

Intrusion Detection and Prevention IDP 5.0 Release Notes

September 25, 2009
Part Number: 530-029724-01
Revision 03

Contents

Overview	2
Feature Parity	2
New Features	2
Changed Features	3
Removed Features	4
Unsupported Features	5
Supported Upgrade Paths	5
Downgrading or Reverting	5
Licensing	5
Compatibility with Network and Security Manager	5
Compatibility with Juniper Networks Infranet Controller	6
Browser Requirements	6
Upgrading IDP Software	6
Upgrading with NSM	6
Upgrading with the CLI	8
Resolved Issues	10
Known Issues	12
Documentation	15
Getting Help	16

Overview

Juniper Networks Intrusion Detection and Prevention Series devices enable you to enforce a security policy that protects your network from attacks and gather information about applications, clients, 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.

Feature Parity

This software release supports the following IDP appliance models: IDP75, IDP200, IDP250, IDP600, IDP800, IDP1100, IDP8200. All of these models now support the same feature set. Table 1 on page 2 describes the features added to IDP in this software release to achieve feature parity.

Table 1: Support Add to IDP Appliance Models to Achieve Parity

IDP75, IDP200, IDP250, IDP600, IDP800, IDP1100	IDP8200
Multicore architecture	<ul style="list-style-type: none"> ■ Backdoor rulebase ■ Honeypot rulebase ■ Inspection of decrypted traffic (SSL) ■ Inspection of encapsulated traffic (GRE, GTP) ■ Profiler, including application volume tracking and OS fingerprinting ■ Packet capture and packet logging ■ External bypass ■ Support for <code>scio ccap</code> and <code>scio pcap</code> commands

New Features

This release includes the following new features:

- Application policy enforcement (APE) rulebase.
- NSM support for application volume tracking (AVT).
- User-role-based rules in the IDP rulebase and APE rulebase.
- Autorecovery of IDP engines.
- Flow bypass when the IDP engine experiences heavy load.
- Deployment mode per virtual router, enabling a single appliance to be deployed in transparent and sniffer mode.
- Inspection of IPsec ESP NULL traffic.

- Inspection of MPLS traffic.
- Support for jumbo frames.
- Diagnostic tools:
 - **scio idp-cpu-utilization**. Displays actual CPU utilization of IDP engines.
 - **scio var -s s0 -f outfile flowtable**. Writes the output of the `scio var` command to the specified filename.
 - **scio subs service detail s0**. Displays the active and total session count, by service.

Changed Features

The following features have changed:

- In the Appliance Configuration Manager (ACM), you now specify deployment mode per virtual router, not per device. By design, adjacent interface pairs make up a virtual router. For example, interface eth2 and interface eth3 make up vr0; eth4 and eth5 make up vr1; and so forth.

If you are upgrading an appliance that has been deployed in transparent mode, we recommend you run the ACM wizard to review the [configuration for your virtual routers](#). We do not expect issues, but we nonetheless recommend you verify your ACM settings after upgrade.

If you are upgrading an appliance that has been deployed in sniffer mode and had used multiple sniffer interfaces, you *must* run the ACM wizard to ensure the correct configuration. Here is why: before IDP 5.0, all interfaces for an appliance deployed in sniffer mode were automatically assigned to virtual router vr0. When you upgrade to IDP 5.0, vr0 contains only interface eth2 and interface eth3, not all interfaces. If you want to use eth4 or eth5 as a sniffer interface, for example, you must explicitly activate vr1 and select sniffer mode.

- In ACM, NIC state options for IDP200, IDP600, and IDP1100 are now the same as those for IDP75, IDP250, IDP800, and IDP8200: NICs off, NIC bypass, External bypass. Use **NICs off** for cases where you previously had used **Normal**.
- If you configure NTP, the IDP appliance synchronizes its clock to the NTP server clock one time per day. You use ACM to configure NTP. To facilitate your analysis of logs and reports, we recommend you synchronize your network devices to the same NTP server. For details on configuring NTP, see the ACM online help.
- You now use NSM and not ACM to set maximum packet captures and logs stored. To change this setting in the NSM Device Manager, double-click the IDP device and select **Report Settings**. The defaults have also changed. The default maximum packet captures stored on the IDP device is now 10,000. The default number of log files stored is now 50,000.
- You now use NSM to enable/disable application identification. Application identification is enabled by default. To change this setting in the NSM Device Manager, double-click the IDP device and select **Sensor Settings**.

