

# IDP Detector Engine Release Notes

**Part Number: 530-029025-01**  
**Revision July 29, 2009, Rev 01**

## **Contents**

Recent Release History .....	2
IDP Detector Engine Overview .....	3
Understanding IDP Detector Engine Version Numbers .....	4
Displaying the IDP Detector Engine Version Number .....	5
Updating the IDP Detector Engine .....	6
Troubleshooting an IDP Detector Engine Update .....	8
Reverting the IDP Detector Engine Version .....	8
New Features and Resolved Issues .....	8
Known Issues .....	10
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
July 29, 2009	<ul style="list-style-type: none"> <li>■ 5.0.110090709</li> <li>■ 4.2.110090709</li> <li>■ 4.1.110090709</li> <li>■ 4.0.110090709</li> </ul>	Quarterly update, including new features, stability improvements, and improved accuracy. For details, see “New Features and Resolved Issues” on page 8.
June 11, 2009	<ul style="list-style-type: none"> <li>■ 10.2.150090602</li> <li>■ 10.2.140090602</li> </ul>	Released a new detector engine to support MX hardware (detector engine 10.2.150090602).  Resolved performance issues reported for detector engine 10.2.140090426.
May 28, 2009	<ul style="list-style-type: none"> <li>■ 5.0.110090504</li> </ul>	Resolved an issue with the SIP decoder.
May 12, 2009	<ul style="list-style-type: none"> <li>■ 10.2.140090426</li> </ul>	Resolved an issue with LDAP and TNS decoders.
April 27, 2009	<ul style="list-style-type: none"> <li>■ 3.1.125133</li> </ul>	Quarterly update, including stability improvements and improved accuracy.
April 15, 2009	<ul style="list-style-type: none"> <li>■ 10.2.140090407</li> <li>■ 4.2.110090322</li> <li>■ 4.1.110090407</li> <li>■ 4.0.110090407</li> <li>■ 3.5.126103</li> <li>■ 3.4.125129</li> </ul>	Quarterly update, including new features, stability improvements, and improved accuracy.
January 27, 2009	<ul style="list-style-type: none"> <li>■ 4.2.110090121</li> </ul>	Major update corresponding with the release of IDP 4.2r2. Updates include: <ul style="list-style-type: none"> <li>■ A new decoder for the MODBUS serial communications protocol.</li> <li>Improved accuracy with new contexts and other changes to reduce false positives.</li> <li>■ Increased security coverage with new anomalies.</li> <li>■ Resolution of issues with DNS, H.225 SGN, HTML, LDAP, MS-SQL, SIP, and SMB decoders.</li> </ul>

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

Release Date	Detector Engine Version	Features and Resolved Issues
January 15, 2009	<ul style="list-style-type: none"> <li>■ 4.1.110090107</li> <li>■ 4.0.110090107</li> <li>■ 3.4.121591</li> <li>■ 3.1.121592</li> </ul>	Major update, including: <ul style="list-style-type: none"> <li>■ A new decoder for the MODBUS serial communications protocol.</li> <li>■ Resolution of issues with DNS, H.225 SGN, LDAP, MS-SQL, SIP, SMB, and TNS decoders.</li> <li>■ Increased security coverage with new anomalies.</li> <li>■ Improved accuracy with new contexts and other changes to reduce false positives.</li> </ul>
January 5, 2009	<ul style="list-style-type: none"> <li>■ 3.4.118904</li> <li>■ 3.1.118905</li> </ul>	Provides the following new features and fixes: <ul style="list-style-type: none"> <li>■ 397759, 397759-2. Resolved an issue in the DNS decoder that could result in a security module crash.</li> <li>■ 400464, 400467. Improved the SMB decoder with new features and anomalies.</li> <li>■ 400468, 400469. Resolved an issue in the SMB decoder. It now generates UUID context.</li> </ul>
December 31, 2008	<ul style="list-style-type: none"> <li>■ 4.1.110081106</li> <li>■ 4.0.110081106</li> </ul>	Improves coverage and accuracy for the SIP, SMB, DNS, MS-SQL, and HTTP protocols.
October 23, 2008	<ul style="list-style-type: none"> <li>■ 4.1.110081008</li> <li>■ 4.0.110081008</li> <li>■ 3.4.117413</li> <li>■ 3.1.117412</li> </ul>	Improves coverage and accuracy for LDAP, SSL, and HTTP protocols.
September 18, 2008	<ul style="list-style-type: none"> <li>■ 4.1.110080916</li> </ul>	Improves coverage and accuracy for SSI and SIP protocols.
August 21, 2008	<ul style="list-style-type: none"> <li>■ 3.4.114929</li> <li>■ 3.1.115140</li> </ul>	Improves coverage and accuracy for the VOIP/SIP protocol.

## 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 OS, ScreenOS, or JUNOS code bases. 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 family 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
J-Services: MX Series	JUNOS 9.4 and later	10.2.150YYMMDD
SRX: SRX5800, SRX5600, SRX3600, SRX3400	JUNOS 9.2 and later	10.2.140YYMMDD
JSRX: SRX650, SRX240, SRX210	JUNOS 9.4 and later	9.2.160YYMMDD
JSR: J-Series	JUNOS 9.5 and later	9.2.130YYMMDD
IDP8200, IDP800, IDP250, IDP75, IDP1100, IDP600, IDP200	IDP 5.0.x	5.0.110YYMMDD
IDP8200	IDP 4.2.x	4.2.110YYMMDD
IDP 75/250/800, IDP 50/200/600/1100, IDP 10/100/500/1000	IDP 4.1.x	4.1.110YYMMDD
IDP 50/200/600/1100, IDP 10/100/500/1000	IDP 4.0.x	4.0.110YYMMDD
ISG 1000/2000	ScreenOS 6.2.x	3.5.xxxxxx
ISG 1000/2000	ScreenOS 6.1x, 6.0.x	3.4.xxxxxx
ISG 1000/2000	ScreenOS 5.4.x, 5.0.x	3.1.xxxxxx

## Displaying the IDP Detector Engine Version Number

---

**NSM** 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.

**IDP OS CLI** 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 ~]#

```

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

1. Connect to the CLI as the user **admin** and 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]#
```

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

**JUNOS CLI** To display the IDP detector engine version number on a JUNOS 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

---

**NSM** To update IDP detector engine using NSM:

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:

For IDP or ISG, 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.

