

IDP Series Release Notes

IDP OS 5.1r1

February 8, 2011
Revision 01

Contents

Overview	2
Supported Hardware	2
New and Changed Features	2
Unsupported Features	4
Known Limitations	4
Supported Upgrade Paths	5
Downgrading or Reverting	6
Licensing	6
Compatibility with Network and Security Manager	6
Compatibility with Juniper Networks Infranet Controller	7
Browser Requirements	7
Upgrading IDP Software	7
Upgrading with NSM	8
Upgrading with the CLI	10
Resolved Issues	12
Known Issues	15
Documentation	20
Getting Help	22

Overview

Juniper Networks Intrusion Detection and Prevention Series devices enable you to enforce a security policy that leverages continuous security research by the [Juniper Security Center](#) to protect your network from attacks. The IDP Series also includes features that enable you to gather information about applications and servers in your network.

These release notes contain information about what is included in this product release: supported features, unsupported features, changed features, known problems, and resolved problems. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Supported Hardware

IDP 5.1r1 is supported on the following platforms:

- IDP8200, IDP800, IDP250, IDP75
- IDP1100, IDP600, IDP200

New and Changed Features

The following table summarizes new and changed features.

Table 1: New Features

Feature	Description
High availability	IDP OS Release 5.1 supports high availability in network designs where you have deployed redundant network paths and use the failure detection features of a firewall, router, or switch to manage the cutover from the primary path to the backup path in cases of failure. For details, see IDP Series Deployment Scenarios .
Simulation mode	<p>Beginning in IDP OS Release 5.1, you can operate the IDP Series device in simulation mode. In simulation mode, the original packets are forwarded immediately and the IDP Series device processes a copy, logging actions that would have been taken if simulation mode were not enabled.</p> <p>You operate an IDP Series device in simulation mode in the following situations:</p> <ul style="list-style-type: none"> • When you first deploy the IDP Series device in your network and you want to evaluate the security actions it takes without disrupting traffic. • When you implement a new feature or change a security policy and you want to evaluate the impact without disrupting traffic. • As a workaround to avoid traffic outages when IDP processing is resulting in crashes and other failures. <p>For details, see Simulation Mode Overview and its related topics.</p>
Enhanced system resource instrumentation	IDP OS Release 5.1 supports extensive system resource instrumentation, so you can use SNMP utilities to monitor device health and load. For details, see SNMP Statistic Reporting and Traps Task Summary and its related topics.

Table 1: New Features (*continued*)

Feature	Description
Enhanced application identification	<p>Beginning with IDP OS Release 5.1, the application identification feature can match extended application signatures used in APE rulebase rules. <i>Extended application</i> signatures are also called <i>nested application</i> signatures. The predefined extended application signatures developed for IDP OS Release 5.1 include the most prevalent Web 2.0 applications running over HTTP. If your security policy includes APE rules configured to match extended application signatures, the application identification process identifies and generates the following HTTP contexts: http-url-parsed, http-url-parsed-param-parsed, http-header-host, and http-header-content-type. The application identification feature can then match application signature patterns in those contexts.</p> <p>J-Security Center updates application signatures and develops new ones as necessary. Beginning with IDP OS Release 5.1, you can use NSM to browse predefined application objects, predefined extended application objects, and application groups. You can also use NSM to create custom application definitions, if needed. You cannot, however, create custom extended application definitions.</p> <p>For details, see Using Application Identification, Using Application Objects, and their related topics.</p>
Enhanced APE rulebase features	<p>Beginning with IDP OS Release 5.1:</p> <ul style="list-style-type: none"> You can create rules that match extended application objects (also called nested application objects). You can apply a new action to matching rules: DiffServ + Ratelimiting. If you use user-role based matching, you can set a global option to enable an aggregate limit for matching user-roles (default) or a per-subscriber rate limit (by using a CLI command). <p>For details, see Understanding the APE Rulebase and its related topics.</p>
Enhanced attack signature	<p>IDP OS Release 5.1 supports the following configurable constraints to enable you to fine-tune custom attack signatures:</p> <ul style="list-style-type: none"> Within bytes—Configure a byte range where the attack pattern must be detected. Within packets—Configure a packet range where the attack pattern must be detected. Context checking—Configure a byte-length requirement for matching contexts. <p>This release also supports bit-level matching for binary protocols.</p> <p>For details, see the IDP Series Custom Attack Object Reference and Examples Guide.</p>
Configurable syslog communication	<p>Beginning with IDP OS Release 5.1, you can specify the protocol and port to use for syslog messages. See Configuring Syslog Collection (NSM Procedure).</p>
Bidirectional packet capture	<p>Beginning with IDP OS Release 5.1, you can use a new utility to capture packets at the Rx interface (receiving interface) and also at the Tx interface (transmitting interface). See Using jnetTcpdump to Capture Packets.</p>

Table 1: New Features (*continued*)

Feature	Description
Enhanced debugging and troubleshooting tools	<p>You can use the following CLI command enhancements to display system information:</p> <ul style="list-style-type: none"> • scio app cache—A new option, listall, allows you to list the entire application identification cache. Previously, only the most recent 32 were listed. • scio logview—A new command that enables you to troubleshoot log collection by NSM. The command allows you to view raw log data on the IDP Series device so you can compare it to the logs seen at NSM. • scio subs—A new option displays aggregate statistics for all IDP engines on IDP8200. IDP8200 has multiple IDP engines. To view an aggregation, use scio subs aggregatestatus s0. To view statistics per engine, use scio subs status s0. • scio var—The TCP and UDP flow tables now include a column for application.

