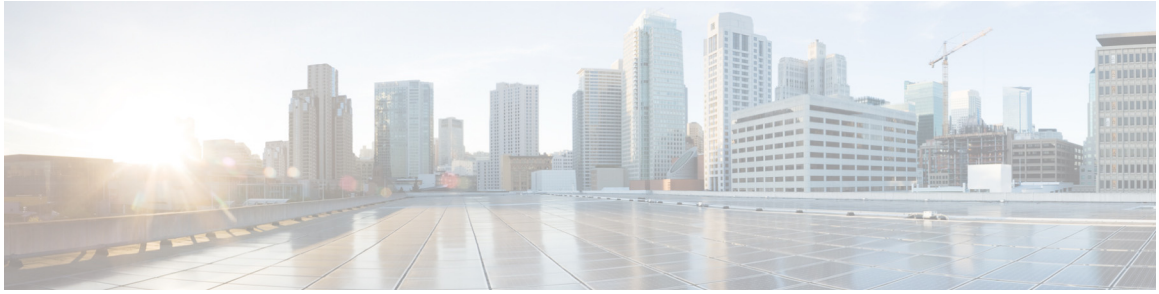

Release Notes for Cisco Intrusion Prevention System Manager Express 7.2.5

Published: January 15, 2014, OL-30817-01

Contents

IME File List

The following files are part of Cisco IME 7.2.5:

- IME-7.2.5.exe
- IME-7.2.5.readme.txt

Cisco Systems, Inc.
www.cisco.com

System Requirements

The IME has the following system requirements:

- Supported IPS versions
  - IPS 5.1
  - IPS 6.0
  - IPS 6.1
  - IPS 6.2
  - IPS 7.0
  - IPS 7.1
  - IPS 7.2
  - IPS 7.3
- Minimum hardware requirements
  - Pentium, AMD Athlon, or equivalent processor running at 2 GHz (minimum)
  - Color monitor with at least 1024 x768 resolution and a video card capable of 16-bit colors
  - 100-GB hard-disk drive
  - 2-GB RAM
- Supported TCP/UDP ports
  - 47002
  - 47003
  - 47006
  - 47007
  - 47008
  - 47009
  - 47010
- Supported Operating Systems
  - Windows Vista Business and Ultimate (32-bit only)
  - Windows XP Professional (32-bit only)
  - Windows Server 2003R2
  - Windows 7 (32- and 64-bit)
  - Windows Server 2008 (32- and 64-bit)
  - Windows Server 2008R2
  - Windows Server 2012
  - VMWare
- Supported Cisco IPS hardware platforms
  - IPS 4240
  - IPS 4255
  - IPS 4260

- IPS 4270-20
- IPS 4345
- IPS 4345-DC
- IPS 4360
- IDSM2
- AIM IPS
- NME IPS
- 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

Note Although the IME also supports the IDS 4210, IDS 4215, IDS 4235, IDS 4250, and NM CIDS, these platforms do support any IPS software past IPS 6.1, and some of the IME features are not supported.

System Restrictions

The following system restrictions apply to the platforms and IPS software versions supported by IME 7.2.5:

- The ASA 5585-X IPS SSP is supported in IPS 7.1(*x*) and IPS 7.2(1)E4.
- The IPS 4345 and IPS 4360 are supported in IPS 7.1(2)E4 and later, IPS 7.2(1)E4 and later, and IPS 7.3(1)E4 and later.
- The ASA 5500-X IPS SSP series are supported in IPS 7.1(2)E4 and later, and IPS 7.2(1)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 IPS 4510 and IPS 4520 are supported in IPS 7.1(4)E4 and later., IPS 7.2(1)E4 and later, and IPS 7.3(1)E4 and later.
- The ASA 5500 AIP SSC-5 is only supported in IPS 6.2(*x*).

