

# IDP Series Release Notes

## IDP OS 5.1r4

July 20, 2017  
Revision 03

### Contents

Overview . . . . .	2
Supported Hardware . . . . .	2
New and Changed Features . . . . .	2
Unsupported Features . . . . .	2
Known Limitations . . . . .	3
Supported Upgrade Paths . . . . .	3
Downgrading or Reverting . . . . .	4
Licensing . . . . .	4
Compatibility with Network and Security Manager . . . . .	4
Compatibility with Juniper Networks Infranet Controller . . . . .	4
Browser Requirements . . . . .	4
Upgrading Software on an HA Cluster . . . . .	4
Upgrading Software on a Standalone Device . . . . .	5
Upgrading with NSM . . . . .	5
Upgrading with the CLI . . . . .	7
Resolved Issues . . . . .	8
Known Issues . . . . .	10
Errata . . . . .	18
IDP Series Custom Attack Objects Reference and Examples Guide . . . . .	18
Documentation . . . . .	19
Documentation Feedback . . . . .	20
Revision History . . . . .	20

## Overview

---

Juniper Networks Intrusion Detection and Prevention Series devices enable you to enforce a security policy that leverages continuous security research by the Juniper Networks [Security Intelligence 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 5.1r4 is supported on the following platforms:

- IDP8200, IDP800, IDP250, IDP75

## New and Changed Features

---

There are no new features introduced in IDP OS Release 5.1r4. If you are not familiar with IDP OS 5.1 features, see the [IDP OS Release 5.1r1 release notes](#).

## Unsupported Features

---

The following features are not supported in IDP OS Release 5.1r4:

- SSL decryption using IDEA-based algorithms or ciphers. This feature is also not supported in IDP OS Release 5.0.x.
- On IDP8200, 10 Gigabit fiber interfaces do not support interface signaling or peer port modulation. This feature is also not supported in IDP OS Release 5.0.x.
- Authentication to the ACM through RADIUS with RSA SecurID.

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 platform IDP75, 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:

- 5.1r3



**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 device (such as a 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 1 on page 3](#) describes the changes to files and directories you will notice when you upgrade.

**Table 1: Changes to Files, Directories, and Key Settings**

Upgrade Path	Files and Directories
From 5.1r3	No special changes to attend to before or after upgrade.

## 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 IDP OS Release 5.1r4, we verified compatibility with the following release of Network and Security Manager (NSM):

- NSM 2012.2R9

You can download the NSM client and server software from the Juniper Customer Support Software Download website:

<http://www.juniper.net/customers/support/softserv.jsp>



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.

## Browser Requirements

---

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

- Internet Explorer 10.x, 11.x
- Firefox 35.x

## Upgrading Software on an HA Cluster

---

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 Software on a Standalone Device

---

During an upgrade, the IDP Series device 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 software. You must use NSM to complete the IDP detector engine and attack object updates.

This section provides the following alternative workflows:

- [Upgrading with NSM on page 5](#)
- [Upgrading with the CLI on page 7](#)



**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 an upgrade. We understand this is not possible or desirable in all deployments, so connecting through the console is not required to upgrade.

---

### Upgrading with NSM

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

To update the IDP OS software:

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

To add an IDP OS 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 OS 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**.  
.....

## 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 OS 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 the user `admin` and enter `su -` to switch to the user 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 must initiate the FTP session from the IDP Series device.
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**.

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

The software upgrade is complete.

## Resolved Issues

[Table 2 on page 8](#) describes issues that are resolved when you upgrade from IDP OS Release 5.1r3 to IDP OS Release 5.1r4. If you are upgrading from an earlier version, read the release notes for the subsequent releases to learn about the issues that were resolved in them.