Unsupported Features

The following features are not supported in IDP OS Release 5.1:

- SSL decryption using IDEA-based algorithms or ciphers. Also not supported in IDP OS Release 5.0.x.
- On IDP8200, 10 gigabyte fiber interfaces do not support interface signaling or peer port modulation. Also not supported in IDP OS Release 5.0.x.
- Authentication to the ACM via RADIUS with RSA SecurID (authentication via RADIUS server is supported). Same as IDP OS Release 5.0.x.

Note that IDP75 does not have an HA interface. We do not support an HA deployment with IDP75 devices. Also, IDP75 has only one pair of traffic interfaces. We do not support a mixed mode deployment with IDP75 devices.

Known Limitations

For single core platforms (IDP75, IDP200, IDP600), we recommend you disable application volume tracking (AVT). The AVT feature is fully functional, but the AVT process is CPU intensive. During stress testing, high CPU usage by the AVT feature resulted in link flapping.

Note that if you disable AVT, IDP Reporter application volume reports are empty.

To disable AVT:

1. From NSM Device Manager, double-click a device and then click **Profiler Settings**.
2. Click the **General** tab.
3. Deselect **Enable AVT**.
4. Click **Apply**.
5. From NSM Device Manager, right-click the device and select **Update Device** to push your configuration change to the device.

Supported Upgrade Paths

You can upgrade directly from any of the following versions:

- 5.0r2
- 5.0r1
- 4.1r4

Beginning with IDP OS Release 5.0, IDP Series does not support bridge, proxy-arp, or router mode. Before upgrading to IDP OS 5.1, you must redeploy the IDP Series device in transparent or sniffer mode.



NOTE: The upgrade paths assume your current IDP Series device has been in use and the device had been added to NSM. You might encounter unexpected behavior during the upgrade if you are upgrading from a newly reimaged, undeployed IDP OS 4.2 or 4.1 device (such as a 2009 factory image of the IDP OS). In these cases, we recommend you add the IDP device to NSM and import the device configuration into NSM prior to performing the upgrade. Doing so will avoid the file permissions issue described in KB 15071.

Table 2 on page 5 describes the changes to files and directories you will notice when you upgrade.

Table 2: Changes to Files and Directories

Upgrade Path	Files and Directories
From 5.0r2	No changes to attend to before upgrade.
From 5.0r1	<p>Before you upgrade, take note of the following changes and recommended actions:</p> <ul style="list-style-type: none"> • IDP 5.1r1 stores packet logs in numbered subdirectories of <code>/usr/idp/device/var/pktlogs/</code>. To implement this change, your existing <code>/usr/idp/device/var/pktlogs/</code> directory will be overwritten. If you have been using the option to maintain packet data locally and send to NSM on demand, copy any packet logs you want saved from <code>/usr/idp/device/var/pktlogs/</code> to a remote location before you upgrade. Previously collected packet capture logs will not be available to NSM. This action is not required if you have been using the option to always include packet data when NSM sends the event log. • Your custom settings in the <code>/usr/idp/device/bin/user_funcs</code> file are preserved when you upgrade. No action is required.

Table 2: Changes to Files and Directories (*continued*)

Upgrade Path	Files and Directories
From 4.1r4	<p>When you upgrade from IDP OS 4.1r4 to IDP OS 5.1r1, you are reimaging the disk with a new operating system. All partitions except /var/idp are rewritten.</p> <p>In addition, IDP 5.1r1 stores packet logs in numbered subdirectories of /usr/idp/device/var/pktlogs/. This is the same directory structure introduced in IDP 4.1r4. Note, however, that the upgrade process preserves only packet log files in /usr/idp/device/var/pktlogs/0/. Packet log files in other directories will be lost upon upgrade. If you have been using the option to maintain packet data locally and send to NSM on demand, copy logs from /usr/idp/device/var/pktlogs/1/ and higher numbered log directories to a remote location before you upgrade. This action is not required if you have been using the option to always include packet data when NSM sends the event log.</p> <p>The upgrade process restores your license and most of your previous settings. The following settings are not preserved:</p> <ul style="list-style-type: none"> • The upgrade does not retain settings no longer supported in IDP 5.1. • The upgrade process saves a backup of your previous /usr/idp/device/bin/user_funcs file, but installs a new user_funcs file in order to provide appropriate content for IDP 5.1.

