 multicast static-group entries on an interface. A warning message appeared indicating that the IGMP Group Limit has been exceeded.
- **5549**—Admins could not change the DHCP Mode from Server to None.
- **5509**—Admins could not define a name for a rule in a Security Policy.
- **5405**—NetScreen-Security Manager enabled admins to define the port mode for a subinterface before defining the IP address for the subinterface. (When using the ScreenOS CLI or WebUI, admins must define the IP address before port mode.)
- **5332**—A subdomain name could not be changed.
- **4946**—When an address object and global MIP object have the same name, admins could not include either object alone in a firewall rule; selecting one object automatically selects the other.
- **4632**—Old domain versions did not have a timestamp.
- **4579**—NetScreen-Security Manager did not correctly display all available roles for an admin in the Manage Administrators and Roles dialog options. An admin with full permissions to view all activities for a role could not see those activities unless the role is explicitly assigned to the admin.
- **4391**—NetScreen-Security Manager permitted admins to create only 10 aggregate interfaces for a NetScreen-5400 security device, which supports 19 aggregate interfaces.

Import/Update

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

- **6419**—When the object name was the same with the exception of the case, the policy that used this object was not unset.
- **6335**—When you use NetScreen-Security Manager to remove the gateway IP Address on an interface and then update the device, the command "unset int untrust gateway" was not sent to the device.
- **6184**—No mechanism prevented accidental device configuration import.
- **5899**—NetScreen-Security Manager sent an outdated `set url type websense` command to the device with every device update attempt. (The command was updated to `websense/scfp` in ScreenOS 5.1.)
- **5898**—After NetScreen-Security Manager upgrades NetScreen-5GT security devices running ScreenOS 5.0 to 5.1r3, device updates failed due to new failover enable option in ScreenOS 5.1.
- **5811**—When attempting to update a device for which no actual changes occur, NetScreen-Security Manager generated unnecessary log action messages.

- **5707**—Activating and updating a modeled NetScreen-5GT security device failed upon attempting to send the command "set url config disable" to the device.
- **5681**—For an imported multicast policy, NetScreen-Security Manager did not import the destination address, generating a validation error. To avoid this validation error, manually add the destination address.
- **5252**—When using VIP objects in firewall rules for NetScreen-5GT and 5XT devices running ScreenOS 5.1, updating their device configurations caused device update failures.
- **5222**—Setting the DHCP Relay Parameters caused device update failures.
- **5160**—After upgrading a device to ScreenOS 5.1r3, NetScreen-Security Manager attempted to set the RIP poll interval in minutes instead of seconds (the device calculates the interval in seconds). This mismatch caused device update failures.
- **5080**—After activating a modeled NetScreen-5GT device that does not have an AntiVirus (AV) licence key installed, the first device update failed due to AV errors.
- **4647**—Changing the default value for the BGP keep-alive setting caused device update failures.
- **4632**—Updates to NetScreen-5GT security devices failed when you have enabled URL filtering. This has been fixed for security devices running ScreenOS 5.2 or higher.
- **3407**—When NetScreen-Security Manager imports address objects or address object groups that use the same name but with different content and defined in different zones, problems occurred when importing the device configuration. (the import fails or the import result is not correct).

Directives

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

- **5704**—Malfunctioning security device resulted in large number of messages from a single device. This prevented you from running directives.
- **5211**—When managing large numbers of devices running ScreenOS 5.1, NetScreen-Security Manager occasionally was unable to send directives to any managed device.

Security Policies

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

- **6152**—After pasting a copied rule within a Security Policy, admins had to set the Preferred ID for the rule to be a unique value.

- **5873**—Using the “Save As” to save a Security Policy removed all devices from the Install On column.
- **5716**—To achieve best memory usage for a large Security Policy, NetScreen-Security Manager monitors the number of open rulebases and rule groups and unloads any data not required by the current view. Opening multiple rulebases and rule groups in a single Security Policy caused invalid references to appear in rule groups; because some unviewed rules are unloaded from memory, some rule groups might appear as empty. The workaround was to restart the NetScreen-Security Manager UI.
- **4556**—When pasting a cut or copied rule within a Security Policy, you had to first select an existing rule, then paste the cut or copied rule.