**Table 2: Resolved Issues**

PR	Description
938445	IDP engine's policy push and database update on NSM resulted in a crash.
896142	The <b>sctop</b> utility command displayed an error message on the terminal.
873736	Change or update of IDP Reporter default password failed.
883957	IDP is vulnerable to CVE-2013-2094.
829404	IDP Peer Port Modulator (PPM) was sending interface status logs to NSM continuously.
891408	Some attacks are not being triggered from signature <b>TROJAN: PUSHDO-ACTIVITY</b> IDP.
817736	When multiple VRs are enabled, generating report through Appliance Configuration Manager resulted as no for the item multiple VRs enabled.
807625	Link flaps for every 2 to 3 seconds after syslog is restarted.
801863	On IDP OS 5.1r3, there is no alert message when the disk array status changes to "degraded" or one disk fails.
790986	After upgrading IDP8200 to 5.1r3, observed high CPU utilization even at low traffic rates.



Table 2: Resolved Issues (*continued*)

PR	Description
952236	IDP sends the logs to NSM with protocol number, once the session rate limit is reached.
955692	IDP engine restarts unexpectedly.
956023	On IDP800 running with IDP OS 5.1R3, the system forwarding logs to NSM and syslog.
964832	On an IDP75 device a core file has been created with an associated error on log messages.
965573	NSM displaying incorrect values for IDP swap memory usage (Always 90%) for all IDP8200 devices on IDP OS 5.1R3.
741167	Occasionally, PPM disables all interfaces.
732827	SNMP polling is not running and dumped core file.
726058	IDP Nested Application Identification is not detecting Application Objects when going through a proxy.
588448	IDP OS Perl is not using the <b>taint</b> option.
710640	NTP vulnerabilities are not addressed in IDP device.
735495	Cyrus SASL library base 64 encoder buffer is overflowed.
735498	OpenSSL is open to multiple vulnerabilities; Unix/Linux CVE-2011-4108, CVE-2011-4109, CVE-2011-4576, CVE-2011-4577, CVE-2011-4619, and CVE-2012-0027 .
735505	OpenSSL is open to multiple vulnerabilities; Unix/Linux CVE-2011-3207, and CVE-2011-3210.
735506	Security scan on IDP OS 5.1r3 found OpenSSL Session Renegotiation vulnerability.
735508	Security scan on IDP OS 5.1r3 found Apache User Enumeration vulnerability.
754115	Tracking the resolutions for the PRs 735495, 735498, 735499, 735503, 735505, 735506, 735508, 773266, 787262, 823042, and 710640.
773266	IDP600 detects vulnerabilities related to NTP.
787262	Cyrus SASL library version below 2.1.23 causing security vulnerability.
823042	IDP OS 5.1r3 on IDP800 is vulnerable to CVE-2012-0814, CVE-2010-4478, CVE-2011-0539 and CVE-2012-0053.
957517	IDP OS 5.1r3 on IDP800 there is a multiple buffer overflows in the CMU Cyrus SASL library before 2.1.23.
957521	IDP OS 5.1r3 on IDP800 there is a Heap-based buffer overflow in the <b>Perl_repeatcpy</b> function.
957526	The <b>asn1_d2i_read_bio</b> function in OpenSSL before 0.9.8v does not properly interpret integer data.

Table 2: Resolved Issues (*continued*)

PR	Description
957532	Multiple integer errors in <code>crypto/buffer/buffer.c</code> on OpenSSL 0.9.8v allows remote attackers to conduct buffer overflow attacks.
963319	IDP OS 5.1r3 on IDP800 is vulnerable to CVE-2012-5526, CVE-2012-6329, CVE-2012-2686, CVE-2013-0166, CVE-2013-0169, CVE-2010-5107, CVE-2012-0884, CVE-2012-1165, CVE-2012-0021, CVE-2012-0031, CVE-2010-5107, CVE-2012-2333, CVE-2008-5077, CVE-2008-7270, and CVE-2009-0021.
697830	IDP products are affected by CVE-2011-3192, while the signature update page lists none of the products are being affected by the apache killer.
968317	IDP8200's SNMP monitoring is displaying 100% CPU utilization, but not utilized 100%.
1004703	Dropping retransmissions out of sequential synchronization impacts the connections for higher latency devices such as mobile VPNs.
1029371	IDP OS 5.1r3 is vulnerable to CVE-2014-6271, CVE-2014-7169, CVE-2014-6277, CVE-2014-6278, and CVE-2014-7186.