Downgrading or Reverting

You cannot downgrade or revert to a previous version. You can reimage the operating system, if necessary. For details on reimaging, see the installation guide for your IDP Series device.

Licensing

The upgrade procedure preserves your earlier license configuration. The reimaging procedure does not. If you reimage the appliance, see the installation guide for information on licensing.

Compatibility with Network and Security Manager

At the time of the IDP OS Release 5.1r1, we verified compatibility with the following release of Network and Security Manager (NSM):

- NSM 2010.4 build LGB14z2q21

NSM 2010.4 build LGB14z2q21 is required to support new IDP OS Release 5.1 features.

Table 3: Download Locations for NSM 2010.4 (Requires Log In)

NSM Software	URL
NSM Client	https://download.juniper.net/software/nsm/2010.4q21/nsm2010.4q21_ui_win_x86.zip (Windows)
	https://download.juniper.net/software/nsm/2010.4q21/nsm2010.4q21_ui_linux_x86.zip (Linux)

Table 3: Download Locations for NSM 2010.4 (Requires Log In) (*continued*)

NSM Software	URL
NSM Server	https://download.juniper.net/software/nsm/2010.4q21/nsm2010.4q21_servers_sol_sparc.zip (Solaris)
	https://download.juniper.net/software/nsm/2010.4q21/nsm2010.4q21_servers_linux_x86.zip (Linux)
MD5 checksum	https://download.juniper.net/software/nsm/2010.4q16/md5sum.txt



NOTE: NSMXpress users should consult KB 13946 for information on how to upgrade NSMXpress to a patch version of NSM.

Compatibility with Juniper Networks Infranet Controller

The user-role-based policy feature depends on deployment with IC Series Unified Access Control (UAC) 4.1r1 or later. Contact your Juniper Networks sales representative for information on UAC release dates.

Browser Requirements

The ACM, QuickStart utility, and IDP Reporter have been tested on the following browsers:

- Internet Explorer 7.x, 6.x
- Firefox 3.x, 2.x

Upgrading IDP Software

During upgrade, the IDP Series appliance is gracefully shut down. If you have configured bypass for traffic interfaces, you do not need to be concerned about traffic disruption. If you have not configured bypass, you should plan to complete your upgrade at an appropriate time.

You can use NSM or the CLI to upgrade the IDP OS. You must use NSM to complete the IDP detector engine and attack object updates.



TIP: If possible, use a laptop to connect to the console port of the IDP Series device when you upgrade. This will enable you to view any console messages that can assist in identifying any issues during upgrade. We understand this is not possible or desirable in all deployments, so connecting via console is not required to upgrade.

This section provides the following upgrade workflows to upgrade a standalone IDP Series device:

- Upgrading with NSM on page 8
- Upgrading with the CLI on page 10



NOTE: Upgrading an HA deployment involves special considerations. For information on upgrading an HA deployment, see “Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1” in *IDP Series Deployment Scenarios*.

Upgrading with NSM

This section describes a workflow for upgrading IDP software using only NSM.

To update IDP software:

1. Add the IDP software to the NSM GUI server.
2. Push the IDP software from the NSM GUI server to one or more IDP Series devices.

To add an IDP software image to the NSM GUI server:

1. Download the software image:
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
 - b. Enter the IDP Series device serial number to display a view of applicable software releases available for download.
 - c. Click the applicable link to display the software download page.
 - d. Download the software to a location you can access from your NSM client.
2. From the NSM main menu, select **Tools > Software Manager** to display the Software Manager dialog box.
3. Click the + button to display the Open dialog box.
4. Select the IDP software image you just downloaded and click **Open** to add the software image to the NSM GUI server.
5. Click **OK**.

To push the software image from the NSM GUI server to IDP Series devices:

1. From the NSM main menu, select **Devices > Software > Install Device Software** to display the Install Device Software dialog box.
2. From the Select OS Name list, select **ScreenOS/IDP**.
3. From the Select Software Image list, select the image file you just added to the NSM GUI server.

4. In the Select Devices list, select the IDP Series devices on which to install the software update.
5. Click **Next** and complete the wizard steps.
6. Select **Automate ADM Transformation** to automatically update the Abstract Data Model (ADM) for the device after NSM installs the update.



NOTE: If you clear this setting, the update is installed onto the device, but you cannot manage the device from NSM until the device ADM is updated.

7. Click **Finish** to display upgrade status in the Job Information dialog box.
8. When the upgrade finishes, click **Close** to exit the Job Information dialog box.

The software upgrade is complete.



NOTE: You might encounter unexpected behavior if you have changed the factory BIOS settings for the IDP Series device. We advise that you do not change the factory BIOS settings.

The console will hang at GRUB after reboot if you have changed the BIOS setting **Console redirection > Continue Console redirection after POST to ON**.

To resolve this issue, press the Delete key to enter BIOS and set this option to **OFF**.