---

For JUNOS devices, select **Devices > IDP Detector Engine > Load IDP Detector Engine for JUNOS** and complete the wizard steps.



**NOTE:** There is a known issue using NSM to update the detector engine on devices running JUNOS 9.4 and 9.5. To work around, use the JUNOS CLI or J-Web to update.

---

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**.

**JUNOS CLI** To update a JUNOS device using the JUNOS CLI:

1. Download the security package. The security package includes the detector and the latest attack objects and groups.

```
user@host> request security idp security-package download full-update
```

2. Update the attack database, the active policy, and the detector with the new package.

```
user@host> request security idp security-package install
```

3. Check the attack database update status with the following command. The command output displays information about the downloaded and installed versions of attack database versions.

```
user@host> request security idp security-package install status
```

4. Commit the configuration.

For additional information, see the [Security Configuration Guide for J-series Services Routers and SRX-series Services Gateways](#).

**J-Web** To update a JUNOS device using J-Web Quick Configuration:

1. Select **Configuration > Quick Configuration > Security Policies > IDP Policies**.
2. From the IDP policies page, click **Security Package Update**.
3. From the IDP page, click **Signature/Policy Update**.
4. Complete the configuration as described in the online help or *Security Configuration Guide*.
5. Click **Apply**.

For additional information, see the [Security Configuration Guide for J-series Services Routers and SRX-series Services Gateways](#).

## Troubleshooting an IDP Detector Engine Update

In NSM, 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

Table 3 on page 8 describes new features and fixed issues included in this release.

**Table 3: New Features and Resolved Issues**

PR	Description	5.0.x	4.2.x	4.1.x/4.0.x
<b>New Features</b>				
436438	<p>Added two new RTP decoders: audio and video.</p> <p>These decoders are disabled by default. If you want to use them, enter the following CLI command:</p> <pre>scio const -p sip set sc_sip_rtp_detect 1</pre> <p><b>NOTE:</b> The RTP audio and video decoders are not supported currently for OS that run on multiple CPU (IDP 5.0 and IDP 4.2).</p>	n/a	n/a	7-29-09

**Table 3: New Features and Resolved Issues (continued)**

PR	Description	5.0.x	4.2.x	4.1.x/4.0.x
442414	Added the following protocol anomalies to detect HTTP traffic where the length of the URL exceeds the specified bytes: <ul style="list-style-type: none"> <li>■ HTTP:AUDIT:LENGTH-OVER-256</li> <li>■ HTTP:AUDIT:LENGTH-OVER-512</li> <li>■ HTTP:AUDIT:LENGTH-OVER-1024</li> <li>■ HTTP:AUDIT:LENGTH-OVER-2048</li> <li>■ HTTP:AUDIT:LENGTH-OVER-4096</li> <li>■ HTTP:AUDIT:LENGTH-OVER-8192</li> </ul>	7-29-09	7-29-09	7-29-09
<b>Stability Improvements</b>				
433175, 433819	Resolved a memory-related issue with the MSRPC decoder in the 4.1 detector that had resulted in high CPU, link flapping, and /var/log/kernel log messages similar to the following: <pre>kernel:Mar 19 10:19:56 kernel: __alloc_pages: 3-order allocation failed (gfp=0x20/0) kernel:Mar 19 10:20:33 kernel: __alloc_pages: 3-order allocation failed (gfp=0x20/1) kernel:Mar 19 10:20:33 kernel: __alloc_pages: 3-order allocation failed (gfp=0x20/0) kernel:Mar 19 10:22:29 kernel: __alloc_pages: 3-order allocation failed (gfp=0x20/1) kernel:Mar 19 10:22:29 kernel: __alloc_pages: 3-order allocation failed (gfp=0x20/0)</pre>	7-29-09	7-29-09	7-29-09
444981	Resolved an issue with the SIP decoder that had resulted in a crash.	7-29-09	7-29-09	7-29-09
455804	Resolved an issue with the ICMP decoder that had resulted in a crash when processing the NON_ZERO_DATA_LENGTH anomaly.	7-29-09	n/a	n/a
458042	Resolved an issue with the SMB decoder that had resulted in a crash.	7-29-09	7-29-09	7-29-09
458791	Resolved a memory-related issue with the LDAP decoder that had resulted in a crash.	7-29-09	7-29-09	7-29-09
<b>Improved Accuracy</b>				
423369	Additional refinements to improve the accuracy of the SMB:ERROR:GRIND anomaly.	7-29-09	7-29-09	7-29-09
440351	Resolved an issue with the SMTP decoder that had caused unexpected behavior matching the SMTP:INVALID-DUP BOUNDARY attack object.	7-29-09	7-29-09	7-29-09
446744	Resolved an issue with the HTTP decoder that could lead to unexpected results when processing unicode text.	7-29-09	7-29-09	7-29-09

## Known Issues

---

There are no known issues to report.

## Contacting Juniper Networks Technical Assistance Center (JTAC)

---

If you need additional information or assistance, contact JTAC by E-mail ([support@juniper.net](mailto: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.