

Intrusion Detection and Prevention Release Notes

January 27, 2009 (updated February 13, 2009)
Part Number: 530-023833-02
Revision 4.2r2

Contents

- Overview2
- New Features and Enhancements2
- Unsupported Features2
- Supported Upgrade Paths3
- Compatibility with Network and Security Manager3
- Browser Requirements5
- Upgrading IDP Software6
- Verifying Your License7
- Downloading and Installing a License Key8
- Resolved Issues9
- Known Issues11
- Documentation13
- Getting Help14

Overview

Juniper Networks Intrusion Detection and Prevention (IDP) devices detect intrusions and prevent attacks on 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. This software release supports IDP 8200.

New Features and Enhancements

This release resolves issues reported in 4.2r1. For details, see “Resolved Issues” on page 9.

IDP 4.2r2 does not require the network driver patch previously required to support the following I/O modules:

- IDP-1GE-4SX-BYP 4-port 1 GigE SX fiber interface card with bypass
- IDP-10GE-2SR-BYP 2-port 10 GigE SR interface card with bypass
- IDP-10GE-2XFP 2-port 10 GigE XFP interface card (non-bypass)

You do not have to install a network driver patch after you upgrade.

If you are a new customer, the IDP 8200 included in your shipment has IDP 4.2r1 preinstalled. We recommend that you upgrade to IDP 4.2r2 before using your I/O modules, so that you will not have to install the IDP 4.2r1 network driver patch.

Unsupported Features

The following features are not supported in IDP 4.2r2:

- 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
- Bridge, proxy-ARP and router deployment modes
- High availability
- External bypass

Supported Upgrade Paths

You can upgrade from IDP 4.2r1 (whether or not your 4.2r1 installation includes the JNET driver patch or any customer support patches).

Compatibility with Network and Security Manager

Your version of Network and Security Manager (NSM) might require a schema update to support your IDP platform and software version. The schema update is also known as forward support. Check your NSM release notes for the latest version support for IDP devices.

At the time of the IDP 4.2r2 release, we verified compatibility with the following releases of NSM:

- NSM 2008.1 (requires a schema update)
- NSM 2007.3r2 or later (requires a schema update)

To download and install a schema update:

1. Download the schema update software:
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer user name and password.
 - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote) > Network and Security Manager > 2008.1** (or **2007.3**, depending on your NSM release).
 - c. On this page, locate your NSM release number and download a corresponding pair of schema update files.

NSM Release	Download
2008.1r1	<ul style="list-style-type: none"> ■ server: nsm2008.1r1_schema_update_server.zip ■ client: nsm2008.1r1_schema_update_ui_win.zip or nsm2008.1r1_schema_update_ui_linux.zip
2007.3r4	<ul style="list-style-type: none"> ■ server: nsm2007.3r4_schema_update_server.zip ■ client: nsm2007.3r4_schema_update_ui_win.zip or nsm2007.3r4_schema_update_ui_linux.zip
2007.3r3	<ul style="list-style-type: none"> ■ server: nsm2007.3r3_schema_update_server.zip ■ client: nsm2007.3r3_schema_update_ui_win.zip or nsm2007.3r3_schema_update_ui_linux.zip
2007.3r2	<ul style="list-style-type: none"> ■ server: nsm2007.3r2_schema_update_server.zip ■ client: nsm2007.3r2_schema_update_ui_win.zip or nsm2007.3r2_schema_update_ui_linux.zip

2. Install the server schema update on the NSM server:
 - a. Log in to the NSM server host computer as root.
 - b. Copy the NSM server schema update file to a temporary location. We recommend `/tmp`.
 - c. Unzip the schema update. For example, type the following command:

```
unzip nsmreleasenumbe_schema_update_server.zip
```

Where *releasenumbe* is a specific NSM release number, such as 2007.3r2, 2007.3r3, 2007.3r4, or 2008.1r1.

- d. Run the schema update. For example, type the following command:

```
sh nsmreleasenumbe_schema_update_server.sh
```

Where *releasenumbe* is a specific NSM release number, such as 2007.3r2, 2007.3r3, 2007.3r4, or 2008.1r1.

The update begins automatically. During the update process, the installer

stops and restarts the management system.

3. Install the client schema update on the NSM client computer:
 - a. Log in as an user with administrator privileges on the computer where you are installing the UI.
 - b. Copy the client schema update file to the same location where you have installed the UI.
 - c. Unzip the schema update.
 - d. Run the schema update:
 - If you are upgrading the UI on a Windows-based PC, double-click the installer executable.
 - If you are upgrading the UI on a Linux-based computer, launch it from a command line using the following command:

```
sh nsmreleasename_schema_update_ui_linux.bin
```

Where *releasename* is a specific NSM release number, such as 2007.3r2, 2007.3r3, 2007.3r4, or 2008.1r1.

