

IDP Detector Engine Release Notes

Part Number: 530-029025-01
Revision December 3, 2009, Rev 02

Contents

Recent Release History	2
IDP Detector Engine Overview	4
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
Resolved Issues	8
Junos Detector Engines	8
ScreenOS Detector Engines	10
Known Issues	10
Contacting Juniper Networks Technical Assistance Center (JTAC)	11

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
December 3, 2009	<ul style="list-style-type: none"> ■ 10.2.160091104 ■ 10.2.150091104 ■ 10.2.140091104 ■ 3.5.134268 ■ 3.4.134268 ■ 3.1.134269 	<p>Quarterly release for Junos OS and ScreenOS platforms. For details, see “Resolved Issues” on page 8.</p> <p>NOTE: A new detector engine for JSR (J Series) is not available at this time.</p>
September 2, 2009	<ul style="list-style-type: none"> ■ 10.2.160090831 ■ 10.2.150090831 ■ 10.2.140090831 ■ 10.2.130090831 	Quarterly release for Junos OS platforms.
September 2, 2009	<ul style="list-style-type: none"> ■ 5.0.110090831 ■ 4.2.110090831 ■ 4.1.110090831 ■ 4.0.110090831 	Resolved an issue with the previously released IDP OS detector engine.
August 20, 2009	<ul style="list-style-type: none"> ■ 5.0.110090817 ■ 4.2.110090817 ■ 4.1.110090817 ■ 4.0.110090817 	Resolved issues reported with the July 29, 2009 detector engine.
August 17, 2009	<ul style="list-style-type: none"> ■ 3.5.133962 ■ 3.4.133962 ■ 3.1.133961 	Quarterly update for ScreenOS platforms, including new features, stability improvements, and improved accuracy.
July 29, 2009	<ul style="list-style-type: none"> ■ 10.2.160090831 ■ 10.2.140090831 ■ 10.2.130090831 ■ 5.0.110090709 ■ 4.2.110090709 ■ 4.1.110090709 ■ 4.0.110090709 	Quarterly update for IDP OS platforms, including new features, stability improvements, and improved accuracy.
June 11, 2009	<ul style="list-style-type: none"> ■ 10.2.150090602 ■ 10.2.140090602 	<p>Released a new detector engine to support MX hardware (detector engine 10.2.150090602).</p> <p>Resolved performance issues reported for detector engine 10.2.140090426.</p>

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

Release Date	Detector Engine Version	Features and Resolved Issues
May 28, 2009	■ 5.0.110090504	Resolved an issue with the SIP decoder.
May 12, 2009	■ 10.2.140090426	Resolved an issue with LDAP and TNS decoders.
April 27, 2009	■ 3.1.125133	Quarterly update, including stability improvements and improved accuracy.
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.
January 27, 2009	■ 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.
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.

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 OS 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/subscribe.jsp?actionBtn=Modify> (login required). We also suggest you subscribe to the RSS feed to follow signature update announcements. Go to <http://rss.juniper.net/p/subscribe> (no login required).

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
Branch SRX: SRX650, SRX240, SRX210, SRX100	Junos OS 9.4 and later	10.2.160YYMMDD
J-Services: MX Series	Junos OS 9.5 and later	10.2.150YYMMDD
High-end SRX: SRX5800, SRX5600, SRX3600, SRX3400	Junos OS 9.2 and later	10.2.140YYMMDD
JSR: J-Series	Junos OS 9.5 and later	10.2.130YYMMDD
IDP8200, IDP800, IDP250, IDP75 IDP1100, IDP600, IDP200	IDP 5.0.x	5.0.110YYMMDD
IDP8200	IDP 4.2.x	4.2.110YYMMDD
IDP800, IDP250, IDP75 IDP1100, IDP600, IDP200, IDP50 IDP1000, IDP500, IDP100, IDP10	IDP 4.1.x	4.1.110YYMMDD

Table 2: IDP Detector Engine Version Compatibility (continued)

Hardware	Operating System	IDP Detector Engine Version
IDP1100, IDP600, IDP200, IDP50 IDP1000, IDP500, IDP100, IDP10	IDP 4.0.x	4.0.110YYMMDD
ISG2000, ISG1000	ScreenOS 6.3.x, 6.2.x	3.5.xxxxxx
ISG2000, ISG1000	ScreenOS 6.1x, 6.0.x	3.4.xxxxxx
ISG2000, ISG1000	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 OS CLI To display the IDP detector engine version number on a Junos OS device:

1. Log into the Junos OS CLI and enter operational mode. For details, see the Junos OS 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 OS devices, select **Devices > IDP Detector Engine > Load IDP Detector Engine for JUNOS** and complete the wizard steps.

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 OS CLI To update a Junos OS device using the Junos OS 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 OS 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 *Junos Software 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).

Resolved Issues

The following sections describe issues resolved in this release:

- Junos Detector Engines on page 8
- ScreenOS Detector Engines on page 10

Junos Detector Engines

The following table describes issues resolved in Junos detector engines.

Table 3: Junos OS Detector Engines: Resolved Issues

Tracking PR	Description
DNS	
448109	Resolved an issue with the DNS decoder that had Dec 09? Dec 09? ??? resulted in only the first anomaly in a session being detected.
464269	Resolved an issue with the DNS decoder. The implementation for processing the transaction scope for chain signatures required changes.

Table 3: Junos OS Detector Engines: Resolved Issues (continued)

Tracking PR	Description
HTTP	
225151	Resolved an issue with the HTTP decoder where the http-object-tag-clsid context had not spanned over packets.
387759	Additional refinements to the HTTP decoder to reduce false positives for brute force login attempts.
474103	Resolved an issue with the HTTP decoder that had resulted in false positives with the CLSID context.
473926	Improved the accuracy of header overflow detection with the HTTP decoder.
MSRPC	
467450	Added logic to process the following new MSRPC contexts: <ul style="list-style-type: none"> ■ msrpc-call. Matches the request data in a MSRPC session. ■ msrpc-ans. Matches the response data in a MSRPC session. ■ msrpc-raw. Matches raw data in a MSRPC session.
477098	Resolved an issue with the MSRPC decoder that had resulted in a crash.
SIP	
473276	Changed the SIP decoder so that it is not used when the IDP engine processes Microsoft Live Communication Server (LCS) flows. Such traffic had triggered a lot of false positives.

Table 3: Junos OS Detector Engines: Resolved Issues *(continued)*

Tracking PR	Description
SMTP	
471116	Changed the SMTP decoder so that the SMTP: INVALID-FILENAME anomaly does not trigger on a zero-length filename.
439820	Changed the SMTP decoder to reduce false positives that had been triggered by the SMTP:COMMAND:HELP anomaly.
452345	Resolved an issue with the SMTP decoder that had resulted in false positives triggered by the SMTP:AUDIT:DUPLICATE:HEADER anomaly.
484391	Resolved a memory-related issue with the SMTP decoder that had resulted in a crash.
SSH	
476813	Resolved a memory-related issue with the SSH decoder that had resulted in a crash.
UDP	
469994	Resolved an issue with the UDP reader that could result in a crash under high stress.

ScreenOS Detector Engines

The following table describes issues resolved in ScreenOS detector engines.

Table 4: ScreenOS Detector Engines: Resolved Issues

Tracking PR	Description	Versions Fixed
HTTP		
225151	Resolved an issue with the HTTP decoder where the http-object-tag-clsid context had not spanned over packets.	3.4.134268 3.1.134269
477057	Resolved an issue with the HTTP decoder where URL parsing had stopped unexpectedly when encountering a null character.	3.5.134268 3.1.134269

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) 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.