



Release Notes for the Cisco Intrusion Prevention System Device Manager 7.1.5

Published: July 16, 2012, OL-27622-01

Revised: October 28, 2013

Contents

- [System Requirements, page 1](#)
- [System Restrictions, page 3](#)
- [New and Changed Information, page 3](#)
- [Obtaining Software on Cisco.com, page 4](#)
- [Starting the IDM, page 5](#)
- [Logging In to the IDM, page 6](#)
- [Restrictions and Limitations, page 7](#)
- [Cisco Security Intelligence Operations, page 7](#)
- [Related Documentation, page 8](#)
- [Obtaining Documentation, Using the Cisco Bug Search Tool, and Submitting a Service Request, page 8](#)

System Requirements

The IDM has the following system requirements:

- Supported IPS versions
 - IPS 6.2
 - IPS 7.0
 - IPS 7.1



Cisco Systems, Inc.
www.cisco.com

- Supported Operating Systems
 - Windows Vista Business and Ultimate (32-bit only)
 - Windows XP Professional (32-bit only)
 - Windows 7 (32- and 64-bit)
 - Windows Server 2003
 - Windows Server 2008 (32- and 64-bit)
 - Red Hat Linux Desktop Version 4
 - Red Hat Enterprise Linux Server Version 4
- Supported Java Plug-in
 - Java SE 6.0
- JRE 1.6 or later
- Supported browsers
 - Internet Explorer 6.0 and 7.0
 - Firefox 2.0
- 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 4240
 - IPS 4255
 - IPS 4260
 - IPS 4270-20
 - IPS 4345
 - IPS 4345-DC
 - IPS 4360
 - AIM IPS
 - NME IPS
 - IDSM2
 - ASA 5500 AIP SSC-5
 - ASA 5500 AIP SSM-10
 - ASA 5500 AIP SSM-20
 - ASA 5500 AIP SSM-40
 - ASA 5512-X IPS SSP
 - ASA 5515-X IPS SSP
 - ASA 5525-X IPS SSP
 - ASA 5545-X IPS SSP
 - ASA 5555-X IPS SSP

- ASA 5585-X IPS SSP-10
- ASA 5585-X IPS SSP-20
- ASA 5585-X IPS SSP-40
- ASA 5585-X IPS SSP-60

System Restrictions

The following system restrictions apply to the platforms and IPS software versions supported by IDM 7.1.5:

- The ASA 5585-X IPS SSP is supported in IPS 7.1(1)E4 and later.
- The IPS 4345 and the IPS 4360 are supported in IPS 7.1(3)E4 and later.
- The ASA 5500-X IPS SSP is supported in IPS 7.1(3)E4 and later.
- The IPS 4270-20 is supported in IPS 6.2(x), 7.0(x), and IPS 7.1(3)E4 and later.
- The ASA 5500 AIP SSC-5 is only supported in IPS 6.2(x).



Note The ASA 5500 AIP SSC-5 does not support creating custom signatures, adding signatures, or cloning signatures. You can tune (edit) existing signatures.

- The IPS 4240, IPS 4255, IPS 4260 appliances are supported in 6.2(x), IPS 7.0(x), and IPS 7.1(5)E4 and later.
- The AIM IPS and NME IPS are supported in 6.2(x) and IPS 7.0(x).
- The ASA 5500 AIP SSM is supported in 6.2(x), IPS 7.0(x), and IPS 7.1(5)E4 and later.
- The IDSM2 is supported in 6.2(x) and IPS 7.0(x).
- Anomaly detection is disabled by default beginning in IPS 7.1(2)E4.
- AAA RADIUS is only supported in IPS 7.0(4)E4 and later and IPS 7.1(3)E4 and later.
- Global correlation is supported in IPS 7.0 and later.
- The the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP do not support bypass mode.

New and Changed Information

IDM 7.1.5 has the following new features:

- Support for IPS 7.1(5)E4.

IDM 7.1.5 is included in IPS 7.1(5)E4

- Signature threat profiles—In the IDM Startup Wizard, you can apply a signature template to individual signature policies, which adjusts the signature coverage and response actions enabling the sensor to make better choices in various deployment and threat scenarios.



Note Signature threat profiles are supported on the IPS 4345, IPS 4360, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP.

- Inspection load statistics—Displays the inspection load history across varying time periods.
- HTTP advanced decoding— Enables deeper inspection of HTTP traffic.



Note HTTP advanced decoding is supported on the IPS 4345, IPS 4360, ASA 5585-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, and ASA 5555-X IPS SSP.



Note Enabling HTTP advanced decoding severely impacts system performance.

- The default value of the Cisco server IP address has been changed from 198.133.219.25 to 72.163.4.161 in the Auto Update URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new IP address.

For More Information

- For a list of the IPS 7.1(5)E4 features, refer to [New and Changed Information](#).
- For more information about signature threat profiles, refer to [Applying Signature Threat Profiles](#).
- For more information about inspection load statistics, refer to [Displaying Inspection Load Statistics](#).
- For more information about HTTP advanced decoding, refer to [Adding, Editing, and Deleting Virtual Sensors](#).
- For more information about automatic update, refer to [Configuring Automatic Update](#).

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 7.1.5:

- 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.
- 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](#).

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

- *Documentation Roadmap for Cisco Intrusion Prevention System*
- *Cisco Intrusion Prevention System Device Manager Configuration Guide*
- *Cisco Intrusion Prevention System Manager Express Configuration Guide*
- *Cisco Intrusion Prevention System Command Reference*
- *Cisco Intrusion Prevention System Sensor CLI Configuration Guide*
- *Cisco Intrusion Prevention System Appliance and Module Installation Guide*
- *Installling and Removing Interface Cards in Cisco IPS-4260 and IPS 4270-20*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500-X Series Appliances and the Cisco Intrusion Prevention System 4300 Series Appliances*

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Copyright © 2012-2013 Cisco Systems, Inc. All rights reserved.