

IDP Detector Engine Release Notes

Part Number: 530-029025-01
Revision April 15, 2009 — Revision 02

Contents

Recent Release History	2
IDP Detector Engine Overview	3
Understanding IDP Detector Engine Version Numbers	3
Displaying the IDP Detector Engine Version Number (NSM Procedure)	4
Displaying the IDP Detector Engine Version Number (CLI Procedure)	4
Updating the IDP Detector Engine	6
Troubleshooting an IDP Detector Engine Update	6
Reverting the IDP Detector Engine Version	6
New Features and Resolved Issues	7
Known Issues	9
Contacting Juniper Networks Technical Assistance Center (JTAC)	10

Recent Release History

The following table summarizes the features and resolved issues in recent releases. You can use this table to help you decide to update the IDP detector engine version in your deployment.

Table 1: IDP Detector Engine Features and Resolved Issues by Release

Release Date	Detector Engine Version	Features and Resolved Issues
April 15, 2009	<ul style="list-style-type: none"> ■ 10.2.140090407 ■ 4.2.110090322 ■ 4.1.110090407 ■ 4.0.110090407 ■ 3.5.126103 ■ 3.4.125129 	Quarterly update, including new features, stability improvements, and improved accuracy. For details, see “New Features and Resolved Issues” on page 7.
January 27, 2009	<ul style="list-style-type: none"> ■ 4.2.110090121 	<p>Major update corresponding with the release of IDP 4.2r2. Updates include:</p> <ul style="list-style-type: none"> ■ A new decoder for the MODBUS serial communications protocol. Improved accuracy with new contexts and other changes to reduce false positives. ■ Increased security coverage with new anomalies. ■ Resolution of issues with DNS, H.225 SGN, HTML, LDAP, MS-SQL, SIP, and SMB decoders.
January 15, 2009	<ul style="list-style-type: none"> ■ 4.1.110090107 ■ 4.0.110090107 ■ 3.4.121591 ■ 3.1.121592 	<p>Major update, including:</p> <ul style="list-style-type: none"> ■ A new decoder for the MODBUS serial communications protocol. ■ Resolution of issues with DNS, H.225 SGN, LDAP, MS-SQL, SIP, SMB, and TNS decoders. ■ Increased security coverage with new anomalies. ■ Improved accuracy with new contexts and other changes to reduce false positives.
January 5, 2009	<ul style="list-style-type: none"> ■ 3.4.118904 ■ 3.1.118905 	<p>Provides the following new features and fixes:</p> <ul style="list-style-type: none"> ■ 397759, 397759-2. Resolved an issue in the DNS decoder that could result in a security module crash. ■ 400464, 400467. Improved the SMB decoder with new features and anomalies. ■ 400468, 400469. Resolved an issue in the SMB decoder. It now generates UUID context.
December 31, 2008	<ul style="list-style-type: none"> ■ 4.1.110081106 ■ 4.0.110081106 	Improves coverage and accuracy for the SIP, SMB, DNS, MS-SQL, and HTTP protocols.

Table 1: IDP Detector Engine Features and Resolved Issues by Release *(continued)*

Release Date	Detector Engine Version	Features and Resolved Issues
October 23, 2008	<ul style="list-style-type: none"> ■ 4.1.110081008 ■ 4.0.110081008 ■ 3.4.117413 ■ 3.1.117412 	Improves coverage and accuracy for LDAP, SSL, and HTTP protocols.
September 18, 2008	<ul style="list-style-type: none"> ■ 4.1.110080916 	Improves coverage and accuracy for SSI and SIP protocols.
August 21, 2008	<ul style="list-style-type: none"> ■ 3.4.114929 ■ 3.1.115140 	Improves coverage and accuracy for the VOIP/SIP protocol.
July 22, 2008	<ul style="list-style-type: none"> ■ 4.1.110080701 ■ 4.0.110080701 	Improves coverage and accuracy for SMTP, SIP, and H.225 protocols.
July 17, 2008	<ul style="list-style-type: none"> ■ 4.1.110080700 ■ 4.0.110080700 	Improves coverage and accuracy for HTTP, LDAP, and SMB protocols.
June 19, 2008	<ul style="list-style-type: none"> ■ 4.1.110080600 ■ 4.0.110080600 	Improves coverage and accuracy for SIP, HTTP, and MSSQL protocols.
June 10, 2008	<ul style="list-style-type: none"> ■ 3.4.112183 	Improves coverage and accuracy for SIP and HTTP protocols.

