Release Notes for the Cisco Intrusion Prevention System Device Manager 7.3.1

Published: January 15, 2014, OL-30816-01

Contents

System Requirements

The IDM 7.3.1 has the following system requirements:

- Supports IPS 7.3(1)E4
- Supported Operating Systems
  - Windows Vista Business and Ultimate (32-bit only)
  - Windows XP Professional (32-bit only)
  - Windows 7 (32- and 64-bit)

Cisco Systems, Inc.
www.cisco.com

  - Windows Server 2003
  - Windows Server 2008 (32- and 64-bit)
  - Red Hat Linux Desktop Version 4
  - Red Hat Enterprise Linux Server Version 4
- Java SE 6.0 or later
- JRE 1.6 or later
- Supported browsers
  - Internet Explorer 6.0 or later
  - Firefox 2.0 or later
  - Chrome
- Minimum hardware requirements
  - 512 MB or more strongly recommended
  - Pentium, AMD Athlon, or equivalent running at 1 Ghz or higher
  - 1024 x 768 resolution and 256 colors (minimum)
- Supported Cisco IPS hardware platforms:
  - IPS 4345
  - IPS 4345-DC
  - IPS 4360
  - IPS 4510
  - IPS 4520

New and Changed Information

IDM 7.3.1 has the following new features:

- Support for IPS 7.3(1)E4.

  IDM 7.3.1 is included in IPS 7.3(1)E4.
- Threat profile enhancements:
  - You no longer have to manually tune signature sets for deployment.
  - You can create a new signature instance using a threat profile, view a list of signatures contained in a certain profile, and create a new signature instance without applying a threat profile.
  - You can apply/remove a threat profile for a signature instance, assign a threat profile to a virtual sensor, apply a template to a signature instance, and create a new signature instance with a threat profile applied on the fly.
  - You can view the list of signatures that are present in a threat profile.
  - You can remove a threat profile from the virtual sensor or remove the threat profile from the signature instance assigned to the virtual sensor.
  - You can determine if a threat profile has been applied on a sensor.

  - You can preserve user tunings. A message is displayed stating that the tunings are preserved when the threat profile is applied and your tunings will be preferred in case of a conflict. When a threat profile is applied on a signature instance, the IDM first applies the user tunings (current configuration) on the default configuration, then it applies the signature template to the complete configuration. During this process if a tuned signature is found, it will not be changed.
  - Configuration > Signature Configuration > Add Policy/Clone Policy

    You can add a threat profile here.
  - Configuration > Policies > Signature Definitions

    You can manage signature instances and threat profiles here.
  - Configuration > Policies > Signature Definitions > sig0

    Right-click the signature instance to apply, remove, replace templates, and delete signature instances. You can identify the threat profile on the bottom pane and mouse-over on the signature instance, which shows the threat profile name, profile version, signature version, and virtual sensor assignment.
  - Configuration > Policies > Signature Definitions > sig0 > All Signatures > Threat Profile

    Apply/replace/delete threat profiles here.
  - Configuration > Policies > IPS Policies

    You can identify the threat profile for the virtual sensor.
  - Edit Virtual Sensor

    You can identify the threat profile and can creat a new signature instance with a threat profile.
  - Threat profiles provide Cisco-recommended set of signatures for different deployment profiles: Edge, Data Center, Web Applications, and SCADA.
  - Threat profiles are delivered along with signature sets as a part of signature updates; your tunings are retained.
- Link Aggregation Control Protocol (LACP) support for the IPS 4500 series sensors:
  - Provides scalability with an aggregate throughput of 80 Gbps with 16 sensors connected in a port channel.
  - Helps the switch to detect the IPS failures faster and redistribute the traffic among other members of the port channel.
  - Configuration > Interfaces > LACP

    You can configure LACP here. You must have inline VLAN pairs configured first on your sensor and LACP configured on a Cisco Nexus 7K or Catalyst 6K switch.
  - Sensor Monitoring > LACP > LACP Neighbor

    You can view the LACP neighbors with the system details.
  - Sensor Monitoring > LACP > LACP Internal

    You can view the LACP internals with their system details.
- Improved and stable SMB Advanced signature engine:
  - Enhanced inspection for MSRPC request handling code execution vulnerability
  - Support for Big-endian MSPRC traffic
  - Multiple DCE-RPC requests in single WriteAndX command
  - SMB AndX command with wordcount 0

  - SMB Predator Decoy trees evasion
  - Buffer overflow attempt to exploit the call_trans2open function of Samba
  - Evasion with small RPC segments in conjunction with window resizing
- Base64 decoding support for HTTP traffic:
  - Inspection capability improvement with cross site scripting (XSS)
  - Prevents client-side exploits by inspecting Base64 encoded data
  - Decodes the HTML, CSS, and XML Base64 encoded data carried in the HTTP response payload
- Improved software capacity to enable additional signatures
- TCP failover/fallback session continuity

For More Information

- For detailed information on threat profiles, refer to Configuring Threat Profiles.
- For detailed information on configuring LACP on the 4500 series sensors, refer to Configuring LACP.

Obtaining Software on Cisco.com

You can find major and minor updates, service packs, signature and signature engine updates, system and recovery files, firmware upgrades, and Readmes on the Download Software site on Cisco.com. Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com in a release train format, a new release every three months. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

You must have an account with cryptographic access before you can download software. You set this account up the first time you download IPS software from the Download Software site.

Note You must be logged in to Cisco.com to download software. You must have an active IPS maintenance contract and a Cisco.com password to download software. You must have a sensor license to apply signature updates.

Downloading Cisco IPS Software

To download software on Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 From the Support drop-down menu, choose **Download Software**.