- Next Steps:**
1. If you are upgrading from IDP OS Release 5.0r1 or 5.0r2, skip this step. You completed it when you upgraded to IDP 5.0r1. If you are upgrading from IDP OS 4.1r4:
 - a. Run through the ACM wizard to [reconfigure your virtual routers](#). In IDP OS Release 5.0 and later, you use ACM to configure deployment mode per virtual router.
 - b. If necessary, copy any custom settings from the backup copy of user_funcs to the new user_funcs file.
 2. Check to see if J-Security Center has released an update for the detector engine or attack database:

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.
 3. Push the updated IDP detector engine to IDP Series devices:

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.



NOTE: Updating the IDP detector engine on a device does not require a reboot of the device.

4. Push a security policy update job to update attack objects in use in your security policy:
 - a. In NSM, select **Devices > Configuration > Update Device Config**.
 - b. Select devices to which to push the updates and set update job options.
 - c. Click **OK**.

Upgrading with the CLI

This section describes a workflow where you use the CLI to upgrade the software image on the IDP Series device. You still use NSM to update the detector engine and attack objects.

To upgrade IDP OS from the CLI:

1. Download the software image to a host that runs an FTP server. Follow these steps:
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
 - b. Enter the IDP Series device serial number to display a view of applicable software releases available for download.
 - c. Click the applicable link to display the software download page.
 - d. Save the **sensor_version.sh** file (where *version* is the number that identifies the software release version).
2. Connect to the IDP command-line interface in one of the following ways:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and enter **su -** to switch to root.
 - If you prefer, make a connection through the serial port and log in as root.



NOTE: To make an SSH connection, you must have enabled SSH for the management port (eth0). For details, see the ACM online Help.

3. Use SCP or FTP to copy the software image file to the IDP appliance. The IDP appliance does not run an FTP server, so you have to initiate the FTP session from the IDP appliance.
4. Run the upgrade script by entering **sh sensor_version.sh**, where *version* is the number that identifies the OS release version. When the script has finished, enter **reboot**.



NOTE: You might encounter unexpected behavior if you have changed the factory BIOS settings for the IDP Series device. We advise that you do not change the factory BIOS settings.

The console will hang at GRUB after reboot if you have changed the BIOS setting **Console redirection > Continue Console redirection after POST** to **ON**.

To resolve this issue, press the Delete key to enter BIOS and set this option to **OFF**.

5. In the NSM Device Manager, right-click the device, select **Adjust OS Version**, and complete the wizard steps.

The software upgrade is complete.

- Next Steps:**
1. If you are upgrading from IDP OS Release 5.0r1 or 5.0r2, skip this step. You completed it when you upgraded to IDP 5.0. If you are upgrading from IDP OS Release 4.1r4:
 - a. Run through the ACM wizard to **reconfigure your virtual routers**. In IDP 5.0 and later, you use ACM to configure deployment mode per virtual router.
 - b. If necessary, copy any custom settings from the backup copy of user_funcs to the new user_funcs file.
 2. Check to see if J-Security Center has released an update for the detector engine or attack database:

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.
 3. Push the updated IDP detector engine to IDP Series devices:

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.



NOTE: Updating the IDP detector engine on a device does not require a reboot of the device.

4. Push a security policy update job to update attack objects in use in your security policy:
 - a. In NSM, select **Devices > Configuration > Update Device Config**.
 - b. Select devices to which to push the updates and set update job options.
 - c. Click **OK**.

Resolved Issues

The following table describes issues that are resolved when you upgrade to from IDP OS 5.0r2 to IDP OS 5.1r1. If you are upgrading from IDP OS 5.0r1 or IDP OS 4.1r4, read the release notes for the subsequent releases to learn about the issues that were resolved in them.

Table 4: Resolved Issues

PR	Description
Previously Unsupported Functionality	
308133	IDP OS 4.1r4 did not support peer port modulation for 1 gigabyte fiber I/O modules. Beginning with IDP OS 5.0r2 (and continuing with IDP OS 5.1r1), we do support peer port modulation for 1 gigabyte fiber I/O modules.
Unexpected Behavior	
417818	Resolved an issue where the SYN Protector rulebase had failed to reset the destination server connections when configured in Passive mode.
430000	Resolved an issue that had caused speed and duplex settings to be auto-negotiated, even if auto-negotiation was not configured. The issue had occurred on IDP200, IDP6000, and IDP1100.
438306	Resolved an issue where the close client action had not functioned when processing VLAN tagged MPLS traffic.
439660	Resolved an issue where VLAN Q in Q traffic had not been distributed among the IDP engines (IDP8200).
510099	Resolved an issue with the Radius PAM module that had resulted in Radius authentication for SSH to fail.
543532	Resolved an issue with idpLogReader debug logs where the IP address bits had been displayed in reverse order. NSM displayed the logs correctly.
Configuration Issues	
517629	Resolved an issue where ACM had rejected Radius username formats containing a period (for example, john.doe).