Device Configuration

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

- **6133**—You could not create aggregate interfaces on a security device running in transparent mode.
- **6131**—The service_table.nml meta data file contained incorrect indentation.
- **6071**—NetScreen-Security Manager sent commands that are out of context and unused by the physical device; these commands, which the device ignores, produced harmless warning messages.
- **6051**—You could not add a tunnel, loopback, or redundant interface to a NetScreen-500 security device running ScreenOS 5.0.0r9. Although the device supports 27 tunnels, only 22 tunnels could be added to the device.
- **6028**—Changing or adding a security device to the Install On column of a rule created a duplicate device within the Install On column.
- **5940**—When viewing the Security Devices tree for the first time, an error message appeared, indicating that the device view cannot be created.
- **5936**—The search functionality did not work properly when searching service objects.
- **5498**—When an authentication server name contained spaces, updating a device that uses that authentication server object caused device update failures.
- **5438**—After deleting a VIP that was inherited from a template, admins could not create a new VIP.
- **5256**—Changing the virtual router for a zone bound to an interface did not reset the interface IP.
- **5226**—When creating a custom URL profile, a “Cannot Create View” error message appeared.

- **4839**—When adding a security device that uses NACN, you had to set the connection method to SSH in the device configuration before copying commands to the device console. If the connection method is not explicitly set to SSH, NetScreen-Security Manager might use Telnet instead.
- **23753**—j2ssh does not support timeout in user authentication and channel opening. If the network fails during these two operations, j2ssh hangs. However, because J2ssh supports timeout in preceding connections for establishing and the following shell command execution, only a very small opportunity exists for a network failure to cause the hang.
- **23746**—When adding a new custom service object, if you entered the name of the service object first, a persistent validation warning appeared (entering all required custom service object information does not remove the validation warning triangle).

Validation

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

- **5764/23734/21956/22989/22979/18777**—NetScreen-Security Manager displayed incorrect validation errors when executing the Validate Device directive.
- **5760**—When creating a new host address object, switching from IP to DNS (or DNS to IP) caused a validation warning to persist for the domain name field.
- **5732**—NetScreen-Security Manager validated fields that were not available, generating unnecessary validation messages.
- **5352/5301**—When creating a custom service object, NetScreen-Security Manager did not validate that a source port is defined.
- **5275**—NetScreen-Security Manager incorrectly displayed the validation error "IP address belongs to the same subnet" when an IP address exists in two subnets in two different virtual routers.

VPN

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

- **5655**—When configuring a VPN in VPN Manager, admins could not select an untrust interface that uses DHCP.
- **5499**—Adding new devices to an existing VPN caused VPN Manager to swap tunnel numbers for interfaces in route-based VPNs, which can break manually defined static routes.

Virtual Systems

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

- **5711**—After a vsys was set to the RMA state, you could not update a vsys configuration on the device.
- **5317**—Update of vsys failed to complete on the ISG 2000.
- **5253**—On a vsys device, you could not use subinterfaces to add a VSI interface.
- **4989**—In the right-click menu options for a vsys device, the View Statistics option did not appear.
- **3638**—After NetScreen-Security Manager upgrades a managed vsys to ScreenOS 5.0.0r8, the Device Monitor did not display the correct firmware version for vsys.

NSRP

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

- **5841**—When a NetScreen-25 cluster device is included in multiple device groups, upgrading the firmware on that cluster caused the upgrade firmware dialog to display each cluster member twice.
- **5732**—When NSRP config sync for vrouter is disabled (to enable different routing configuring on cluster members), NetScreen-Security Manager did not push device-level OSPF settings for VPN Manager-created VPN tunnels.
- **5185**—ethernet 8 appeared as a valid interface for NSRP configurations, but was not supported by any version of ScreenOS. Additionally, after setting ethernet 8 as an interface for NSRP, you could not reset the interface. To work around this issue, “None” was added to the list of available interfaces.

Delta Config Summary

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

- **5406**—After you create a new subinterface for a device, a delta config summary displayed two CLI commands:

```
set interface <interface> tag <tag number> zone <zone>
set interface <interface> route
```

However, NetScreen-Security Manager only installs the first CLI during an actual device update; the second CLI command is not sent to the device.

- **5081**—A delta config summary report displayed discrepancies for NetScreen-5GT (Trust-Untrust, 10 user license) security device in an NSRP configuration.
- **4921**—When a non-Super admin runs a delta config summary, an error message appeared.

- **3660**—When deleting a CA certificate from a device, if the CA certificate did not also exist within NetScreen-Security Manager, a delta config summary report did not warn admins of impending CA certificate deletion.