- You now use NSM to enable/disable application volume tracking. Application volume tracking is enabled by default. To change this setting in the NSM Device Manager, double-click the IDP device and select **Profiler Settings**.
- In the NSM Profiler Viewer, the Application Profiler tab is now used for application volume tracking logs. The previous functionality on the Application Profiler tab is now on the Protocol Profiler tab.
- The default for maximum frame size has been changed from Ethernet frame size (1514 bytes) to jumbo frame size (9014 bytes). You can configure an even larger frame size if necessary. The maximum frame size is 16,014 bytes.
- The maximum number of TCP/UDP/ICMP/Other sessions has increased for the following platforms:
 - IDP75 - 100,000
 - IDP250 - 300,000
 - IDP800 - 1,000,000
- We have greatly improved the policy loading time, especially for IDP8200. In previous releases, a policy load operation could take 10 to 20 minutes, depending on the policy size. Policy load now takes 1 to 2 minutes, depending on the policy size.
- The **Use alternate ports as http service** setting that appears in the NSM configuration editor Protocol Thresholds and Configuration tab is no longer used. The IDP engine now automatically detects HTTP traffic over any port.
- Advanced users should be aware that default and valid values have changed for the **scio const set sc_max_busy_packet_mem** command. You now specify a percentage of memory usage rather than a number of bytes. The default is 5 percent. Most users should not change the defaults related to memory.

Removed Features

The following features have been removed:

- Bridge mode.
- Proxy-ARP mode.
- Router mode.
- VLAN retagging (previously supported only in bridge, proxy-ARP, and router mode).
- Support for the **statview** utility has been reduced. In IDP 5.0, we support only the **statview view** command. You must use IDP Reporter, Application Usage Manager, or NSM to view application volume reports.

Unsupported Features

The following features are not supported in IDP 5.0:

- High availability (standalone or third-party).
- IDP50. You cannot run IDP 5.0 software on the IDP50 appliance.
- SSL decryption using IDEA-based algorithms or ciphers.
- IDP 8200 10 Gigabit Ethernet interfaces do not support peer port modulation (PPM).
- On IDP800, the following I/O modules do not support peer port modulation:
 - 4-port 1-GigE fiber SFP (without internal bypass) (IDP-1GE-4SFP)
 - 4-port 1-GigE fiber SX (with internal bypass) (IDP-1GE-4SX-BYP)
- Authentication to the ACM via RADIUS with RSA SecurID (authentication via RADIUS server is supported).

Supported Upgrade Paths

You can upgrade directly from any of the following versions:

- 4.2r2
- 4.2r1
- 4.1r3

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.

Licensing

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

Compatibility with Network and Security Manager

The new features in this release require Network and Security Manager (NSM) 2008.2r2 (May 2009).

Compatibility with Juniper Networks Infranet Controller

The user-role-based policy feature depends on deployment with Unified Access Control (UAC) 3.0r1 or later.

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 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.

The upgrade to IDP 5.0 reimages the disk with a new operating system. All partitions except `/var/idp` are rewritten. The upgrade process restores your license and most of your previous settings. The following settings are not preserved:

- The upgrade does not retain settings no longer supported in IDP 5.0.
- 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 5.0.
- Due to a known issue, the upgrade does not preserve SSL keys previously added to support decryption of traffic to SSL servers.

You can use NSM or the CLI to upgrade IDP software. You must use NSM to complete the IDP detector engine and attack object updates. This section provides the following upgrade workflows:

- Upgrading with NSM on page 6
- Upgrading with the CLI on page 8

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 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 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 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 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.
9. In the NSM Device Manager, right-click the IDP device and select **Import Device**.

The software upgrade is complete.

Next Steps:

1. Run through the ACM wizard to [reconfigure your virtual routers](#). In IDP 5.0, you use ACM to configure deployment mode per virtual router.
2. If necessary, copy any custom settings from the backup copy of user_funcs to the new user_funcs file.

3. If applicable, [re-add SSL server private keys to the IDP keystore](#). For procedures, see the *IDP Administration Guide*.
4. 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.

5. Push the updated IDP detector engine to IDP 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.

6. 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 device. You still use NSM to update the detector engine and attack objects.