Table 4: Resolved Issues (*continued*)

PR	Description
Detection Accuracy	
414795	Resolved an issue where APE rules could behave unexpectedly. If you configured a rule to drop Telnet traffic, for example, all traffic running over the standard Telnet port (port 23) would be dropped.
436273	Improved accuracy detecting attacks in highly fragmented HTTP traffic.
Logging / Packet Capture	
274827	All formats: Corrected log messages when an IDP rulebase rule matches ICMP or UDP attacks and the rule action is set to close client and server. The action actually taken is a drop connection. In previous releases, the log had been the action specified in the rule—"close client and server". In this release, we now report the action actually taken by the IDP Series device—"drop connection".
392392	Packet capture: You cannot use tcpdump to capture packets in both directions. In IDP OS Release 5.1, we support a new utility, called jnetTcpdump , that you can use to capture packets in both directions.
388321	Changed threshold: When traffic through the IDP Series device exceeds session capacity, the device generates an event log and drops the traffic (if the constant for logging implicit drops is enabled). To avoid generating many logs around a similar event, the IDP Series device does not log additional instances until a threshold is reached. In this release, we have changed the delay threshold from 1024 to 100 instances.
429095	Syslog: NIC state events reported in syslog messages had not indicated that the virtual router has returned to "Normal mode".
429097	Syslog: Changes in link status (link down or link up) had not been reported in syslog messages.
430766	NSM Profiler: Updates to Network Profile tab logs had lagged behind Protocol Profile tab logs. These two views are now updated simultaneously.
440475	NSM Log Viewer: Resolved an issue where variable data had not been displayed in the NSM Log Viewer collection.
493119	SNMP: The SNMP trap <code>jnxIdpSensorFreeDiskSpace</code> had been generated when the disk space exceeds the threshold but a downtrap had not been generated when it fell below the threshold.
495852	SNMP: In IDP OS 5.0r2 release notes, we reported that we had changed the polling interval for SNMP traps and SNMP polling to five minutes to decrease latency and CPU utilization for single core platforms (IDP600, IDP200, IDP75), where the IDP engine, JNET driver, and control plane processes share the same CPU. SNMP reporting has been improved in IDP OS Release 5.1. For single core platforms, CPU utilization is reported at 5 seconds, 1 minute, and 5 minutes. Traps are sent for the 1 minute and 5 minute intervals.
547870	Resolved an issue where the packet reassembly module had generated an inordinate number of logs for the same issue, leading to disk usage concerns.

Table 4: Resolved Issues (*continued*)

PR	Description
CPU Utilization	
474709	Resolved an issue where we had reported incorrect CPU utilization for single core platforms (IDP600, IDP200, IDP75). For single core platforms, you can now use the Linux top command to query CPU utilization. This value is reported to SNMP but not to NSM. For multicore platforms, you use the scio idp-cpu-utilization command and not the Linux top command.
502048	Resolved an issue where, if the IDP OS services were restarted while the device was processing traffic, the scio idp-cpu-utilization query returned 0 (an incorrect value).
552181	Resolved an issue on IDP8200 where IDP engine CPU load had been incorrectly reported as 0%.
Stability	
415604	Resolved an issue where the autorecovery feature had failed to restart an IDP engine in a hung state.
423847	We have changed the timeout for a TCP session marked for flow bypass to 60 seconds (was 5 seconds).
482866	Resolved an issue where the autorecovery process incorrectly considered the IDP engine to be in a hung state and consequently terminated the IDP engine. This had occurred during "All Attacks" policy push.
494931	Resolved an issue found in stress testing where continuously pushing a policies with APE rules would eventually result in policy push errors.
496207	Resolved an issue where running scio cpu-utilization command in single core platforms caused a drop in throughput and increase in latency.
497333	Resolved an issue where there had been a decrease in free packets after the auto-recovery process restarted the IDP engine (IDP1100, IDP600, IDP200 only).
497628	Improved code so that a core dump is generated more often when IDP engine crashes. However, under low memory conditions, a core dump might not be generated.
506585	Resolved an issue where memory had not been freed after successive policy pushes.
522406	Resolved an issue that had caused a kernel panic after reboot.
540685	Resolved an issue where the command to disable protocol decoding scio const -d set PROTOCOLNAME 0 had resulted in the device dropping traffic rather than passing it through as intended.
541187	Resolved an issue that had killed the autorecovery process before recovery was completed.
548261	Resolved a memory issue that had caused a detector engine update to fail when the security policy was large (IDP75).
560281	Changed implementation to avoid a memory leak issue that had been reported in 5.0r2.
567916	Resolved an issue where time updates from an NTP server stopped working after installing a patch release.

Table 4: Resolved Issues (*continued*)

PR	Description
Performance	
496205	Improved latency on single core platforms (IDP600, IDP200, IDP75).

Known Issues

The following table describes issues that are present in IDP 5.1r1.