## Known Issues

Table 3 on page 10 describes issues that are present in IDP 5.1r4.

Table 3: Known Issues

PR	Description
Upgrade	
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.
497226	A manually set IDP Series device system clock setting is not preserved after upgrading to IDP OS 5.1 (release 5.1r1, 5.1r2, 5.1r3, or 5.1r4).  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.

Table 3: Known Issues (*continued*)

PR	Description
591151	<p>During an upgrade, userspace device management failure messages like those shown below are printed to the serial port console screen. You can ignore these messages.</p> <pre> GRUB Loading stage2... Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue.Red Hat nash version 5.1.19.6 starting       Welcome to Juniper Networks IDP OS       Press 'I' to enter interactive startup. Setting clock (utc): Wed Mar  9 02:51:43 PST 2011 [ OK ] Starting udev: udevd-event[2198]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.2/host1/ioerr_cnt' failed udev-event[2199]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.2/host2/ioerr_cnt' failed udev-event[2201]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.1/host4/ioerr_cnt' failed udev-event[2202]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.1/host5/ioerr_cnt' failed udev-event[2197]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.2/host0/ioerr_cnt' failed udev-event[2200]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.2/host3/ioerr_cnt' failed udev-event[2807]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.2/host0/target0:0:0/ioerr_cnt' failed [ OK ] Loading default keymap (us): [ OK ] </pre>
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 nonconfigurable.</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>
591152	<p>After you use ACM to apply a configuration change, ACM displays a page with status on the update. Within these logs, there is an erroneous message that you can ignore: "/bin/echo: write error: Invalid argument".</p>
591857	<p>After you use ACM to apply a configuration change that requires a reboot, ACM displays a page that confirms the configuration changes. The page is labeled "Configuration Saved &amp; Applied". In previous releases, this page was labeled "Confirm Configuration".</p>
Configuration	
303672	<p>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.</p>

Table 3: Known Issues (*continued*)

PR	Description															
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	<p>In the following scenario, NSM policy validation should report a rule shadowing condition because the second rule could never be applied.</p> <table border="1"> <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	<p>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> <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	<p>The NSM object editor does not enforce correct use of the within bytes constraint for custom signature attack objects.</p> <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 <b>Context</b>. If you configured one of the packet contexts, select <b>Packet</b>. If you configured one of the stream contexts, select <b>Stream</b>.</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 5.1 (release 5.1r1, 5.1r2, 5.1r3, or 5.1r4) does not support the within bytes constraint for custom compound attack objects.															
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.															

Table 3: Known Issues (*continued*)

PR	Description
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 (release 5.1r1 or 5.1r2), 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:16/00:00:00:00/40 tag 1 cdb 0x0 data 24576 out res 50/00:38:a5:70:16/00:00:00:00/40 Emask 0x2 (HSM violation)</pre> <p>You can safely ignore these messages.</p>
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 OS CLI to run <b>idp.sh restart</b> . However, the problem will recur following add device or import configuration procedures.
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 <b>Device_critical_log</b> and <b>Device_warning_log</b> instead of the strings <b>Critical</b> and <b>Warning</b> that appear for other network devices.
415164	In NSM, packet data cannot be displayed correct for certain malformed IP packets.
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.