IDP Detector Engine Overview

The IDP detector engine is a dynamic protocol decoder that includes support for decoding more than 60 protocols and more than 500 service contexts. The IDP detector engine is used by the IDP process engine in packet analysis.

The detector engine code base is packaged and released separately from the IDP or ScreenOS operating system and software code base. Juniper Networks Security Center (J-Security Center) releases IDP detector engine updates more frequently in order to ensure IDP products protect your network against recently discovered vulnerabilities.



NOTE: We recommend you subscribe to the IDP Signature Updates technical bulletin to be notified when J-Security Center releases IDP detector engine updates. Go to <https://www.juniper.net/alerts/>.

Understanding IDP Detector Engine Version Numbers

The IDP detector engine versions that are compatible with your system vary by product line and operating system version. The following table summarizes IDP detector engine version compatibility.

Table 2: IDP Detector Engine Version Compatibility

Hardware	Operating System	IDP Detector Engine Version
SRX	JUNOS 9.x	10.2.xxxxxxxxxx
IDP 8200	IDP 4.2.x	4.2.xxxxxxxxxx
IDP 75/250/800, IDP 50/200/600/1100, IDP 10/100/500/1000	IDP 4.1.x	4.1.xxxxxxxxxx
IDP 50/200/600/1100, IDP 10/100/500/1000	IDP 4.0.x	4.0.xxxxxxxxxx
ISG 1000/2000	ScreenOS 6.2.x	3.5.xxxxxxx
ISG 1000/2000	ScreenOS 6.1.x, 6.0.x	3.4.xxxxxxx
ISG 1000/2000	ScreenOS 5.4.x, 5.0.x	3.1.xxxxxxx

Displaying the IDP Detector Engine Version Number (NSM Procedure)

To view the version of the latest IDP detector engine that has been downloaded to the NSM GUI server:

- In NSM, select **Tools > View/Update NSM Attack Database** and click **Next**.

The wizard displays the IDP detector engine versions that have been downloaded to the NSM GUI server.

To view version information for the IDP detector engine installed on an IDP device:

- In the NSM device manager, double-click the IDP or ISG device to display the device configuration editor.

For standalone IDP devices, the Info node displays version information, including the IDP detector engine version.

For ISG devices, navigate to **Security > SM Settings** to display the IDP detector engine version.

Displaying the IDP Detector Engine Version Number (CLI Procedure)

To display the IDP detector engine version number on an IDP Series device:

1. Connect to the CLI as the user `admin` and switch to the user `root`.
2. Run the `scio getsystem` command as shown in the following example:

```
login as: admin
```

```

admin's password:
Last login: Thu Apr  9 17:31:47 2009 from 10.150.99.42

[admin@idp ~]$ su -

Password:

[root@idp ~]# scio getsystem

Product Name:  NS-IDP-8200
Serial Number: 0254092008000019
Software Version: 5.0.127636
IDP Mode: transparent
HA Mode: Disabled
Detector Version: 5.0.110090408
Software License: Evaluation
Software Expiration Date: 4/25/2009
[root@idp ~]#

```

To display the IDP detector engine version number on an ISG Series device:

1. Connect to the CLI as the user **admin** and enter **su - to** switch to the user root.
2. Run the **get system** command as shown in the following example:

```

[root@default host admin]# get system

[.]
IDP files version:

detector.so 3.1.101390

[root@default host admin]# [root@default host admin]#

```

The line for detector.so shows the version of the detector—in this example, version 3.1.101390.

To display the IDP detector engine version number on an SRX device:

1. Log into the JUNOS CLI and enter operational mode. For details, see the JUNOS documentation.
2. Enter the command shown in the following example:

```

user@host> show security idp security-package-version

Attack database version:31(Wed Apr 16 15:53:46 2008)
Detector version :9.1.140080400
Policy template version :N/A

```

In this example, the detector version number is 9.1.140080400.

Updating the IDP Detector Engine

Updating the IDP detector engine is a three part process.

To update IDP detector engine:

1. 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.

2. 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.

3. Run a security policy update job to initialize the IDP detector engine update:
 - 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**.

Troubleshooting an IDP Detector Engine Update

The default URL from which to obtain updates is <https://services.netscreen.com/restricted/sigupdates/nsm-updates/NSM-SecurityUpdateInfo.dat>. If you encounter connection errors, ensure this setting has not been inadvertently changed.