Table 5: Known Issues

PR	Description
Unsupported Functionality	
497226	<p>A manually set IDP Series device system clock setting is not preserved after upgrading to 5.1r1.</p> <p>Workaround: Use NTP to set the IDP Series device system clock. If you do not want to use NTP, you can use ACM to reset the system clock after you have completed the upgrade.</p>
572045	<p>When you encounter a hung system, you might want to force a core dump. To do this, you type a SysRq key combination. You can use the SysRq key combination on IDP8200, IDP800, IDP250, and IDP75; but not IDP1100, IDP600, or IDP200.</p>
ACM	
286327	<p>Cosmetic issue: when no installed I/O module supports bypass, the ACM Configure Virtual Routers page should not display the user interface group for NIC State. When no installed I/O module supports bypass, NIC state is non-configurable.</p>
298918	<p>ACM does not reject poorly formed alias names. In particular, ACM does not reject constructions with incomplete double-quote strings. For example, "hello (missing end-quote). As a result, the alias name does not appear in NSM.</p> <p>To avoid this issue, be careful to use complete double-quote constructions for alias names. For example, "hello".</p>
Detection Accuracy	
279408	<p>UDP port scanning works if there is no response from the Victim PC. However, if the response comes in the form of "UDP Port not reachable," the detection ignores the flow because the response packet is more than 20 bytes (default value).</p> <p>To work around this issue:</p> <ol style="list-style-type: none"> 1. In the NSM Device Manager, double-click the name of the device to display the configuration editor. 2. Click Sensor Settings. 3. Click the Run-time parameters tab. 4. Under Traffic Signatures, increase the value for Byte threshold for suspicious flows.

Table 5: Known Issues (*continued*)

PR	Description															
508363	False positive where SSL:Audit:Non-SSL is wrongly detected in HTTPS traffic. The issue only occurs when SSL:Audit:Non-SSL is included in a compound signature with another member having stream256 context.															
Configuration																
303672	In custom attack objects, in attack signatures, negation inside case-insensitive block is not supported. To work around this issue, rewrite the signature to avoid negation inside a case-insensitive block.															
415301	Policy validation through NSM does not return a warning if the APE rulebase rate limit you specify exceeds the ingress and egress capacity of device. You must be careful to consider the capacity of your links when you specify APE rulebase rate limiting actions.															
426720	In the following scenario, NSM policy validation should report a rule shadowing condition because the second rule could never be applied. <table border="1" data-bbox="354 827 1170 961"> <thead> <tr> <th>Rule</th> <th>Source</th> <th>Destination</th> <th>Service</th> <th>Attacks</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>any</td> <td>any</td> <td>HTTP</td> <td>All SMTP attacks</td> </tr> <tr> <td>2</td> <td>any</td> <td>any</td> <td>HTTP</td> <td>All HTTP attacks</td> </tr> </tbody> </table> <p>Traffic to port 80 would be inspected for only SMTP attacks and not HTTP attacks.</p>	Rule	Source	Destination	Service	Attacks	1	any	any	HTTP	All SMTP attacks	2	any	any	HTTP	All HTTP attacks
Rule	Source	Destination	Service	Attacks												
1	any	any	HTTP	All SMTP attacks												
2	any	any	HTTP	All HTTP attacks												
431702	You must be careful configuring speed and duplex for IDP75 and IDP800 onboard interfaces and IDP8200 I/O module copper interfaces. The speed and duplex setting for the IDP Series interfaces and the peer switch or firewall interfaces must match. The best practice is to set both to AUTO. If you do not use auto-negotiation on both sides, you must ensure the explicitly specified speed and duplex settings match. <p>We have observed traffic dropping if the IDP Series interfaces are configured as 100/10/1000 half/full duplex (AUTO-OFF) and the peer switch or firewall is configured as AUTO-ON.</p>															
536881	The NSM object editor does not enforce correct use of the within bytes constraint for custom signature attack objects. <p>When you set a byte range constraint, you set a start point that is Context, Packet, or Stream. Your selection must be consistent with the pattern context setting for the attack object. For example, if you configured one of the service contexts, select Context. If you configured one of the packet contexts, select Packet. If you configured one of the stream contexts, select Stream.</p> <p>In NSM, it is possible to select a start point that is inconsistent with the pattern context setting. For example, the NSM object editor allows you to configure a pattern context http-variable and then set a within bytes start point that is start-of-packet. However, the within bytes match logic will be resolved to the start point you should have selected: context.</p>															
536967	When you configure a custom signature attack object, you can optionally set multiple within bytes constraints. Multiple entries are evaluated as a Boolean OR. This PR is to track a request for support for cases where you would want multiple entries processed as a Boolean AND.															
537217	If you change the third-party HA setting (enable to disable, and vice versa), ACM reboots the device.															
537481	IDP OS Release 5.1 does not support the within bytes constraint for custom compound attack objects.															

