

IDP Detector Engine Release Notes

June 24, 2015
Part Number: 530-029025-01

Contents

Recent Release History	2
IDP Detector Engine Overview	4
Understanding IDP Detector Engine Version Numbers	5
Displaying the IDP Detector Engine Version Number	5
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	6
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	7
Using the Junos OS CLI to Update the Detector Engine Software	8
Using J-Web to Update the Detector Engine Software	8
Troubleshooting an IDP Detector Engine Update	8
Reverting the IDP Detector Engine Version	9
Resolved Issues	9
Requesting Technical Support	9
Self-Help Online Tools and Resources	10
Opening a Case with JTAC	10
Revision History	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
June 25, 2015	IDP OS <ul style="list-style-type: none"> 5.1.110150609 Junos OS <ul style="list-style-type: none"> 12.6.160150609 12.6.150150609 12.6.140150609 12.6.130150609 Screen OS <ul style="list-style-type: none"> 3.5.141332 	Service release for IDP OS, Junos OS, and ScreenOS platforms.
September 10, 2014	IDP OS <ul style="list-style-type: none"> 5.1.110140822 Junos OS <ul style="list-style-type: none"> 12.6.160140822 12.6.150140822 12.6.140140822 12.6.130140822 Screen OS <ul style="list-style-type: none"> 3.5.140842 	Service release for IDP OS, Junos OS, and ScreenOS platforms.
June 17, 2014	IDP OS <ul style="list-style-type: none"> 5.1.110140603 Junos OS <ul style="list-style-type: none"> 12.6.160140603 12.6.150140603 12.6.140140603 12.6.130140603 ScreenOS <ul style="list-style-type: none"> 3.5.140733 	Feature release. This release introduces new HTTP service contexts http-flash , http-ole , and http-pdf . Predefined signatures that used to use the http-data context to detect Flash, OLE, and PDF files have been rewritten to use the new context. If you have created custom signatures to detect Flash, OLE, or PDF, we recommend you rewrite your signatures to use the new, simpler contexts.

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

Release Date	Detector Engine Version	Features and Resolved Issues
February 11, 2014	IDP OS <ul style="list-style-type: none"> • 5.1.110140207 Junos OS <ul style="list-style-type: none"> • 12.6.160140207 • 12.6.150140207 • 12.6.140140207 • 12.6.130140207 ScreenOS <ul style="list-style-type: none"> • 3.5.140407 	Service release for IDP OS, Junos OS, and ScreenOS platforms.
November 26, 2013	IDP OS <ul style="list-style-type: none"> • 5.1.110131122 Junos OS <ul style="list-style-type: none"> • 12.6.160131122 • 12.6.150131122 • 12.6.140131122 • 12.6.130131122 ScreenOS <ul style="list-style-type: none"> • 3.5.140347 	Service release for IDP OS, Junos OS, and ScreenOS platforms.
July 25, 2013	IDP OS <ul style="list-style-type: none"> • 5.1.110130715 Junos OS <ul style="list-style-type: none"> • 12.6.160130715 • 12.6.150130715 • 12.6.140130715 • 12.6.130130715 ScreenOS <ul style="list-style-type: none"> • 3.5.140185 	Service release for IDP OS, Junos OS, and ScreenOS platforms.

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

Release Date	Detector Engine Version	Features and Resolved Issues
April 16, 2013	IDP OS <ul style="list-style-type: none"> • 5.1.110130325 Junos OS <ul style="list-style-type: none"> • 12.6.160130325 • 12.6.150130325 • 12.6.140130325 • 12.6.130130325 ScreenOS <ul style="list-style-type: none"> • 3.5.140032 	Service release for IDP OS, Junos OS, and ScreenOS platforms.

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 Intelligence Center releases IDP detector engine updates more frequently in order to ensure that 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 the Security Intelligence 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	IDP 5.1.x	5.1.110YYMMDD
SRX Series (branch): SRX650, SRX240, SRX210, SRX100	Junos OS 9.4 and later	12.6.160YYMMDD
M/MX Series	Junos OS 9.4 and later	12.6.150YYMMDD
SRX Series (high end): SRX5800, SRX5600, SRX3600, SRX3400, SRX1400	Junos OS 9.2 and later	12.6.140YYMMDD
J Series	Junos OS 9.5 and later	12.6.130YYMMDD
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: **ScreenOS 6.1 reached **end-of-life** on January 28, 2012. We advise you to upgrade to ScreenOS 6.2 or later.

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 6](#)
- [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 Series device:

- In the NSM device manager, double-click the IDP or ISG Series 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 in to 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 7](#)
- [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 8](#)

Using NSM to Update the Detector Engine Software

To update the 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).

Resolved Issues

Table 3 describes issues that have been resolved in this release.

Table 3: Resolved Issues

PR	Description
IDP	
1034091	In IDP detector engine versions prior to version 5.1.110150609, IDP ran in transparent mode. This issue is now resolved.
1041355	The Network Time Protocol (NTP) authenticator field message length was not being updated. This issue is now resolved.
1060049	The anomaly DNS:AUDIT:REP-MISMATCHING-AN was raised when a domain name system (DNS) type A did not respond to a query. This issue is now resolved.
1079042	Resolved a memory-related issue that could result in a flowd on core with the warning message “?sc_ssl_process_decrypted?”.
1044441	On IDP, while updating a policy, a warning message appeared. This issue is now resolved.
1001808	On an SRX Series device, after IDP was enabled, the CPU displayed 100%. This issue is now resolved.
1013564	Updating IDP from NSM failed at the same time as the associated link flap. This issue is now resolved.
1082510	On IDP, running the Virtual Teletype (VTY) debugging commands resulted in a core dump and a failover. This issue is now resolved.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

Revision History

26 June 2015—Revision 2, IDP Detector Engine Release Notes

24 June 2015—Revision 1, IDP Detector Engine Release Notes

Copyright © 2015, 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.