To upgrade IDP software 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. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote)**. In the row for IDP, click **5.0**.
 - c. 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 software release version. When the script has finished, enter **reboot**.
5. In the NSM Device Manager, right-click the device, select **Adjust OS Version**, and complete the wizard steps.
6. In the NSM Device Manager, right-click the IDP device and select **Import Device**.

The software upgrade is complete.

Next Steps:

1. Run through the ACM wizard to [reconfigure your virtual routers](#). In IDP 5.0, you use ACM to configure deployment mode per virtual router.
2. If necessary, copy any custom settings from the backup copy of user_funcs to the new user_funcs file.
3. If applicable, [re-add SSL server private keys to the IDP keystore](#). For procedures, see the *IDP Administration Guide*.
4. 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.

5. Push the updated IDP detector engine to IDP 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.

6. 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 issues are resolved when you upgrade to IDP 5.0r1:

- PR 278471. In IDP 4.2r2, the **scio ccap all** command was not supported. In IDP 5.0, this command is supported.
- PR 286020. In ACM, the default interface setting for all interfaces is now **NICs OFF**.
- PR 287003. In IDP 4.2r2 release notes, we reported an issue with the ACM Configure Forwarding Interfaces page: the NIC State drop-down list boxes should not include **External Bypass** because IDP 4.2r2 did not support external bypass. This issue is not applicable to IDP 5.0. External bypass is supported.
- PR 288644. In IDP 4.2r2 release notes, we reported an issue with NIC OFF logs: these logs were erroneously sent for non-sniffing interfaces (when IDP is in sniffer mode). This issue is not applicable to IDP 5.0. In IDP 5.0, NIC state is not set for sniffer interfaces.
- PR 288651. Resolved an issue where NIC OFF log messages were displayed for interfaces that are not selected as forwarding interfaces. We reported this issue in the IDP 4.2r2 release notes.
- PR 288663. Resolved an issue where link status (up/down) messages did not appear when the device comes up. We reported this issue in the IDP 4.2r2 release notes.
- PR 299413. In IDP 4.2r2 release notes, we reported an issue with error messages when installing I/O modules: if the number of interfaces is fewer than six, you encountered ACM or console messages indicating “cannot find eth6 and eth7.” This issue is not reproducible in IDP 5.0.
- PR 297270. In IDP 4.1r3 release notes, we reported that IDP Reporter is not compatible with Mozilla Firefox 3.0. In IDP 5.0, we have verified compatibility with Firefox 3.0.
- PR 307900. Resolved an issue with IDP Reporter where the Top Activities report displayed “No data available.”
- PR 310511. Resolved an issue that had caused some attacks in HTTPS traffic to go undetected. The root cause of this problem appears to have been an

insufficient SSL buffer size. In IDP 4.1r3, the buffer size was increased from 8 to 32 bytes to resolve this issue. In IDP 5.0, the buffer size is also 32 bytes.

- PR 312966. Resolved a link flapping issue related to peer port modulation that had been reported on IDP800 with copper I/O modules.
- PR 390652. In IDP 4.1r3, IDP 50/200/600/1100 required a patch to support internal bypass for copper ports. In IDP 5.0, a patch is not required. Note that IDP 5.0 supports IDP200, IDP600, IDP1100 but not IDP50.
- PR 397564. Resolved a link flapping issue that had been reported on IDP800 copper I/O modules and IDP250 copper ports. We reported this issue in IDP 4.1r3 release notes and addressed it with the IDP 4.1j2 patch.
- PR 399529. In IDP 4.1r3, an issue with PPM incorrectly identifying link status had caused frequent interface flaps. The issue was addressed with the IDP 4.1j2 patch. With IDP 5.0, a patch is not required.
- PR 401177. Resolved an issue that had caused high CPU usage to be reported for IDP800. We reported this issue in IDP 4.1r3 release notes.
- PR 400869. In IDP 4.1r3, an attack object update had failed for signatures VOIP:SKYPE:LOGIN-1 and VOIP:SKYPE:LOGIN-2 with error “Missing member VOIP:SKYPE:LOGIN-1.” The issue was addressed with the IDP 4.1j2 patch. With IDP 5.0, a patch is not required.
- PR 406411. Resolved an issue with the way the application identification feature handled RSH traffic. This was fixed in IDP 4.2r2. The fix is available to IDP200, IDP600, IDP1100, IDP75, IDP250, and IDP800 through upgrade to IDP 5.0.
- PR 409316. Resolved an issue where NSM had incorrectly reported protocol for port 445 as HOPOPT instead of TCP.
- PR 411971. Resolved an issue where NSM logs erroneously indicated VLAN ID for traffic that did not have a VLAN ID.
- PR 412490. In IDP 4.2r2 release notes, we reported an issue with logs for 1 Gigabit Ethernet copper traffic interfaces and 10 Gigabit Ethernet fiber (with bypass) traffic interfaces. IDP had correctly logged the event that the virtual router has entered bypass, but it did not log the event where IDP has returned to normal operations. This issue is not present in IDP 5.0.
- PR 412491. In IDP 4.2r2 release notes, we reported an issue with logs for 1 Gigabit Ethernet fiber (with bypass) traffic interfaces. IDP had correctly logged the event that the virtual router has entered NICs off state, but it did not log the event where IDP has returned to normal operations. This issue is not present in IDP 5.0.
- PR 412494. In IDP 4.2r2 release notes, we reported an issue with logs for 1 Gigabit Ethernet fiber (with bypass) traffic interfaces. IDP had incorrectly logged the event where IDP returns to normal operations after a period in bypass state. In the log, in the column for interface, IDP reported only one interface of the virtual router pair. For example, it insufficiently reported the interface as **interface = ,eth5** instead of **interface = eth4,eth5**. This issue is not present in IDP 5.0.
- PR 414417. Resolved an SNMP issue with IDP8200. The issue had resulted in failed `snmpget` requests.