- 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 IPS 6.2(*x*), IPS 7.0(x), and IPS 7.1(5)E4 and later.
- The AIM IPS and NME IPS are supported in IPS 6.2(*x*) and IPS 7.0(*x*).
- The ASA 5500 AIP SSM is supported in IPS 6.2(*x*), IPS 7.0(*x*), and IPS 7.1(5)E4 and later.
- The IDSM2 is supported in IPS 6.2(*x*) and IPS 7.0(*x*).
- Anomaly detection is disabled by default beginning in IPS 7.1(2)E4.
- AAA RADIUS is supported in IPS 7.0(4)E4 and later, IPS 7.1(3)E4 and later, IPS 7.2(*x*), and IPS 7.3(*x*)
- Global correlation is supported in IPS 7.0 and later.
- The ASA 5500 AIP SSM, ASA 5500-X IPS SSP and ASA 5585-X IPS SSP do not support bypass mode.
- On the IPS 4510 and IPS 4520, no interface-related configurations are allowed when the SensorApp is down.

New and Changed Information

IME 7.2.5 has the following new features:

- Support for 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 IME 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 > *sensor_name* > Signature Configuration > Add Policy/Clone Policy

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

    You can manage signature instances and threat profiles here.

  - Configuration > *sensor_name* > 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 > *sensor_name* > Policies > Signature Definitions > sig0 > All Signatures > Threat Profile

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

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

    You can identify the threat profile and can create 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 > *sensor_name* > LACP > LACP Neighbor

    You can view the LACP neighbors with the system details.
  - Sensor Monitoring > *sensor_name* > 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
- For detailed information on configuring LACP on the 4500 series sensors, refer to

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.

Installing or Upgrading Cisco IME and Migrating Data Into IME

Note Beginning with IME 7.0.3, you are required to create a password to access the IME.

Cisco IEV, Cisco IOS IPS, and CSM

If you have a version of Cisco IPS Event Viewer installed, the Install wizard prompts you to remove it before installing the IME.

The IME event monitoring is also supported in IOS-IPS versions that support the Cisco IPS 5.x/6.x signature format. We recommend IOS-IPS 12.4(15)T4 if you intend to use the IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.

Caution Do not install the IME on top of existing installations of CSM. You must uninstall CSM before installing the IME.

Installation Notes and Caveats

Note If you are using Windows 7 or Windows Server 2008, uninstall any earlier version of the IME before upgrading it. Otherwise, just upgrade from your current IME version.

Observe the following when installing or upgrading the IME:

- You can install the IME over all versions of the IME but not over IEV. All alert database and user settings are preserved.
- The IME detects previous versions of IEV and prompts you to manually remove the older version before installing the IME or to install the IME on another system. The installation program then stops.
- Make sure you close any open instances of the IME before upgrading to a new version of the IME.
- Disable any anti-virus or host-based intrusion detection software before beginning the installation, and close any open applications. The installer spawns a command shell application that may trigger your host-based detection software, which causes the installation to fail.

- You must be administrator to install the IME.
- The IME coexists with other instances of the MySQL database. If you have a MySQL database installed on your system, you do NOT have to uninstall it before installing the IME.

Installing or Upgrading the IME

To install the IME, follow these steps:

Step 1 From the Download Software site on Cisco.com, download the IME executable file to your computer, or start the IDM in a browser window, and under Cisco IPS Manager Express, click **download** to install the IME executable file. IME-7.2.5.exe is an example of what the IME executable file might look like.

Step 2 Double-click the executable file. The Cisco IPS Manager Express - InstallShield Wizard appears. You receive a warning if you have a previous version of Cisco IPS Event Viewer installed. Acknowledge the warning, and exit installation. Remove the older version of IEV, and then continue the IME installation.

Step 3 Click **Next** to start the IME installation.

Step 4 Accept the license agreement and click **Next**.

Step 5 Click **Next** to choose the destination folder, click **Install** to install the IME, and then click **Finish** to exit the wizard. The Cisco IME and Cisco IME Demo icons are now on your desktop.

Note The first time you start the IME, you are prompted to set up a password.

Migrating IEV Data

To migrate IEV 5.*x* events to the IME, you must exit the installation and manually export the old events by using the IEV 5.*x* export function to move the data to local files. After installing the IME, you can import these files to the new IME system.

