

IDP Detector Engine Release Notes

Part Number: 530-029025-01
Revision August 11, 2011

Contents

Recent Release History	2
IDP Detector Engine Overview	4
Understanding IDP Detector Engine Version Numbers	4
Displaying the IDP Detector Engine Version Number	6
Using NSM to Display the Detector Engine Version	6
Using the IDP OS CLI to Display the Detector Engine Version	6
Using the Junos OS CLI to Display the Detector Engine Version	7
Using the ScreenOS CLI to Display the Detector Engine Version	7
Updating the IDP Detector Engine	7
Using NSM to Update the Detector Engine Software	8
Using the Junos OS CLI to Update the Detector Engine Software	8
Using J-Web to Update the Detector Engine Software	9
Troubleshooting an IDP Detector Engine Update	9
Reverting the IDP Detector Engine Version	9
Inspecting Compressed HTTP Traffic	9
IDP OS: Suppressing Compressed HTTP	9
Junos OS: Decompressing Compressed HTTP	10
Resolved Issues	11
Contacting Juniper Networks Technical Assistance Center (JTAC)	12

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
August 11, 2011	<ul style="list-style-type: none"> • IDP OS <ul style="list-style-type: none"> • 5.1.110110809 • 5.0.110110809 • Junos OS <ul style="list-style-type: none"> • 11.6.160110809 • 11.6.150110809 • 11.6.140110809 • 11.6.130110809 • ScreenOS <ul style="list-style-type: none"> • 3.5.138480 • 3.4.138480 	Quarterly release for IDP OS, Junos OS, and ScreenOS platforms. For details on new features, see “Inspecting Compressed HTTP Traffic” on page 9. For a summary of other improvements, see “Resolved Issues” on page 11.
June 15, 2011	<ul style="list-style-type: none"> • IDP OS <ul style="list-style-type: none"> • 5.1.110110609 • 5.0.110110609 • 4.1.110110609 	Resolved issue with the SMB and VNC protocol decoders.
April 1, 2011	<ul style="list-style-type: none"> • IDP OS <ul style="list-style-type: none"> • 5.1.110110331 • 5.0.110110331 • 4.1.110110331 • Junos OS <ul style="list-style-type: none"> • 11.4.160110331 • 11.4.150110331 • 11.4.140110331 • 11.4.130110331 • ScreenOS <ul style="list-style-type: none"> • 3.5.137717 • 3.4.137717 	Resolved issues related to the HTTP and SMB protocol decoders.

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

Release Date	Detector Engine Version	Features and Resolved Issues
March 1, 2011	<ul style="list-style-type: none"> • IDP OS <ul style="list-style-type: none"> • 5.1.110110223 • 5.0.110110223 • 4.1.110110223 • Junos OS <ul style="list-style-type: none"> • 11.4.160110223 • 11.4.150110223 • 11.4.140110223 • 11.4.130110223 • ScreenOS <ul style="list-style-type: none"> • 3.5.137562 • 3.4.137562 	Quarterly release for IDP OS, Junos OS, and ScreenOS platforms.
December 7, 2010	<ul style="list-style-type: none"> • IDP OS <ul style="list-style-type: none"> • 5.0.110101203 • 4.2.110101203 • 4.1.110101203 • Junos OS <ul style="list-style-type: none"> • 10.4.160101203 • 10.4.150101203 • 10.4.140101203 • 10.4.130101203 • ScreenOS <ul style="list-style-type: none"> • 3.5.137241 • 3.4.137241 	Quarterly release for IDP OS, Junos OS, and ScreenOS platforms. Improved coverage and accuracy for the HTTP, SMB, MSRPC, and LDAP protocol decoders.
October 21, 2010	<ul style="list-style-type: none"> • IDP OS – 5.0.110101021 • Junos OS – 10.4.140101021 	Resolved issues and improved stability of the detector used with IDP OS 5.0 and Junos OS high-end SRX.
September 27, 2010	5.0.110100923	PR 543814. Resolved a memory-related issue with the TNS protocol decoder that could result in a crash in mixed network environments with highly fragmented traffic. This issue was found in the 5.0.110100823 detector engine (IDP OS).

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

Release Date	Detector Engine Version	Features and Resolved Issues
August 24, 2010	<ul style="list-style-type: none"> • IDP OS <ul style="list-style-type: none"> • 5.0.110100823 • 4.2.110100823 • 4.1.110100823 • Junos OS <ul style="list-style-type: none"> • 10.4.160100823 • 10.4.150100823 • 10.4.140100823 • 10.4.130100823 • ScreenOS <ul style="list-style-type: none"> • 3.5.136540 • 3.4.136540 	Quarterly release for IDP OS, Junos OS, and ScreenOS platforms. We now support IEC104 and MODBUS protocol decoders for Junos OS. This release also improves stability, coverage, and accuracy for several protocol decoders.