- PR 421001. Resolved an issue with Close Client, Close, and IP Action: Close. We reported this issue in IDP 4.2r2 release notes.
- PR 424795. In 4.1r2 and 4.1r3, there was an issue with the peer port modulation feature. Immediately after the feature was enabled or disabled, the link speed for traffic interfaces configured for auto-negotiation would fall from 1 Gbps to 100 Mbps. This issue is not present in IDP 5.0.
- PR 426869. In IDP 4.1r3, link flapping related to NIC bypass operations during high CPU stress was reported on IDP200 and IDP600. The issue is not reproducible in IDP 5.0.
- PR 424919. Resolved an issue where IDP8200 had sent TCP challenge packets out from the wrong interface.
- PR 428900. Resolved an issue with IDP Reporter where a Profile SMTP and email address could not be saved.
- PR 431769. Resolved an issue reported in IDP 4.2r2 related to the application volume tracking feature that had resulted in a segmentation fault.
- PR 432575. The event severity reported in syslog logs is now the same as NSM logs.
- PR 441030. Resolved an issue reported in 4.2r2 that had resulted in a segmentation fault when detector update and policy push jobs were processed.
- PR 443972. Resolved an issue where the Recommended action coded in a traffic anomaly attack object was not the action taken.

Known Issues

The following issues have been reported in this release:

- PR 279408. 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).

To work around this issue:

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**.
- PR 286327. 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.
 - PR 287179. After system unavailability, IDP does not send a log that IDP has returned to normal operations.

- PR 288824. Under high traffic conditions, the following exception messages are displayed in the console:

```
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:16/00:00:00:00/40
tag 1 cdb 0x0 data 24576 out res 50/00:38:a5:70:16/00:00:00:00/40 Emask
0x2 (HSM violation)
```

You can safely ignore these messages.

- PR 298918. 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.

To avoid this issue, be careful to use complete double-quote constructions for alias names. For example, “hello”.

- PR 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.
- PR 388321. When traffic through the IDP appliance exceeds session capacity, the IDP 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 appliance does not log additional instances until 1024 additional instances have occurred. We have received a request to make this delay value (1024) configurable.
- PR 392392. Unable to capture traffic in both directions with `tcpdump` when packet capture has been enabled with the `scio const set sc_pcap_outbound_pkts 1` command.
- PR 407900. In NSM log viewer, the strings for log severities for IDP devices are inconsistent with other network devices. For IDP 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.
- PR 415164. In NSM, packet data cannot be displayed correct for certain malformed IP packets.
- PR 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.
- PR 417818. The SYN Protector rulebase fails to reset the destination server connections when configured in Passive mode. To avoid this issue, use Relay mode instead.
- PR 417869. The SYN Protector rulebase, when configured in Relay mode, is not triggered when processing SYN packets with Explicit Congestion Notification (ECN) and Congestion Window Reduced (CWR) flags enabled.
- PR 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.

