Release Notes for Cisco Intrusion Prevention System Manager Express 7.1.1

Published: February 14, 2011, OL-24340-01

Revised: October 28. 2013

Contents

- IME File List, page 2
- System Requirements, page 2
- Installation Error, page 4
- New and Changed Information, page 4
- MySDN Decommissioned, page 5
- Obtaining Software on Cisco.com, page 5
- Installing or Upgrading Cisco IME and Migrating Data Into IME, page 6
- Creating and Changing the IME Password, page 8
- Recovering the IME Password, page 9
- Cisco Security Intelligence Operations, page 9
- Restrictions and Limitations, page 10
- Caveats, page 10
- Related Documentation, page 11
- Obtaining Documentation, Using the Cisco Bug Search Tool, and Submitting a Service Request, page 12

Cisco Systems, Inc.
www.cisco.com

IME File List

The following files are part of Cisco IME 7.1.1:

- Cisco IME
  - IME-7.1.1.exe
- Readme
  - IME-7.1.1.readme.txt

System Requirements

IME has the following system requirements:

- Minimum hardware requirements
  - IBM PC-compatible 2-GHz or faster processor
  - 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
- Operating Systems
  - Windows Vista Business and Ultimate (32-bit only)
  - Windows XP Professional (32-bit only)
  - Windows Server 2003
  - Windows 7 (32- and 64-bit)
  - Windows Server 2008 (32- and 64-bit)

IME supports the following Cisco IPS hardware platforms:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- AIP-SSC-5
- AIP SSM-10
- AIP SSM-20
- AIP SSM-40
- IDSM2
- IPS SSP-10
- IPS SSP-20
- IPS SSP-40
- IPS SSP-60
- NME IPS

Note Although IME also supports 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.

IME supports the following Cisco IPS versions with the following features:

Note The Cisco ASA 5585 with IPS SSP is currently the only platform that supports Cisco IPS 7.1(1)E4. No other Cisco IPS sensors currently support IPS 7.1(1)E4.

- Cisco IPS 7.0
  - IPv6
  - Sensor Configuration
  - Sensor Health Dashboard
  - Events Dashboard
  - Event Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 6.2
  - IPv6
  - Sensor Configuration
  - Sensor Health Dashboard
  - Events Dashboard
  - Event Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 6.1
  - Sensor Configuration
  - Sensor Health Dashboard
  - Events Dashboard
  - Event Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 6.0
  - Events Dashboard
  - Events Monitoring

  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 5.1
  - Events Dashboard
  - Events Monitoring
  - Reporting
  - Up to 10devices
  - Up to 100 EPS
- Cisco IOS IPS 12.3(14)T7 and 12.4(15)T2
  - Events Dashboard
  - Events Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS

Installation Error

Symptom IME 7.1.1 installation is failing with the following error message: `Unhandled Exception. Error Number: 0x80004005, Description: Unspecified Error. Setup will now terminate.`

Conditions You are trying to install the IME over an RDP connection, which has 8-bit color depth or 256 colors. This is an InstallShield error.

Workaround Increase the color depth of the RDP connection to at least 16 bits.

New and Changed Information

IME 7.1.1 has the following new features:

- Support for Windows 7
- Support for Windows Server 2008
- Support for the Cisco IPS SSP
- Support for IPS 7.1(1)E4
- Support for IPS 7.0(4)E4 (AAA support)

MySDN Decommissioned

Because MySDN has been decommissioned, the URL in older versions of IDM and IME is no longer functional. If you are using IPS 6.0 or later, we recommend that you upgrade your version of IDM and IME.

You can upgrade to the following versions to get the functioning MySDN URL:

- IME 7.0.3
- IPS 7.0(4), which contains IDM 7.0(4)E4

If you are using version IPS 5.x, you must look up signature information manually at this URL:

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

For More Information

For more information about MySDN, refer to MySDN.

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 as needed. Major and minor updates are also posted periodically. Check Cisco.com regularly for the most recent 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. You can sign up for IPS Alert Bulletins to receive information on the latest software releases.

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.

Caution Do not change the filename. You must preserve the original filename for the sensor to accept the update.

Downloading 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 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.

- Fill out the form and click **Submit**.

  The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.
- 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.

The File Download dialog box appears.