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 and application signature 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
IDP Series: IDP8200, IDP800, IDP250, IDP75 IDP1100, IDP600, IDP200	IDP 5.1.x	5.1.110YYMMDD
IDP Series: IDP8200, IDP800, IDP250, IDP75 IDP1100, IDP600, IDP200	IDP 5.0.x	5.0.110YYMMDD
IDP Series: IDP800, IDP250, IDP75 IDP1100, IDP600, IDP200, IDP50	IDP 4.1.x	4.1.110YYMMDD
SRX Series (branch): SRX650, SRX240, SRX210, SRX100	Junos OS 9.4 and later	11.6.160YYMMDD
M/MX Series	Junos OS 9.4 and later	11.6.150YYMMDD
SRX Series (high end): SRX5800, SRX5600, SRX3600, SRX3400, SRX1400	Junos OS 9.2 and later	11.6.140YYMMDD
J Series	Junos OS 9.5 and later	11.6.130YYMMDD
ISG Series: ISG2000, ISG1000	ScreenOS 6.3.x, 6.2.x	3.5.xxxxxx
ISG Series: ISG2000, ISG1000	ScreenOS 6.1x, 6.0.x	3.4.xxxxxx



NOTE: 2010 versions of the detector engine for Junos OS were numbered 10.4.1x0.YYMMDD.



NOTE: The last detector engine update for IDP OS 4.2 was 4.2.110101203 on December 7, 2010. We advise you to upgrade to IDP OS 5.0.x or later.



NOTE: The last detector engine update for IDP OS 4.1 was 4.110110609 on June 15, 2011. We advise you to upgrade to IDP OS 5.0.x or later.



NOTE: The last detector engine update for ScreenOS 5.4.x was detector engine 3.1.135801 on May 26, 2010. We advise you to upgrade to ScreenOS 6.x.

Displaying the IDP Detector Engine Version Number

The following topics give procedures for displaying the IDP detector engine version number:

- Using NSM to Display the Detector Engine Version on page 6
- Using the IDP OS CLI to Display the Detector Engine Version on page 6
- Using the Junos OS CLI to Display the Detector Engine Version on page 7
- Using the ScreenOS CLI to Display the Detector Engine Version on page 7

Using NSM to Display the Detector Engine Version

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 IDP OS and Junos OS devices, the Info node displays version information, including the IDP detector engine version.

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

Using the IDP OS CLI to Display the Detector Engine Version

To display the IDP detector engine version number on an IDP OS 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 May  9 17:31:47 2010 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: 5.0.110100517
Software License: Evaluation
Software Expiration Date: 4/25/2011
[root@idp ~]#
```

In this example, the version is 5.0.110100517.

Using the Junos OS CLI to Display the Detector Engine Version

To display the IDP detector engine version 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:1651(Wed May 21 16:42:03 2010)
Detector version :10.4.140100513
Policy template version :N/A
```

In this example, the detector version number is 10.4.140100513.

Using the ScreenOS CLI to Display the Detector Engine Version

To display the IDP detector engine version number on a ScreenOS 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 3.5.135690

[root@default host admin]#
```

The line for detector.so shows the version of the detector. In this example, the version is 3.5.135690.

Updating the IDP Detector Engine

The following topics give procedures for updating IDP detector engine software:

- Using NSM to Update the Detector Engine Software on page 8
- Using the Junos OS CLI to Update the Detector Engine Software on page 8
- Using J-Web to Update the Detector Engine Software on page 9

Using NSM to Update the Detector Engine Software

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 OS or ScreenOS devices, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.

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**.



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

Using the Junos OS CLI to Update the Detector Engine Software

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 Junos OS security configuration [documentation](#).

Using J-Web to Update the Detector Engine Software

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.
5. Click **Apply**.

For additional information, see the Junos OS security configuration [documentation](#).

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 the IDP feature set 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).

Inspecting Compressed HTTP Traffic

The following sections describe HTTP protocol decoder features that enable you to inspect compressed HTTP traffic:

- IDP OS: Suppressing Compressed HTTP on page 9
- Junos OS: Decompressing Compressed HTTP on page 10

IDP OS: Suppressing Compressed HTTP

HTTP compression is a popular Web server feature because compression saves bandwidth. However, compressed data cannot be inspected by attack detection systems. Typically, attack detection systems must either drop or pass through compressed traffic. If your

business and security policy calls for it, you can enable a feature in the HTTP decoder that forces the Web servers to retransmit the data in uncompressed form. The HTTP transaction can then be inspected by the IDP system.

The feature is disabled by default.

When this feature is enabled, the HTTP protocol decoder examines the HTTP header section content encoding value. If it detects gzip compression, the detector engine applies a special algorithm to scramble related headers from the TCP stream and the traffic is forwarded to the Web server. The Web server cannot understand the scrambled encoding type, so it falls back to sending plain (uncompressed) data. We have tested the feature with many common Web server configurations. It is possible that some Web servers will not respond to the scrambled encoding type by sending uncompressed data.

Enabling this feature has a performance cost. When enabled, you might observe decreased performance, and end users might observe slower server response when browsing Internet sites that use HTTP compression. In addition, enabling the feature increases bandwidth utilization because it forces the network to transmit uncompressed data.

To enable the feature, use the following command:

```
[root@default host ~]# scio const -p http set sc_http_compress_suppression 1
```

To disable the feature, use the following command:

```
[root@default host ~]# scio const -p http set sc_http_compress_suppression 0
```



NOTE: The feature is currently supported on IDP OS 5.1 and later.

Junos OS: Decompressing Compressed HTTP

As noted, the IDP OS enables inspection of compressed HTTP traffic by suppressing the transmission of compressed traffic, thereby forcing the Web Server to send uncompressed traffic, which can be inspected. In contrast, the Junos OS enables inspection by performing the decompression.

The feature is disabled by default.

To enable the feature, use the following command:

```
[edit]
user@host# set security idp sensor-configuration detector protocol-name HTTP tunable-name
sc_http_compress_inflating tunable-value 1
```

To disable the feature, use the following command:

```
[edit]
user@host# set security idp sensor-configuration detector protocol-name HTTP tunable-name
sc_http_compress_inflating tunable-value 0
```

For more information about the Junos OS detector engine configuration for HTTP decompression, including memory-management options, see the Junos OS security configuration [documentation](#).



NOTE: This feature is currently supported on Junos OS 11.2 and later.

Resolved Issues

The following table describes issues that have been resolved in this release.

Table 3: Resolved Issues

PR	Description
DNS	
597054	Updated to generate a new service context: dns-update-header. This context matches the header of a DNS UPDATE request or response.
HTTP	
595193	<p>Improved performance by removing:</p> <ul style="list-style-type: none"> • http-get-url-parsed-param • http-post-url-parsed-param • http-head-url-parsed-param • http-get-url-parsed-param-parsed • http-post-url-parsed-param-parsed • http-head-url-parsed-param-parsed • http-text-html-body <p>If your IDP security policy includes custom signatures that use the contexts that have been removed, you must modify your attack object definitions to avoid policy compilation errors. See Example: Modifying Custom Attack Objects Related to Signature Update #1972 in the <i>IDP Series Custom Attack Objects Reference and Examples Guide</i>. The guidelines and examples that explain this update apply to attack objects used in IDP OS, Junos OS, and ScreenOS systems.</p>
IMAP	
589884	Improved implementation to reduce false positives with the <code>IMAP:OVERFLOW:TAG</code> protocol anomaly.
LDAP	
594276	Improved implementation to reduce false positives with the <code>LDAP:INVALID:REQTYPE_INVALID</code> protocol anomaly.
MSRPC	
673258	Resolved an issue with the MSRPC decoder not properly generating the msrpc-call context.
SMB	
659929	In the June 15, 2011 release notes , we reported that we had resolved an issue with the IDP OS detector engine that had resulted in an inordinate number of logs being generated. In this release, we have ported the fix to all platforms.
SSL	
586215	Improved implementation to avoid a potential memory issue when processing fragmented traffic.

Table 3: Resolved Issues (continued)

PR	Description
TFTP	
596408	Added detector engine support to detect a new protocol anomaly: <code>TFTP:MODE_TOO_LONG</code> .
VNC	
593974	Improved implementation to avoid a potential memory issue.
661669	Improved implementation to reduce false positives with the <code>VNC:INVALID:CLIENT-REQUEST</code> protocol anomaly.
Yahoo Messenger	
605135	Updated the detector engine to adapt to changes in the Yahoo Messenger protocol. We have added a context named <code>ymsg-header</code> to match data in the protocol header. We have deleted the context named <code>ymsg-file-name</code> .

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 © 2011, 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. 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.