To restore the default URL:

1. Select **Tools > Preferences**.
2. Click **Attack Object**.
3. Click **Restore Defaults**.

NSM restores the URL in the **Download URL for ScreenOS Devices** text box.

4. Click **OK**.

Reverting the IDP Detector Engine Version

In most cases, your use of IDP will not benefit from reverting the IDP detector engine version. In some cases, however, you might be required to revert. If you encounter

an issue and need to revert, contact Juniper Networks Technical Assistance Center (JTAC).

New Features and Resolved Issues

The following table lists new features and resolved issues. It also indicates whether the issue was included in the 4-15-09 detector engine update or an earlier update; or if the issue is not applicable or not yet fixed. For more details on the conditions where you might encounter an unresolved issue, please contact JTAC.

Table 3: New Features and Resolved Issues

PR	Description	10.2.x	4.2.x	4.1.x/4.0.x	3.5.x	3.4.x
New Features						
295716, 436438	Added a feature to count established RTP/SIP sessions. See "To use the RTP/SIP session counter:" on page 9.	n/a	4-15-09	4-30-08	n/a	not fixed
309099	Added anomalies: URL-THRESHOLD-256, URL-THRESHOLD-512, URL-THRESHOLD-1024, URL-THRESHOLD-2048, URL-THRESHOLD-4096, URL-THRESHOLD-8192.	4-15-09	4-15-09	4-15-09	4-15-09	4-15-09
414182	Added a new decoder for encrypted traffic. The decoder is reported in counters as UNSPECIFIED and has application identification signature 8123.	n/a	not fixed	4-15-09	n/a	not fixed
424848	Added support for SIP/IPv6.	n/a	n/a	n/a	4-15-09	n/a
428205	Added support for IPv6/ICMPv6 anomalies.	n/a	n/a	n/a	4-15-09	n/a
Changed Features						
301844	Removed the default association of port TCP/88 to HTTP. The service is now detected by the application identification feature..	n/a	4-15-09	7-17-08	4-15-09	n/a
429029	Changed the name of a service type from ICMP6 to ICMPv6.	n/a	n/a	n/a	4-15-09	n/a
Stability Improvements						
276555	Resolved an issue with the DNS decoder reported in 4.1.110071200 that had resulted in a crash.	4-15-09	n/a	12-31-08	n/a	n/a
291850	Resolved in issue found in the SIP decoder during IDP 4.2 development and testing.	n/a	4-15-09	4-15-09	n/a	n/a

Table 3: New Features and Resolved Issues (continued)

PR	Description	10.2.x	4.2.x	4.1.x/4.0.x	3.5.x	3.4.x
389022, 419983	Fixed a memory leak issue with the LDAP decoder.	4-15-09	1-27-09	10-23-08	n/a	1-15-09
403225, 397759	Fixed a crash in the DNS decoder due to buffer overrun in RR - Resource Record.	4-15-09	1-27-09	12-31-08	n/a	1-05-09
415094	Resolved a buffer overrun condition reported in 3.4.114520 that had resulted in a crash.	n/a	n/a	n/a	4-15-09	4-15-09
420365	Resolved an issue reported in detector 4.0.96141 that had caused a kernel panic in <code>sc_tcp_stream_do_peek()</code> .	n/a	n/a	n/a	4-15-09	4-15-09
424316	Resolved an issue reported in 3.1.121592 that had caused policy compiler failure if the security policy contained MODBUS-related signature attack objects.	n/a	n/a	n/a	n/a	n/a
Improved Accuracy						
297066	Fixed a false positive with anomaly LDAP_FORMAT_ENC_INCORRECT_TAG. We had treated an optional tag as mandatory.	n/a	n/a	7-17-08	n/a	1-15-09
302403	Fixed a false positive with the SMTP Duplicate Header anomaly. <code>Resent-<header-suffix></code> : had been incorrectly treated as <code><header-suffix></code> .	n/a	4-15-09	7-22-08	4-15-09	n/a
312327	Corrected an error with parsing the + character in the HTTP decoder.	n/a	4-15-09	12-31-08	n/a	1-15-09
418711	Fixed a false positive with anomaly FTP:REQERR:REQ-TOO-MANY-ARGS that could occur when filenames with certain syntax were the arguments of commands.	4-15-09	4-15-09	4-15-09	4-15-09	4-15-09
420878	Fixed a false positive with anomaly SMTP:AUDIT:DUPLICATE:HEADER. We had incorrectly mapped <code>To:</code> , <code>Delivered-to:</code> , <code>CC:</code> , and <code>Bcc:</code> to the same values.	4-15-09	4-15-09	4-15-09	4-15-09	4-15-09
421542	Fixed false positives with anomalies LDAP:FORMAT:DN_FMTERR and LDAP:FORMAT:ENC_INCORRECT_TAG.	n/a	4-15-09	n/a	n/a	n/a
423369	Fixed a false positive for the SMB:ERROR:GRIND anomaly.	4-15-09	4-15-09	4-15-09	n/a	not fixed