Logging

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

- **6233**—Exporting logs to PDF failed with the following message "Internal Error was seen and the application needs to be restarted".
- **5710**—Audit Log Viewer would throw an exception while browsing.
- **5529**—Search did not function properly in the Log Viewer module.
- **5840**—Log Viewer did not display Device Down log entries for security devices running ScreenOS 5.0 and/or 5.1.
- **5036**—The Log Viewer "tail log" functionality did not correctly tail log entries for HA configurations.

Reports

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

- **6473**—Reports were not available to users who have the domain administrator permissions for all subdomains except the global domain.
- **5436**—Custom reports did not display correctly.

Monitoring

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

- **6408**—Monitoring option was not available for tunnel interfaces.
- **5913**—In the Device Monitor, sorting by ScreenOS version did not sort patch versions correctly.
- **5584**—For servers running Solaris, the Server Monitor displayed an incorrect value for the Total Disk space (in the Service Detail Status).
- **4835**—In the Server Manager, the GUI Server status toggled from UP to DOWN every few seconds.
- **4737**—Every time you performed a firmware upgrade out of band, the Real Time Monitor did not indicate the upgraded version of the device.
- **4583**—The NSRP Monitor VSD0 summary tab did not display master/backup status for security devices.

Upgrade

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

- **6327**—After upgrading NetScreen-Security Manager from FP2r3 to FP3-IDPr1, the management system assumed an incorrect device policy name, causing device updates to fail.
- **6258**—After upgrading NetScreen-Security Manager from FP1r2 to FP3-IDPr1, vsys logging stopped.
- **6196**—After upgrading NetScreen-Security Manager from FP2r3 to FP3r2 (build LGB3z2a1), updating a vsys security device failed with the error "Unable to create Device DM, Invalid MIP object defined in the rule".
- **6198**—After upgrading from NetScreen-Security Manager FP2r3 to FP3r2 (build LGB3z2a1), rules in the Global Rulebase that contain vsys security devices displayed an error.
- **6087**—After upgrading NetScreen-Security Manager to FP3r2, some security devices could not connect to the management system.
- **6045**—Upgrading NetScreen-Security Manager from FP2r3 to FP3r2 would unset the SNMP name in an NSRP cluster.
- **5747**—When upgrading a particular database from NetScreen-Security Manager FP3r2 to build LGB3z2a1, the upgrade is successful with no errors but there were missing files. After the upgrade, the guiSvrManager service did not start. The following files were not copied during the upgrade to the patch version.

```
#/var/netscreen/GuiSvr/global/rb_firewall_table.nml
```

```
#/var/netscreen/GuiSvr/global/rb_firewall/*.nml
```

```
#/var/netscreen/GuiSvr/global/subdomain/<subdomainname>/rb_firewall_table.nml
```

```
#/var/netscreen/GuiSvr/global/subdomain/< subdomainname> rb_firewall/*.nml
```

- **23561**—After upgrading from NetScreen-Security Manager 2004 FP1r2 to FP3r2, the device keys were lost.

Migration

The following is an addressed issue with Migration in this release of NetScreen-Security Manager:

- **5773**—Due to a data migration issue that occurred when moving from NetScreen-Security Manager FP3r1 to FP3r2, references to empty DI Profile data were not removed. In NetScreen-Security Manager 2005.1, these references created an inconsistency in the NetScreen-Security Manager configuration database.

High Availability

The following are addressed issues with High Availability (HA) in this release of NetScreen-Security Manager:

- **23805**—Solaris servers in a high availability configuration became intermittently unresponsive.
- **6302**—HA did not replicate correctly when the processes are not running as root.

Management System

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

- **6214**—I-node shortage filled server.
- **6027**—Purging logs from a Device Server running Solaris did not work correctly.
- **6012**—The GUI Server crashes with failed RSA authentication for admin user.
- **5755**—Server crash when adding new objects and browsing through sub domains.

Documentation

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

- **5891**—Documentation did not detail how the number of DI attack groups can be different between a particular ScreenOS release and the number in NetScreen-Security Manager (since NetScreen-Security Manager is a superset).
- **5527**—Documentation did not detail the number of logs that can be added to a pdf.
- **5403**—Screen shot in the Administrators Guide did not represent the CPU utilization details correctly.

Miscellaneous

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

- **6145**—NetScreen-Security Manager created a group member with the ID of the group.
- **6048/6103**—The device daemon crashed with the error "Too many open files".
- **5548**—Some international Microsoft Windows versions did not enable admins to configure the "Starting At" time period setting in the Log Investigator options.
- **5530**—Database corruption caused device status to be none.