**Table 3: Known Issues (continued)**

PR	Description
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 sent to NSM but not to syslog. The logs should be sent to both (if syslog has been set up).
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 3: 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"> <li>• jnxIdpSensorFreePktBuffersFiveSec.0</li> <li>• jnxIdpSensorFreePktBuffersOneMin.0</li> <li>• jnxIdpSensorPktsRxdPerIntfcTable</li> <li>• jnxIdpSensorPktsTxRatePerIntfcTable</li> <li>• jnxIdpSensorPktsDropOnAllIntfc.0</li> <li>• jnxIdpSensorSignatureStatsTable</li> <li>• jnxIdpSensorTopTenSignatureStatsTable</li> </ul> <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 <b>jnetStats</b> 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>
590812	<p>The following log messages appear periodically in lkmStart log entries:</p> <pre>[WARN]:STARTING /usr/idp/device/bin/lkmStart.sh recover [WARN]:STARTING /usr/idp/device/bin/lkmStart.sh recover</pre> <p>The following unexpected log messages appear in idpHMD log entries:</p> <pre>[Error] DVRdriveStatus failed [Error] DVRdriveStatus failed</pre> <p>Please ignore these log messages. They are not related to the true state of the system or system events.</p>

Table 3: Known Issues (*continued*)

PR	Description
719478	We have observed a problem with flow bypass logs and counters. The problem occurs only when debug logging is enabled, logs are being generated at a high rate, and the test traffic load fluctuates above and below the flow bypass threshold. In these conditions, the log rate is so rapid that the IDP OS drops logs for some events. It can be confusing if the IDP OS log record is missing a flow bypass triggered or flow bypass reset message. We acknowledge the problem.
CPU Utilization	
434539	In the NSM Device Monitor > View Device Details > Process Status tab, the CPU utilization for the IDP engine is reported as 0%. You cannot use NSM to monitor device CPU utilization. We recommend you use SNMP to monitor CPU utilization and CLI utilities when investigating high or low CPU utilization. For single core platforms, the CPU utilization reported to SNMP is based on the results of the <b>top</b> command. For multicore platforms, the CPU utilization reported to SNMP is based on the results of the <b>scio idp-cpu-utilization</b> command.
603547	Counterintuitive behavior—In an HA deployment, the IDP Series device in the inactive path shows occasional spikes in CPU utilization even though it is not processing packets. This is expected. The CPU usage is related to state synch operations between the active device and the passive device.
Stability	
430363	IDP8200 stops processing traffic at high load with SYN protection enabled.
499447	For single core platform IDP75, 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.
593999	PKID crash related to SSL inspection (forward proxy) in a stress-test environment.
594004	In a stress-test environment, we observed a condition where SSL forward-proxy processing results in a crash with coredump.
601870	In an IDP8200 stress test, we observed an IDP engine hang related to TSIG processing and subsequent spike in CPU utilization.
604848	In an IDP8200 stress test, we observed a crash with core at <code>sc_icode_instance</code> .



Table 3: Known Issues (*continued*)

PR	Description
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"> <li>1. In the NSM Device Manager, double-click the name of the device to display the configuration editor.</li> <li>2. Click <b>Sensor Settings</b>.</li> <li>3. Click the <b>Run-time parameters</b> tab.</li> <li>4. Under Traffic Signatures, increase the value for <b>Byte threshold for suspicious flows</b>.</li> </ol>
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.
Shutdown Operation	
432893	The <b>shutdown -h now</b> 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.
Unsupported Functionality	
572045	When you encounter a hung system, you might want to force a core dump. To do this, you type a <a href="#">SysRq key combination</a> . You can use the SysRq key combination on IDP8200, IDP800, IDP250, and IDP75.
Expected Behavior	
547354	Packet drops are possible in simulation mode if the JNET free packet buffer is 0.
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 Gb 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 3: Known Issues (*continued*)