To use the RTP/SIP session counter:

1. Enable RTP/SIP detection:

```
[root@defaulthost ~]# scio const -p sip set sc_sip_rtp_detect 1
```

```
scio: setting sc_sip_rtp_detect to 0x1
scio: setting sc_sip_rtp_detect to 0x1
scio: setting sc_sip_rtp_detect to 0x1
scio: setting sc_sip_rtp_detect to 0x1
scio: setting sc_sip_rtp_detect to 0x1
scio: setting sc_sip_rtp_detect to 0x1
[scio@defaulthost ~]#
```

2. View the counter sc_flow_gate_add:

```
[root@defaulthost ~]# scio counter get flow | grep sc_flow_gate_add
```

```
sc_flow_gate_add          3384
sc_flow_gate_add          850
sc_flow_gate_add           0
sc_flow_gate_add         1770
sc_flow_gate_add           0
sc_flow_gate_add         2538
[scio@defaulthost ~]#
```

Known Issues

The following table identifies known issues in this release.

Table 4: Known Issues

Detector Engine Version	Issue
<ul style="list-style-type: none"> ■ 4.2.xxxxx 	<p>IDP engine crashes if all of the following circumstances apply:</p> <ul style="list-style-type: none"> ■ You have updated IDP detector engine to 4.2.110090121 (27-Jan-09). ■ Subsequently, you update IDP detector engine to 4.2.110090322 (15-Apr-09). <p>To work around this issue, restart IDP engine before performing the update to 4.2.110090322 (15-Apr-09):</p> <ol style="list-style-type: none"> 1. Connect to the CLI as the user admin and enter su - to switch to the user root. 2. Enter the following command: <pre>[root@idp ~]# idp.sh restart</pre> <p>You can also contact JTAC for a patch to avoid this issue.</p>

Table 4: Known Issues (continued)

Detector Engine Version	Issue
<ul style="list-style-type: none"> ■ 4.1.xxxxx ■ 4.0.xxxxx 	<p>For standalone IDP devices, after you update to this release, NSM fails to update its inventory information for the IDP detector engine, creating a version mismatch between NSM and the IDP device. In NSM, the previous release information continues to be displayed. In addition, if you push a policy update to the IDP device, you receive the following error:</p> <p>Error Code: Error Text: The Detector version on the device did not match NSM records. NSM has been updated to match the detector version on the device. Please try again to update the device. Error Details: No Details Available.</p> <p>To work around this issue (NSM 2008.2r1, NSM 2008.1.x):</p> <ol style="list-style-type: none"> 1. Push a policy update to the IDP device. <p style="padding-left: 40px;">This policy update fails due to the version mismatch. However, NSM then resolves the mismatch by synchronizing its inventory information to that installed on the IDP device. Verify that after the initial failure and resolution, NSM displays the updated build number.</p> <ol style="list-style-type: none"> 2. Push another policy update to the IDP device. <p style="padding-left: 40px;">This policy update is successful.</p> <p>To work around this issue (NSM 2007.3r4):</p> <ol style="list-style-type: none"> 1. Re-add the IDP device to NSM device manager. 2. Push a policy update to the IDP device to initialize the update. <p>Check the release notes for NSM 2008.2r2 to see if this has been resolved in that release.</p> <p>For complete procedures on adding devices to NSM device manager and pushing configuration updates from NSM to devices, see the <i>IDP Administration Guide</i>.</p>
<ul style="list-style-type: none"> ■ 4.2.xxxxx ■ 4.1.xxxxx 	<p>31051, 313472. In SSL decrypted traffic, some attacks are not detected. The root cause of this problem appears to be an insufficient SSL buffer size.</p>

Contacting Juniper Networks Technical Assistance Center (JTAC)

If you need additional information or assistance, contact 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.