- **5397**—After upgrading a device from ScreenOS 5.0 to 5.0.0r8, NetScreen-Security Manager changed the syslog reporting settings on the device.
- **5291**—Database corruption caused domain_table.nml to become empty.
- **4807**—NetScreen-Security Manager used the OneSecure OID instead of Juniper Networks enterprise OID.
- **4570**—When creating a Rapid Deployment (RD) configlet, an interface netmask error message appeared. To avoid this validation error, retype the default netmask.

6 Known Issues

This section describes known issues with the current release.

Section 5.1 “Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

Section 5.2 “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 5.3 “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 5.4 “Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2005.1” 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

This release contains the following feature limitations:

- NetScreen-Security Manager cannot support the upgrade of NetScreen-500 and ISG 2000 security devices from ScreenOS 5.1 to ScreenOS 5.2. This migration requires a bootrom upgrade; for more details, refer to the *ScreenOS 5.2 Migration Guide*.
- NetScreen-Security manager does not support ScreenOS 5.2r1 for NS5GT-ADSL security devices.

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:".

Role-Based Administration

The following are known issues with Role-Based Administration in this release of NetScreen-Security Manager:

- **24574**—You must be a global domain administrator in order to run the Scheduled Security Update command properly.
- **24016**—The update config activity does not include update policy.

W/A: Add the update policy activity.

Policies

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

- **5343**—Policies support only one MIP per rule for ScreenOS 5.x devices.

Import/Update

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

- **6649**—When you re-import a device, VPN objects that were generated by the VPN Manager are no-longer greyed out, and then become decoupled from the VPN Manager. Further changes in the VPN Manager will no longer apply to these device VPN objects.
- **6638**—If you configure the "SMTP" service object, and update a device running ScreenOS 5.0.0rX, the update fails. This is because the SMTP service object is included in ScreenOS 5.1 and above.
- **24034**—When a device is imported, NetScreen-Security Manager removes device object values that match the default values (or template-provided values). If there is no default, the imported value is retained in the device object data. If you add a template that sets one of these fields, the device object value overrides the template value.

W/A: Right click on the field label and choose to Revert the value to the template or default value.

Firmware Upgrade

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

- **6134**—When upgrading the image for a NetScreen-Hardware Security Client, you need to rename the file name for any ScreenOS 5.x image. (e.g. ns5gt.5.0.0r8.1 needs to be renamed to ns-hsc.5.0.0r8.1).

- **24243**—If you add a security device running ScreenOS 5.0, and then upgrade the firmware version to ScreenOS 5.1, or if you create a device running ScreenOS 5.1 and upgrade the firmware version to ScreenOS 5.2, the following verification error appears when you update the device.

```
Verification failed
The following parameters did not get updated to the device:
set service H.323 timeout 0
The device still has the following parameters which should have been
modified
set service H.323 timeout 30
```

The verification error is not harmful and you can disregard it. However, if you want to clear the error you can either: import the device; change the H.323 timeout value to 30 minutes (for devices running ScreenOS 5.1) on the “Advanced-> Predefined Service Timeout” screen in the device object and update the device; or change the H.323 timeout value to “Default” (for devices running ScreenOS 5.2) on the “Advanced-> Predefined Service Timeout” screen in the device object and update the device.

Virtual Systems

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

- **4071**—Admins in a subdomain can not view shared interfaces in a vsys device.
- **24480**—Names for vsys must be unique throughout all domains.
- **22489/23440/23503/23827**—When a root device connection state changes, that change is not populated to all associated vsys devices. This can cause the UI to display an incorrect vsys connection state; however, all vsys features remain enabled.

NSRP

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

- **24479**—If you create a cluster device in NetScreen-Security Manager FP3r2 or before, and the cluster device contains MIP objects with a policy referring to the MIP objects, and you have unset (or delete) the vsd group 0, then after you import the device and perform a “Summarize Delta Config” action, the following error message appears in the Job window.

```
Error Text: Unable to create device DM.
Invalid mip object in rule No Details Available.
Error Details: No Details Available.
```

This issue is resolved this release of NetScreen-Security Manager. However, if you are migrating from NetScreen-Security Manager FP3r2 or before to NetScreen-Security Manager 2005.1, the error still appears.

W/A: Perform an “Import Device” action on the cluster device in NetScreen-Security Manager 2005.1.