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

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

Installing or Upgrading Cisco IME and Migrating Data Into IME

Cisco IEV, Cisco IOS IPS

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

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 IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.

Installation Notes and Caveats

Note If you are using Windows 7 or Windows Server 2008, uninstall any earlier version of IME before upgrading to IME 7.1.1. Otherwise, just upgrade from your current IME version to IME 7.1.1.

Observe the following when installing or upgrading IME:

- You can install IME over all versions of IME but not over IEV. All alert database and user settings are preserved.
- IME detects previous versions of IEV and prompts you to manually remove the older version before installing IME or to install IME on another system. The installation program then stops.
- Make sure you close any open instances of IME before upgrading to a new version of 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 IME.
- 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 IME.

Installing or Upgrading IME

To install IME, follow these steps:

Step 1 From the Download Software site on Cisco.com, download the IME executable file to your computer, or start IDM in a browser window, and under Cisco IPS Manager Express, click **download** to install the IME executable file.

IME-7.0.47.1.1.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 IME installation.

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

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

Step 5 Click **Next** to choose the destination folder, click **Install** to install 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 IME, you are prompted to set up a password.

Migrating IEV Data

To migrate IEV 5.*x* events to 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 IME, you can import these files to the new IME system.

Note 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 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 more information about Cisco IME, refer to *Installing and Using Cisco Intrusion Prevention System Manager Express 7.1*.

Creating and Changing the IME Password

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

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

Note 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 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
```

Step 3 Restart the IME client.

Step 4 You are prompted to create a password.

No events are lost from the database, including new events between the time you deleted hosts.cfg and restarted 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 7.1.1:

- You can use 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 7.1.1 does not support Cisco IPS 4.*x* or 3.*x* sensors.
- You can install IME 7.1.1 over all versions of IME but not over IEV. All alert database and user settings are preserved.
- IME 7.1.1 detects previous versions of IEV and prompts you to manually remove the older version before installing IME 7.1.1 or to install IME on another system. The installation program then stops.
- Make sure you close any open instances of IME before upgrading to IME 7.1.1.

  Note If you are using Windows 7 or Windows Server 2008, uninstall any earlier version of IME before upgrading to IME 7.1.1. Otherwise, just upgrade from your current IME version to IME 7.1.1.

- 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 IME.
- IME 7.1.1 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 7.1.1.
- 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.
- 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.

Caveats

This section lists the resolved and known caveats, and contains the following topics:

- Resolved Caveats, page 11
- Caveats, page 11

Resolved Caveats

The following known issues have been resolved in the IME 7.1.1 release:

- CSCtf20393—IME display issue with 1024 x 768 screen size
- CSCsu78195—Importing event data results in table full
- CSCsu79782—IME: Unable to delete custom reports
- CSCtd11879—IME Trigger Packet and Context data should be content sensitive
- CSCti28617—IME -- Set default time zone
- CSCtg50407—Unexpected java exception when generate IME Reports
- CSCtb52871— config changes cannot be applied after navigating to event monitoring
- CSCtb39380—IME: Reports for Top items do not return more than 10 Top Items
- CSCti79083— java.io.FileNotFoundException when generate IME reports

Caveats

The following known issues are found in Cisco IME 7.1.1:

- CSCtg50439—Events not retrieved when source address is the victim
- CSCtg63072—Deleted IME customer reports show back after exit/restart IME client
- CSCtg53580— Misspell Exporting as Expoting on Export Alarm Data
- CSCtb88463—Video Help needs updating for 10 device, and new features
- CSCtg14777—IME Installation wizard should warn user if IME client is running
- CSCtj76756—Data archive doesn't work on schedule with Every day at time
- CSCtj42021— IME: “Sensor Certificate Expired” Error Message Needed
- CSCtn18188— IME client killed by fatal error detected by Java Runtime Environment
- CSCtl02274—IME panels freeze after Send a Test Mail if SMTP mail server not setup
- CSCtk66479—IME event viewer not updated with current
- CSCti45547 —Mon Stop Attacker should not populate ipv6 if using Block on another

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*
- *Installing and Using Cisco Intrusion Prevention System Device Manager*
- *Installing and Using Cisco Intrusion Prevention System Manager Express*
- *Cisco Intrusion Prevention System Command Reference*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
- *Installing Cisco Intrusion Prevention System Appliances and Modules*

- *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*

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.