Step 3 Under Select a Software Product Category, choose **Security Software**.

Step 4 Choose **Intrusion Prevention System (IPS)**.

Step 5 Enter your username and password.

Step 6 In the Download Software window, choose **IPS Appliances > Cisco Intrusion Prevention System** and then click the version you want to download.

Note You must have an IPS subscription service license to download software.

Step 7 Click the type of software file you need. The available files appear in a list in the right side of the window. You can sort by file name, file size, memory, and release date. And you can access the Release Notes and other product documentation.

Step 8 Click the file you want to download. The file details appear.

Step 9 Verify that it is the correct file, and click **Download**.

Step 10 Click **Agree** to accept the software download rules. The File Download dialog box appears. The first time you download a file from Cisco.com, you must fill in the Encryption Software Export Distribution Authorization form before you can download the software.

a. Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.

b. Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.

If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again.

Step 11 Open the file or save it to your computer.

Step 12 Follow the instructions in the Readme or the Release Notes to install the update.

Starting the IDM

Note After you upgrade the IPS software on your sensor, you must restart IDM so that the latest features for the new software version are present in IDM.

There are two ways to start the IDM:

- Cross launch from the IME (recommended)

  Open the IME and click **Configuration**. All IDM functionality is available in the IME.

- Through a browser

  Enter the IP address of the target sensor in the address window as follows:

  `https://xx.xx.xx.xx`

Logging In to the IDM

The IDM is a web-based, Java Web Start application that enables you to configure and manage your sensor. The web server for the IDM resides on the sensor. You can access it through Internet Explorer or Firefox web browsers.

Note The IDM is already installed on the sensor.

To log in to the IDM, follow these steps:

Step 1 Open a web browser and enter the sensor IP address. A Security Alert dialog box appears.

```
https://sensor_ip_address
```

Note The default IP address is 192.168.1.2/24,192.168.1.1, which you change to reflect your network environment when you initialize the sensor. When you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format https://*sensor_ip_address:port* (for example, https://192.0.2.1:1040).

Step 2 Click **Yes** to accept the security certificate. The Cisco IPS Device Manager Version window appears.

Step 3 To launch the IDM, click **Run IDM**. The JAVA loading message box appears, and then the Warning - Security dialog box appears.

Step 4 To verify the security certificate, check the Always trust content from this publisher check box, and click **Yes**. The JAVA Web Start progress dialog box appears, and then the IDM on *ip_address* dialog box appears.

Step 5 To create a shortcut for the IDM, click **Yes**. The Cisco IDM Launcher dialog box appears.

Note You must have JRE 1.5 (JAVA 5) installed to create shortcuts for the IDM. If you have JRE 1.6 (JAVA 6) installed, the shortcut is created automatically.

Step 6 To authenticate the IDM, enter your username and password, and click **OK**. Both the default username and password are **cisco**. You were prompted to change the password during sensor initialization. The IDM begins to load. If you change panes from Home to Configuration or Monitoring before the IDM has completed initialization, a Status dialog box appears with the following message:

```
Please wait while IDM is loading the current configuration from the sensor.
```

The main window of the IDM appears.

Note If you created a shortcut, you can launch the IDM by double-clicking the IDM shortcut icon. You can also close the The Cisco IPS Device Manager Version window. After you launch the IDM, it is not necessary for this window to remain open.

Restrictions and Limitations

The following restrictions and limitations apply to Cisco IDM 7.3.1:

- After you upgrade the IPS software on your sensor, you must restart the IDM so that the latest features for the new software version are present in the IDM.
- The IDM has been built and tested with JAVA 7 Update 45 and earlier. The IDM is not compatible with JAVA 7 Update 51. For IDM to function, you must use the older version of Java . Refer to CSCum55433 if you must use Java 7u51 and there is no option to use earlier versions.

- The IDM opens MySDN from the last browser window you opened, which is the default setting for Windows. To change this default behavior, in Internet Explorer, choose **Tools > Internet Options**, and then click the **Advanced** tab. Scroll down and uncheck the **Reuse windows for launching shortcuts** check box.
- For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.
- The IDM does not support any non-English characters, such as the German umlaut or any other special language characters. If you enter such characters as a part of an object name through IDM, they are turned into something unrecognizable and you will not be able to delete or edit the resulting object through IDM or the CLI. This is true for any string that is used by the CLI as an identifier, for example, names of time periods, inspect maps, server and URL lists, and interfaces.

For More Information

For more information about MySDN, refer to MySDN.

Unresolved Caveats

This section lists the unresolved caveats:

- CSCum55433 IDM is being blocked by Java after an upgrade to Java 7.51
- CSCum57386 IDM sometimes doesn't load with complete configuration

Cisco Security Intelligence Operations

The Cisco Security Intelligence Operations site on Cisco.com provides intelligence reports about current vulnerabilities and security threats. It also has reports on other security topics that help you protect your network and deploy your security systems to reduce organizational risk.

You should be aware of the most recent security threats so that you can most effectively secure and manage your network. Cisco Security Intelligence Operations contains the top ten intelligence reports listed by date, severity, urgency, and whether there is a new signature available to deal with the threat.

Cisco Security Intelligence Operations contains a Security News section that lists security articles of interest. There are related security tools and links.

You can access Cisco Security Intelligence Operations at this URL:

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations is also a repository of information for individual signatures, including signature ID, type, structure, and description.

You can search for security alerts and signatures at this URL:

http://tools.cisco.com/security/center/search.x

Related Documentation

For more information on Cisco IPS, refer to the following documentation found at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

Obtaining Documentation, Using the Cisco Bug Search Tool, and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.