Table 5: Known Issues (*continued*)

PR	Description
538247	When you configure a custom compound attack object, you can optionally set within packets constraints. If you set a packet constraint for one member, the program logic counts packets beginning implicitly with the start-of-stream. Request is to include a UI option to specify the starting point.
539399	In ACM, you have the option to use a Radius server as an authentication source for access to ACM. However, the username format allowed by the ACM configuration page does not support all formats deemed valid by RFC 2486. In IDP OS Release 5.1, you can specify a usernames that include periods (such as john.doe), but not special characters such as @ or + that are conventions in the username formats used by some enterprises (such as john.doe@company.com).
552167	HA deployment has an IDP system requirement that a virtual router named vr0 contain eth1 (the HA state sync interface). If you upgrade an IDP OS 4.1r4 device that has HA enabled, eth1 is added to vr0 automatically. Otherwise, you must check the ACM Configure Virtual Routers page to ensure this HA system requirement is met. This requirement only applies if the device belongs to an HA deployment.
Monitoring / Console	
288824	Under high traffic conditions, the following exception messages are displayed in the console: <pre>ata1.00: exception Emask 0x2 SAct 0xfe SErr 0x400000 action 0x2 frozen ata1.00: (spurious completions during NCQ issue=0x0 SAct=0xfe FIS=005040a1:00000001) ata1.00: cmd 61/30:08:8d:6e:16/00:00:00:00:00/40 tag 1 cdb 0x0 data 24576 out res 50/00:38:a5:70:16/00:00:00:00:00/40 Emask 0x2 (HSM violation)</pre> <p>You can safely ignore these messages.</p>
428341	During upgrade with NSM, the NSM Job Information window displays status information that is not consistent with the operations occurring on the IDP Series device.
438582	The NSM software version inventory fails to identify a patch version number when you add the IDP Series device or import a IDP Series device configuration. To work around this issue, you can use the NSM Device Manager to run an Adjust OS operation or use the IDP CLI to run idp.sh restart . However, the problem will recur following add device or import configuration procedures.
416086	The NSM Process Status lists dLogPurger status, which is not a active process in IDP Series devices.
573995	On IDP8200, the scio idp-cpu-utilization utility shows an incorrect CPU utilization for idpengine_0.
Logging / Packet Capture	
227241, 416708	Profiler is unable to capture the OS fingerprint for some destination servers. Reports show "Unknown OS".
287179	After system unavailability, the IDP Series device does not send a log that the device has returned to normal operations.
407900	In NSM log viewer, the strings for log severities for IDP Series devices are inconsistent with other network devices. For IDP Series devices, strings for severity include Device_critical_log and Device_warning_log instead of the strings Critical and Warning that appear for other network devices.
415164	In NSM, packet data cannot be displayed correct for certain malformed IP packets.

Table 5: Known Issues (*continued*)

PR	Description
418220	Logs to IC Series: When log suppression is enabled, logs sent to the IC Series should indicate the repeat count when applicable.
419544	In NSM Profiler logs, alert logs when Profiler detects a new, non-IP protocol always show the protocol as HOPOPT instead of the specific protocol.
423852	In NSM log viewer, the value in the Subcategory column for flow bypass and autorecovery logs is Other. We expect the value to identify the flow bypass or autorecovery event more specifically.
427100	Syslog issue: autorecovery events reported in syslog messages do not indicate which IDP engine restarted.
429086	Database limit exceeded alert log are not displayed in Profiler logs.
437768	We have observed a minor loss of application volume tracking (AVT) data if the AVT .stat file is larger than 1 GB.
446451	Logs generated when a Radius user accesses ACM are not sent to the syslog server. Such logs are sent to NSM.
462005	IDP Reporter Application reports show incorrect statistics for bytes transferred. The report shows only client-to-server bytes, not total bytes.
462680	Request to change content of some syslog messages so they are more useful when viewed through syslog readers, such as STRM.

Table 5: Known Issues (*continued*)

PR	Description
575772	<p>SNMP: For IDP8200 only, the values reported for the following MIB objects are incorrect:</p> <ul style="list-style-type: none"> • jnxIdpSensorFreePktBuffersFiveSec.0 • jnxIdpSensorFreePktBuffersOneMin.0 • jnxIdpSensorPktsRxdPerIntfcTable • jnxIdpSensorPktsTxRatePerIntfcTable • jnxIdpSensorPktsDropOnAllIntfc.0 • jnxIdpSensorSignatureStatsTable • jnxIdpSensorTopTenSignatureStatsTable <p>As a workaround, you can use NSM and IDP Reporter top attack reports to see the data for signature matches. You can log into the CLI and use the jnetStats command to retrieve packet buffer and packet transmission statistics. For example:</p> <pre>[root@defaulthost ~]# jnetStats .././jnetLib.c built on Dec 20 2010 at 23:05:51 with PRODUCTION build of SALEEN -43e. -- Worker Id 0 Stats: freePackets: 444032 dropCount: 0 -- Thread Id 0 Stats: rxPackets: 20846535763 rxBytes: 14757418499789 rxOverflow: 0 rxQueued: 0 txComplete: 18487802326 txCompleteBytes: 14691015670286 allocQueueSize: 1023 txPackets: 18487802326 txBytes: 14692307273740 -- Device Id 0 (eth2) Stats: Link Status: Down rxPackets: 0 rxBytes: 0 rxOverflow: 0 txPackets: 0 txBytes: 0 [...]</pre>
High Availability	
550567	Synchronization from primary device to backup device includes updates to the application identification matches for predefined signatures (the appsig cache). Updates do not include cached entries for custom applications or extended applications (the extappsig cache).
558837	Due to a hardware limitation, interface signaling is not supported for IDP8200 10 gigabyte fiber interfaces.
559087	We do not support attack detection (flow-based or packet-based) in synced sessions processed by the standby device after retransmission on the redundant path. Packets for these sessions are passed through, uninspected. New sessions traversing the redundant path are inspected.