To verify that you have installed the schema update properly, view the NSM UI client login window and verify that the installed version number has changed to reflect the update. You can also use the Help menu option to view the installed version number.

Browser Requirements

The Appliance Configuration Manager (ACM) and QuickStart utility have been tested on the following browsers:

- Internet Explorer 6.0 SP2
- Firefox 1.5 or 2.0
- Netscape 7.2 or 8.1.2

IDP Reporter has been tested on the following browsers:

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



NOTE: IDP Reporter does not support Mozilla Firefox 3.x.

Upgrading IDP Software

When you upgrade IDP software, you perform the following basic steps:

1. Upgrade IDP software (CLI).
2. Update IDP Detector Engine (NSM).
3. Update the NSM attack object database (NSM).
4. Update the security policy installed on the IDP device (NSM).



NOTE: You cannot use NSM to upgrade the device software from IDP 4.2r1 to 4.2r2.

To upgrade:

1. Download the software image to a host that runs an FTP server.
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer user name and password.
 - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote)**. In the row for IDP, click **4.2**.
 - 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:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as the user admin and switch to the user root (su -u root).
 - If you prefer, make a connection through the serial port and log in as the user 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 to the IDP device. IDP does not run an FTP server, so you have to initiate the FTP session from the IDP device.
4. Unplug the HA port cable, if one is attached.
5. Run the upgrade script by typing **sh sensor_version.sh**, where *version* is the number that identifies the software release version. Press **Enter**. When the script has finished, type **reboot** and press **Enter**.
6. Reconnect the HA cable after upgrading all of the members in the cluster (if applicable).
7. In the NSM Device Manager, right-click the device, select **Adjust OS Version**, and complete the wizard steps.

8. Download IDP detector engine and NSM attack database updates to the NSM GUI server:

In NSM, select **Tools > View/Update NSM attack database** and complete the wizard steps.



NOTE: You can download release notes for IDP detector engine from the following location: <http://www.juniper.net/techpubs/software/management/idp/de/index.html>.

9. Push the updated IDP detector engine to IDP devices:

In NSM, select **Devices > IDP Detector Engine > Load IDP Detector Engine** and complete the wizard steps.



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

10. 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**.

Verifying Your License

After you upgrade, check the IDP appliance to ensure that your license key is a permanent license key.

To verify your license:

1. Connect to the IDP command-line interface:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as the user admin and switch to the user root (su -u root).
 - If you prefer, make a connection through the serial port and log in as the user root.



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

2. Run the following scio command:

```
[host]# scio lic list
```

The command returns license information similar to the following example:

```
ID Machine ID Issue Date Expiration OK Feature
-----
1 xxxxxxxxxxxx Mon Jan 12 00:00:00 2009 Never Y idp_key
```

For a permanent license key, the expiration is Never. If you do not have a permanent license installed, log in to License Management System (LMS) to download and install the license.

Downloading and Installing a License Key

The IDP license is installed at the factory. If you reimage the device, you need to re-license it.

To download and install a license key:

1. Download your license:
 - a. Go to <https://www.juniper.net/lcrs/license.do> and log in with your customer user name and password.
 - b. Click **Find license keys** to retrieve your license.

You must provide the device serial number. You can locate the serial number in the following ways:

- In ACM, the serial number is displayed in the lower-left hand corner of the home page.
 - From the CLI, run the **scio getsystem** command to display system information, including the serial number.
- c. Save the license as a text file named lic.txt.
2. Add your license to the IDP device license store:
 - a. Connect to the IDP command-line interface:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and switch **root (su -u 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.

- b. Use SCP or FTP to copy the license file to a temporary location on the IDP device. IDP does not run an FTP server, so you have to initiate the FTP session from the IDP device.
- c. Change directory to the temporary directory:


```
[host]# cd /tmp
```
- d. Change permissions on the file to enable read, write, and execute:


```
[host]# chmod 777 lic.txt
```
- e. Run the following scio command to add the license key:


```
[host]# scio lic add lic.txt
```
- f. Run the following scio command to verify you have successfully added the license key:


```
[host]# scio lic list
```

Resolved Issues

The following issues have been resolved in this release:

- 278695–Resolved an issue where the speed/duplex settings were not persistent through reboots.
- 288030–After a policy push, “Unknown application...” messages had appeared in the NSM job window (depending on the policy). This problem is resolved by upgrading to IDP 4.2r2 and updating to the latest IDP detector engine.
- 288662–Resolved an issue where a reboot in sniffer mode could bring interfaces down and stop attack detection.
- 290280–Resolved an issue where, under high stress, SSH or console access to IDP via the management interface might freeze when checking flow table entries via sctop or scio.
- 298356–Resolved an issue related to shared memory.
- 299054–Improvements have been made to the **tech-support** utility. The **tech-support** utility captures information about your deployment so that you can work with JTAC to troubleshoot the issue.
- 299514, 29953–Corrections and improvements for online Help for the Appliance Configuration Manager (ACM).
- 300370–Resolved an issue with the way flows were destructed.
- 301216–Internal refinements have been made the SYN Protector rulebase to handle a use case where security policies are continuously updated.
- 303939, 395325–IDP Reporter software has been updated. Juniper Networks application usage manager requires the IDP Reporter release included in IDP 4.2r2.
- 307900–Resolved an issue with the way IDP Reporter obtained data from the IDP log reader process.
- 388717–Resolved an issue with the way sciod was renaming an IDP detector engine file. This had caused a problem with automated updates using guiSvrCli.sh.
- 403263–Resolved an issue where IDP engine logs did not have timestamps.
- 406411–Resolved an issue with the way the AI feature handled RSH traffic.
- 407630–Resolved an issue where IDP reboot had erroneously generated a segfault log in /var/log/messages.
- 408002–Improvements to the driver to support 10 Gigabit Ethernet interfaces.
- 409549–Resolved an issue with policy compilation that had resulted in an error compiling a policy with the VOIP:SKYPE:LOGIN-1 attack object.
- 413000–Resolved an issue where the security policy had not been reloaded after an update to the IDP detector engine.

Known Issues

The following issues are present in this release:

- 278471–**scio ccap all** is not supported (as the profiler feature is currently not supported).
- 279408–UDP port scanning works if there is no response from the Victim PC. But 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**.
- 286020–In ACM, the default interface setting for 10 Gigabit Ethernet interface with bypass should be **NIC OFF**.
 - 286327–On the ACM Configure Forwarding Interfaces page, when no installed I/O module supports bypass, the user interface displays the headers for the NIC State drop-down list. When no installed I/O module supports bypass, NIC state is non-configurable. The user interface should not display the NIC State headers.
 - 287003–On the ACM Configure Forwarding Interfaces page, the NIC State drop-down list boxes should not include **External Bypass**. External bypass is not supported.
 - 287179–After system unavailability, IDP does not send a log that IDP has returned to normal operations.
 - 288644–NIC OFF logs are erroneously sent for non-sniffing interfaces (when IDP is in sniffer mode).
 - 288651–NIC OFF log messages are displayed for interfaces that are not selected as forwarding interfaces.
 - 288663–Link status (up/down) messages do not appear when the device comes up.
 - 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)
```

Work around: You can safely ignore these messages.

- 288997—IDP 8200 10 Gigabit Ethernet interfaces do not support peer port modulation (PPM).
- 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.

Work around: When using ACM, be careful to use complete double-quote constructions for alias names. For example, “hello”.

- 299413—After installing I/O modules, if the number of interfaces is fewer than six, you might encounter ACM or console messages indicating “cannot find eth6 and eth7.”

You can safely ignore these messages.

To resolve them so the event is no longer reported:

1. In NSM, edit the policy and verify that only the existing interfaces are set.
2. Push a policy update to the sensor.

The policy update synchronizes the configuration with the new hardware.

- 312966—There is an issue the PPM feature and copper traffic interfaces. PPM can take down links as expected. When PPM brings links back up, links can flap (almost 10 times) before stabilizing. This issue has been observed only when IDP is connected to an HP ProCurve switch and not with back-to-back setup.
- 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.
- 412490—For 1 Gigabit Ethernet copper traffic interfaces and 10 Gigabit Ethernet fiber (with bypass) traffic interfaces, IDP correctly logs the event that the virtual router has entered bypass, but it does not log the event where IDP has returned to normal operations.
- 412491—For 1 Gigabit Ethernet fiber (with bypass) traffic interfaces, IDP correctly logs the event that the virtual router has entered NICs off state, but it does not log the event where IDP has returned to normal operations.
- 412494—For 1 Gigabit Ethernet fiber (with bypass) traffic interfaces, IDP incorrectly logs the event where IDP returns to normal operations after a period in bypass state. In the log, in the column for interface, IDP reports only one interface of the virtual router pair. For example, it insufficiently reports the interface as **interface = ,eth5** instead of **interface = eth4,eth5**.
- 421001—The following security policy actions do not behave as expected:
 - Close Client—The reset packet is not sent to the client.
 - Close—The reset packet is sent to the server, but it is not sent to the client.
 - IP Action: Close—The reset packet is not sent to the client.

To resolve this issue, contact the Juniper Networks Technical Assistance Center (JTAC) to obtain a software patch.

Documentation

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

Table 1 on page 13 lists related IDP documentation.

Table 1: 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 8200 Installation Guide</i>	Describes the IDP 8200 platform. It provides instructions for installing, configuring, updating, and servicing the device.
<i>Intrusion Detection and Prevention Concepts & Examples Guide</i>	Explains IDP features and provides examples of how to use the system.
<i>Intrusion Detection and Prevention 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 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 1 on page 13 lists related NSM documentation.

Table 2: 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.

Table 2: 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>
<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.
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.