Note The IME does not support import and migration functions for IEV 4.*x*.

To export event data from IEV 5.*x* to a local file:

Step 1 From IEV 5.*x*, choose **File > Database Administration > Export Database Tables**.

Step 2 Enter the file name and select the table(s).

Step 3 Click **OK**. The events in the selected table(s) are exported to the specified local file.

Importing IEV Event Data In to IME

To import event data in to the IME, follow these steps:

Step 1 From the IME, choose **File > Import**.

Step 2 Select the file exported from IEV 5.*x* and click **Open**. The contents of the selected file are imported in to the IME.

Importing IEV Event Data In to IME

To import event data in to IME, follow these steps:

Step 1 From IME, choose **File > Import**.

Step 2 Select the file exported from IEV 5.*x* and click **Open**.

The contents of the selected file are imported in to IME.

For More Information

- For the procedure for creating and changing the IME password, see Creating and Changing the IME Password, page 9.
- For instructions on how to obtain Cisco IPS software, see Obtaining Software on Cisco.com, page 6.
- For more information about Cisco IME, refer to *Cisco Intrusion Prevention System Manager Express Configuration Guide for IPS 7.3*.

Creating and Changing the IME Password

Note Beginning with IME 7.0.3, you are required to create a password to access the IME.

When you start the IME for the first time, the Password Policy dialog box appears. Enter a password that you will use to access the IME. Reenter the password to confirm, and then click **OK**. From now on when you log in to the IME, enter your password in the Enter IME password field and click **OK**. To change the IME password, choose **Tools > Change User Password**, and enter your existing password, your new password, and then reenter the new password to confirm. When you uninstall and reinstall the IME, you must create a new user password. You do not have to restart the IME after a password change.

Note The IME does not support user roles or multiple sessions, so you do not need to configure a user name.

Password Requirements

The IME password has the following requirements:

- Must contain at least 8 characters and no more than 80.
- Must contain characters from at least three of the following classes:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters (! @ $ % & *)
- No single character repeated more than two times consecutively.
- All input must be ASCII characters.

Note The IME performs other checks to make sure that the password is secure. You receive an error message if the password does not pass validation.

Recovering the IME Password

To recover the IME password, follow these steps:

Step 1 Stop the IME client.

Step 2 Delete the hosts.cfg file from the installed directory.

Example

```
C:\Documents and Settings\All Users\Application Data\Cisco Systems\IME\iev\hosts.cfg
```

Note This example location may be different depending on which Windows version you have.

Step 3 Restart the IME client.

Step 4 You are prompted to create a new password.

No events are lost from the database, including new events between the time you deleted hosts.cfg and restarted the IME. However, the event account user name and password will be used for both events and configuration. If you had different user names and passwords for the event and configuration roles, you must edit each device to restore them.

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

Restrictions and Limitations

The following restrictions and limitations apply to Cisco IME 7.2.5:

- You can use the IME to monitor sensors running Cisco IPS 5.0 and later; however, some of the new features and functionality in IME are only supported on sensors running IPS 6.1 or later.
- IME 7.2.5 does not support Cisco IPS 4.*x* or 3.*x* sensors.
- You can install IME 7.2.5 over all versions of the IME but not over IEV. All alert database and user settings are preserved.
- IME 7.2.5 detects previous versions of IEV and prompts you to manually remove the older version before installing IME 7.2.5 or to install the IME on another system. The installation program then stops.
- Make sure you close any open instances of the IME before upgrading to IME 7.2.5.

  Note If you are using Windows 7 or Windows Server 2008, uninstall any earlier version of the IME before upgrading. Otherwise, just upgrade from your current IME version.

- Disable any anti-virus or host-based intrusion detection software before beginning the installation, and close any open applications. The installer spawns a command shell application that may trigger your host-based detection software, which causes the installation to fail.
- You must be administrator to install the IME.
- IME 7.2.5 coexists with other instances of the MySQL database. If you have a MySQL database installed on your system, you do NOT have to uninstall it before installing IME 7.2.5.
- 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 IME launches 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 More Information

For more information about MySDN, refer to MySDN.

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.