- PR 423852. In NSM log viewer, the value in the Subcategory column for flow bypass and auto-recovery logs is Other. We expect the value to identify the flow bypass or auto-recovery event more specifically.
- PR 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 *IDP Administration Guide*.
- PR 426720. In the following scenario, NSM policy validation should report a rule shadowing condition because the second rule could never be applied.

Rule	Source	Destination	Service	Attacks
1	any	any	HTTP	All SMTP attacks
2	any	any	HTTP	All HTTP attacks

Traffic to port 80 would be inspected for only SMTP attacks and not HTTP attacks.

- PR 427100. Syslog issue: auto-recovery events reported in syslog messages do not indicate which IDP engine restarted.
- PR 428341. During upgrade to IDP 5.0 with NSM, the NSM Job Information window displays status information that is not consistent with the operations occurring on the IDP device.
- PR 429095. Syslog issue: NIC state events reported in syslog messages do not indicate that the virtual router has returned to “Normal mode”. NSM logs do indicate this in the Subcategory column.
- PR 429097. Syslog issue: changes in link status (link down or link up) are not reported in syslog messages. These events are reported to NSM and appear in the Details column.
- PR 430766. In NSM Profiler, updates to Network Profile tab logs lag behind Protocol Profile tab logs. We expect updates to these two views to be in sync.
- PR 432844, PR 438631. After upgrading to IDP 5.0, the packet storage limit setting (global.pktDataCount) in idp.cfg retains the values configured with ACM in 4.1r3. This can result in unexpected or problematic behavior. Both the supported configuration tool and the default values have changed. See “Changed Features” on page 3. If your 4.1r3 values are outside of the valid range supported in IDP 5.0, we recommend you use NSM to configure values within the valid range and push a configuration update from NSM.
- PR 432893. The **shutdown -h now** 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. For details and a solution, contact JTAC.
- PR 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 appliance command-line interface (CLI) and use the **scio idp-cpu-utilization** command. The correct CPU usage is also reported via SNMP.

- PR 434910. The `scio pcap` command does not work if you have deployed your IDP appliance in mixed mode (one or more virtual routers in transparent mode and one or more in sniffer mode). The `scio pcap` command requires an IDP appliance where all interfaces are configured in sniffer mode.
- PR 438582. The NSM software version inventory fails to identify a patch version number when you add the IDP device or import a IDP 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.
- 440919. The upgrade to IDP 5.0 does not preserve previously installed SSL private keys used to decrypt traffic to SSL servers. You must re-add them after you upgrade. For procedures, see the *IDP Administration Guide*.
- PR 444301. After upgrading to IDP 5.0, the incorrect detector version appears in NSM. To resolve this, re-import the device configuration. From Device Manager, right-click the IDP device and select **Import Device**.

Documentation

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

Table 2 on page 15 lists related IDP documentation.

Table 2: Related IDP Documentation

Document	Description
IDP Detector Engine release notes	Provides information about new features, changed features, fixed problems, and known issues with the IDP Detector Engine release. You can download these release notes from the following location: http://www.juniper.net/techpubs/software/management/idp/de/index.html
<i>IDP Installation Guide</i>	Describes IDP hardware and provides instructions for installing, configuring, updating, and servicing the device.
IDP Series Pathway Pages	A collection of topics from the <i>IDP Administration Guide</i> and <i>IDP Concepts and Examples Guide</i> , in HTML.
<i>IDP Administration Guide</i>	Provides procedures for completing IDP administration tasks with the Network and Security Manager (NSM) central management program; with the IDP device Appliance Configuration Manager (ACM); and with the IDP device command-line interface (CLI).
<i>IDP Concepts and Examples Guide</i>	Explains IDP features and provides examples of how to use the system.
<i>IDP Custom Attack Objects Reference and Examples Guide</i>	Provides examples and reference information for creating custom attack objects.

Table 2: Related IDP Documentation (continued)

Document	Description
<i>IDP Reporter User's Guide</i>	Describes how to use IDP Reporter. The IDP Reporter features and user interface are similar to the Juniper Networks Application Usage Manager features and user interface. Where IDP Reporter includes application usage and attack data for a single IDP device, the application usage manager can aggregate this data for multiple devices and correlate it with subscriber data obtained from SRC devices.

Table 2 on page 15 lists related NSM documentation.

Table 3: 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 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 devices.
<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.