Table 5: Known Issues (*continued*)

PR	Description
CPU Utilization	
434539	In the NSM Device Monitor > View Device Details > Process Status tab, the CPU usage for the IDP engine is reported as 0%. To see the actual CPU usage for an IDP engine, log into the IDP Series device command-line interface (CLI) and use the <code>scio idp-cpu-utilization</code> command (multicore platforms) or Linux <code>top</code> command (single-core platforms). The correct CPU usage is also reported via SNMP.
Stability	
430363	IDP8200 stops processing traffic at high load with SYN protection enabled.
499447	For single core platforms (IDP75, IDP200, IDP600), we recommend you disable application volume tracking (AVT). AVT processes are CPU intensive, resulting in link flapping under stress. Note that if you disable AVT, IDP Reporter application volume reports are empty.
573031	Low memory triggered JNET bypass on IDP800.
Expected Behavior	
547354	Packet drops are possible in simulation mode if the JNET free packet buffer is 0.
Shutdown Operation	
432893	The <code>shutdown -h now</code> command might not behave as expected if you deploy IDP8200 with any of the following fiber I/O modules: IDP-1GE-4SX-BYP, IDP-10GE-2XFP, or IDP-10GE-2SR-BYP. Instead of shutting down, the OS unexpectedly restarts. This issue has been reported only in the initial shipments of this hardware. For details and a solution, contact JTAC.
Documentation	
424045	In NSM Device Manager, a new configuration section for Report Settings does not include online help. For information about the report settings you can configure with NSM, see the “ IDP Logs and Reports in NSM Task Summary ” section in the <i>IDP Series Administration Guide</i> .

Documentation

You can download user documentation from the Juniper Networks Web site:
<http://www.juniper.net/techpubs/>.

Table 6 on page 20 lists related IDP Series documentation.

Table 6: Related IDP Series Documentation

Document	Description
IDP Detector Engine release notes	Provides information about IDP Detector Engine releases, including new features, changed features, fixed problems, and known issues.

Table 6: Related IDP Series Documentation (*continued*)

Document	Description
J-Security Center Attack Signatures	Lists predefined attack signatures developed by J-Security Center.
J-Security Center Application Signatures	Lists predefined application signatures developed by J-Security Center.
IDP Series installation guides	Describes IDP Series hardware and provides instructions for installing, configuring, updating, and servicing the device.
IDP Series Feature Documentation	A collection of topics from the <i>IDP Series Administration Guide</i> and <i>IDP Series Concepts and Examples Guide</i> , in HTML.
<i>IDP Series Administration Guide</i>	Provides procedures for completing IDP Series administration tasks with the Network and Security Manager (NSM) central management program; with the IDP Series device Appliance Configuration Manager (ACM); and with the IDP Series device command-line interface (CLI).
<i>IDP Series Concepts and Examples Guide</i>	Explains IDP Series features and provides examples of how to use the system.
<i>IDP Series Custom Attack Objects Reference and Examples Guide</i>	Provides examples and reference information for creating custom attack objects.
<i>IDP Reporter User's Guide</i>	Describes how to use IDP Reporter, an on-box reporting platform that includes predefined reports on attack detection and application usage. You can also use IDP Reporter to schedule regular publication of reports that are of interest to you or your stakeholders.

Table 6 on page 20 lists related NSM documentation.

Table 7: Related NSM Documentation

Document	Description
Network and Security Manager release notes	Provides information about new features, changed features, fixed problems, and known issues with the NSM release.
<i>Network and Security Manager Installation Guide</i>	Describes how to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NSM.
<i>Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide</i>	Describes how to configure and manage IDP Series devices using NSM. This guide also helps in understanding of how to configure basic and advanced NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, viewing log information, and monitoring the status of IDP Series devices.

Table 7: Related NSM Documentation (*continued*)

Document	Description
<i>Network and Security Manager Administration Guide</i>	<p>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI.</p> <p>This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</p>
Network and Security Manager Online Help	Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.

Getting Help

If you need additional information or assistance, contact Juniper Networks Technical Assistance Center (JTAC) by E-mail (support@juniper.net) or telephone (1-888-314-JTAC within the United States or 1-408-745-9500 from outside the United States).

Copyright © 2009, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.