- **23953**—Clusters do now show the correct minor version after a firmware upgrade.
- **23914**—Config sync does not show the device out of sync when the policy is deleted.
- **23599**—If an audit log is double clicked to see Audit Log details, no further Audit Log details screens can be accessed until the UI is restarted.

Logging

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

- **5528**—Setting the time received filter in the filter summary is inconsistent with the duration in the Log Investigator options dialog.
- **24467**—Only two pages of logs are supported for PDF exports.
- **24253**—NetScreen-Security Manager allows custom service object to have the same name (case-insensitive) while service objects created using CLI are case-sensitive.

Reports

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

- **6235**—Log filter for custom reports does not remember the last IP/subnet mask entered.
- **24433**—If you are running Linux without X-Windows, and you want to generate Scheduled Reports, you need to install the following packages:

```
XFree86
XFree86-100dpi-fonts
XFree86-75dpi-fonts
XFree86-base-fonts
XFree86-libs
XFree86-Xvfb
XFree86-libs-data
XFree86-truetype-fonts
XFree86-Mesa-libGL
XFree86-xf86
XFree86-xauth
XFree86-font-utils
```

If you are running Linux Red Hat ES, you need to install the following additional packages:

```
chkfontpath
cpp
xinitrc
switchdesk
desktop-file-utils
```

Management System

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

- **5692**—Manual shutdown of the haSvr does not cause the shared disk unmount command to be run.

Performance

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

- **6436**—Performance issues outside of NetScreen-Security Manager (e.g. Syslog) may cause syslog files to get piled up inside of the system.
- **6225**—Automatic back up may fail due to performance issue with large number of domain versions.

High Availability

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

- **6302**—HA does not replicate correctly when the processes are not running as root.

Miscellaneous

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

- **6279**—Adjust OS version does not work for modeled devices that are deployed with the not reachable workflow.
- **5843**—If a device is in multiple groups, the Job Manager will not display the correct %complete when a directive is run.
- **3723**—If you are using Rapid Deployment, you can not create a configlet for transparent mode devices.
- **24627**—The "--skip" option of the "guiSvrCli --update-attacks" command is supposed to update the connected devices and flag the disconnected devices as update needed. However, the actual behavior of this option is that it will try to update both the connected and disconnected devices and will not flag any devices as update needed. Disconnected devices will simply timeout and be attempted again during the next scheduled update.
- **24608**—Compound attacks with some members having direction "Server to Client" and others as "Client to Server" are displayed incorrectly under the general "Category" group. For example, attack AOL Admin Server Response (TROJAN:MISC:AOLADMIN-SRV-RESP) should be under "Response_TROJAN-Major", but are listed under "Category_TROJAN-Major". Performance is degraded significantly for attacks containing one or more members having direction "Server to Client".

W/A: Place these attacks under the "Response" group.

- **24033**—If you perform a Get Running Config successfully, but the Delta Config Summary fails, there may be a problem with the random number generator used by the java virtual machine. Contact Juniper Networks Technical Assistance Center for further assistance.
- **24559**—Newly created SIP anomalies/signatures are categorized in the signature database under the VOIP:SIP categories. Since predefined groups in NetScreen-Security Manager filter on this category designation and are currently flattened to only one level of hierarchy, these attacks and signatures are in the VOIP category. When creating SIP custom Attacks, the category that NetScreen-Security Manager assigns the custom attacks is its "service", which is part of the AppService_Table. Since there is an Appservice called SIP, when you create the custom attack, it is assigned to the "SIP" category corresponding to the service. Since there is not a predefined group called "SIP", this attack does not appear under the category tree of pre-defined attacks.

W/A: Create a dynamic group and choose "SIP" as the filter for that group to have these attacks display.

- **24534**—For a WLAN device in transparent mode, the L3 zone is displayed even though it is not accessible on the device.
- **24142**—After creating a device using the "Device is not reachable" option, if you right-click the device and then select Admin> Show Device Commands, the Show Device Command window appears multiple times after edits.
- **24124**—The device export feature does not support IDP policies.
- **24120**—The src-port range on ScreenOS for the service RSH/SIP/H.323 is different from the src-port range of NetScreen-Security Manager.

6.4 Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2005.1

The following are known issue in ScreenOS 5.0 that specifically affects this release of NetScreen-Security Manager:

- **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:

Issue	5.0.0	5.0.0 r9 for 5000 M2	5.0.0-GPRS.r8.5	5.0.0 WLAN	5.0.0 r9 for ISG 1000/ISG 2000	5.0.0IDP1
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

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.