PR	Description
720406	<p>In a test lab environment, we have observed conditions in which the JNET driver free packet buffer count does not recover from zero availability. Depletion of the free pack buffer results in failover to the secondary device. After failover, the secondary device free packet buffer is depleted, resulting in bypass. The behavior is not consistently reproducible.</p> <p>If you observe this behavior, you can take either one of the following actions to restore the IDP Series devices to health:</p> <ul style="list-style-type: none"> <li>On the primary and the secondary device, reset the HA interface using the following commands: <pre>[root@defaulthost ~]# ifconfig down [root@defaulthost ~]# ifconfig up</pre> </li> <li>On the primary and the secondary device, turn off the interface pause parameters for the HA interface using the following commands: <pre>[root@defaulthost ~]# ethtool -A eth1 autoneg off [root@defaulthost ~]# ethtool -A eth1rx off [root@defaulthost ~]# ethtool -A eth1tx off [root@defaulthost ~]# ethtool -a eth1 Pause parameters for eth1: Autonegotiate:  off RX:             off TX:             off</pre> </li> </ul>
Documentation	
424045	<p>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 <a href="#">IDP Logs and Reports in NSM Task Summary</a> section in the <i>IDP Series Administration Guide</i>.</p>

## Errata

This section lists outstanding issues with the documentation.

### IDP Series Custom Attack Objects Reference and Examples Guide

- In the IDP 5.1 release, the *IDP Series Custom Attack Objects Reference and Examples Guide*, "Reference Tables" chapter, "Reference: Nonprintable and Printable ASCII Characters" section, the character DEL is incorrectly documented in "ASCII Reference: Printable Characters" table. The DEL character is a nonprintable ASCII character.
- In the IDP 5.1 release, the *IDP Series Custom Attack Objects Reference and Examples Guide*, "Reference Tables" chapter, "Reference: Nonprintable and Printable ASCII Characters" section, "ASCII Reference: Nonprintable Characters" table, the decimal value is incorrectly documented as:

```
'84
```

The correct information is as follows:

```
84
```

## Documentation

You can download user documentation from the Juniper Networks Web site: <http://www.juniper.net/techpubs/>. The user documentation on the IDP OS 5.1 site applies to IDP OS 5.1r4. [Table 4 on page 19](#) lists the user documentation related to the IDP Series appliance.

**Table 4: Related IDP Series Documentation**

Document	Description
<a href="#">Juniper Networks Security Intelligence Center Attack Signatures</a>	Lists predefined attack signatures developed by the Juniper Networks Security Intelligence Center.
<a href="#">Juniper Networks Security Intelligence Center Application Signatures</a>	Lists predefined application signatures developed by the Juniper Networks Security Intelligence Center.
<a href="#">IDP Detector Engine release notes</a>	Provides information about IDP Detector Engine releases, including new features, changed features, fixed problems, and known issues.
<a href="#">IDP Series installation guides</a>	Describes IDP Series hardware and provides instructions for installing, configuring, updating, and servicing the device.
<a href="#">IDP Series Feature Documentation</a>	Includes a collection of topics from the <i>IDP Series Administration Guide</i> and <i>IDP Series Concepts and Examples Guide</i> , in HTML.
<a href="#">IDP Series Administration Guide</a>	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).
<a href="#">IDP Series Concepts and Examples Guide</a>	Explains IDP Series features and provides examples of how to use the system.
<a href="#">IDP Series Custom Attack Objects Reference and Examples Guide</a>	Provides examples and reference information for creating custom attack objects.
<a href="#">IDP Reporter User's Guide</a>	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 5 on page 19](#) lists related NSM documentation.

**Table 5: Related NSM Documentation**

Document	Description
<a href="#">Network and Security Manager release notes</a>	Provides information about new features, changed features, fixed problems, and known issues with the NSM release.

Table 5: Related NSM Documentation (*continued*)

Document	Description
<a href="#">Network and Security Manager Installation Guide</a>	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.
<a href="#">Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide</a>	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.
<a href="#">Network and Security Manager Administration Guide</a>	<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.

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Revision History

20 July 2017—Revision 3, IDP OS - Release 5.1r4.

28 December 2015—Revision 2, IDP OS - Release 5.1r4.

12 February 2015—Revision 1, IDP OS - Release 5.1r4.

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks 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.