Release Notes for Cisco Intrusion Prevention System 7.1(1)E4

Published: March 31, 2011, OL-19894-01

Revised: October 28, 2013

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

Note The Cisco ASA 5585-X with the ASA 5585-X IPS SSP is supported in ASA 8.2(4.4) and higher as well as ASA 8.4(2) and higher. It is not supported in ASA 8.3(*x*).

Contents

Cisco Systems, Inc.
www.cisco.com

IPS File List

The following files are part of Cisco IPS 7.1(1)E4:

- Readme
  - IPS-7-1-1-E4.readme.txt
- System Image Files
  - IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_20-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_40-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_60-K9-sys-1.1-a-7.1-1-E4.img
- Recovery Image Files
  - IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_20-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_40-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_60-K9-r-1.1-a-7.1-1-E4.pkg

Supported Platforms

Cisco IPS 7.1(1)E4 is supported on the following platforms:

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

ROMMON and TFTP

ROMMON uses TFTP to download an image and launch it. TFTP does not address network issues such as latency or error recovery. It does implement a limited packet integrity check so that packets arriving in sequence with the correct integrity value have an extremely low probability of error. But TFTP does not offer pipelining so the total transfer time is equal to the number of packets to be transferred times the network average RTT. Because of this limitation, we recommend that the TFTP server be located on the same LAN segment as the sensor. Any network with an RTT less than a 100 milliseconds should provide reliable delivery of the image. Be aware that some TFTP servers limit the maximum file size that can be transferred to ~32 MB.

IPS Management and Event Viewers

Note IDM version 7.1.1 is included within IME 7.1.1. You can use IME 7.1.1 to configure IPS 6.1, 6.2, 7.0, and 7.1 sensors.

Use the following tools for configuring Cisco IPS 7.1(1)E4 sensors:

- Cisco IDM 7.1.1

  IDM 7.1.1 is included within the IPS 7.1(1)E4 files.

  IDM 7.1.1 is included within IME 7.1.1.

  IDM 7.1.1 requires JRE 1.6 or later.
- Cisco IME 7.1.1
- IPS CLI included in IPS 7.1(1)E4
- Cisco ASDM 6.3.4

Use the following tools for monitoring Cisco IPS 7.1(1)E4 sensors:

- IDM 7.1.1
- IME 7.1.1
- MARS minimum version 5.2 and latest version 6.0.5
- CSM 4.0 and later

  Note You may need to configure viewers that are already configured to monitor the earlier version sensors to accept a new SSL certificate for the Cisco IPS7.1(1)E4 sensors.

New and Changed Information

Cisco IPS 7.1(1)E4 contains the following new and changed information:

- Support for the ASA 5585-X with IPS SSP-10, IPS SSP-20, IPS SSP-40, or IPS SSP-60.
- String ICMP XL, String TCP XL, and String UDP XL engines that provide optimized operation for the ASA 5585-X with IPS SSP-10, IPS SSP-20, IPS SSP-40, or IPS SSP-60.
- Bypass mode not supported.

  The ASA 5585-X IPS SSP does not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the ASA 5585-X IPS SSP.
- Contains the S552 signature update.

For More Information

- For detailed information about the ASA 5585-X and how to install it, refer to *Cisco ASA 5585-X Adaptive Security Appliance Hardware Installation Guide*.
- For detailed information about the IPS SSP-10, IPS SSP-20, IPS SSP-40, or IPS SSP-60, refer to *Cisco Intrusion Prevention System Security Services Processor Installation Guide for IPS 7.1*.
- For detailed information about the String XL engines, refer to String XL Engines.

The IDM and JRE 1.7

In IPS versions 7.1(1)E4 through 7.1(5)E4, the IDM fails to connect to the sensor due to a failure during the initial handshake, because the web server is not RFC 5746-compliant. Try the following workaround.

Problem Cannot launch the IDM, when the IDM is running under JRE 1.7 with IPS 7.1(1)E4 through 7.1(5)E4.

Solution Use JRE 1.6 or enable the SSL 2.0-compatible ClientHello format in the Java settings under Control Panel.

Starting the IDM

Note After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.

There are two ways to start the IDM:

- Cross launch from the IME (recommended)

  Open the IME and click **Configuration**. All the 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://10.1.9.201:1040).

Step 2 Click **Yes** to accept the security certificate. The Cisco IPS Device Manager Version 7.1 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**. 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 Both the default username and password are **cisco**. You were prompted to change the password during sensor initialization.

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 7.1 window. After you launch the IDM, it is not necessary for this window to remain open.

Installing or Upgrading Cisco IME

This section describes how to install and upgrade the IME, and contains the following topics:

- Before Installing or Upgrading the IME, page 6
- Cisco IME Installation and Upgrade Instructions, page 6

Before Installing or Upgrading the IME

Caution The IME does not automatically uninstall IEV.

IME 7.1.1 detects previous versions of IEV and prompts you to manually remove the older version before installing IME 7.1 or to install the IME on another system. The installation program then stops. 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.

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 IME 7.1.1, you can import these files to the new IME system.

Note IME 7.1.1 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 the 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.

Cisco IME Installation and Upgrade Instructions

If you have a version of Cisco IPS Event Viewer installed, the Install wizard prompts you to remove it before installing the 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 the IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.

IME Installation and Upgrade Caveats

- Make sure you close any open instances of IME 7.0.1 before upgrading 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 the IME.
- Do not install the IME on top of existing installations of CSM. You must uninstall CSM before installing the IME.

Installing or Upgrading to IME 7.1.1

You can install IME 7.1.1 over IME 7.0.1. All alert database and user settings are preserved.

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_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.

Step 3 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 4 Double-click the executable file. The Cisco IPS Manager Express - InstallShield Wizard appears.

Step 5 Click **Next** to start IME installation.

Step 6 Accept the license agreement and click **Next**.

Step 7 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.

For More Information

For more information about Cisco IME, refer to *Cisco Intrusion Prevention System Manager Express Configuration Guide for IPS 7.1*.

Licensing the Sensor

You can install the license key through the CLI, the IDM, or the IME. This section describes how to obtain and install the license key, and contains the following topics:

- Using the IDM or the IME, page 7
- Using the CLI, page 8

Using the IDM or the IME

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

To obtain and install the license key, follow these steps:

Step 1 Log in to the IDM or the IME using an account with administrator privileges.

Step 2 For the IDM choose **Configuration > Sensor Management > Licensing**. For the IME choose **Configuration >** ***sensor_name*** **> Sensor Management > Licensing**. The Licensing pane displays the status of the current license. If you have already installed your license, you can click **Download** to save it if needed.

Step 3 Obtain a license key by doing one of the following:

- Click the **Cisco.com** radio button to obtain the license from Cisco.com. The IDM or the IME contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 4.
- Click the **License File** radio button to use a license file. To use this option, you must apply for a license key at this URL: www.cisco.com/go/license. The license key is sent to you in e-mail and you save it to a drive that the IDM or the IME can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.

Step 4 Click **Update License**, and in the Licensing dialog box, click **Yes** to continue.

The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.

Step 5 Click **OK**.

Step 6 Go to www.cisco.com/go/license.

Step 7 Fill in the required fields. Your license key will be sent to the e-mail address you specified.

Caution You must have the correct IPS device serial number because the license key only functions on the device with that number.

Step 8 Save the license key to a hard-disk drive or a network drive that the client running the IDM or the IME can access.

Step 9 Log in to the IDM or the IME.

Step 10 For the IDM choose **Configuration > Sensor Management > Licensing**. For the IME choose **Configuration >** ***sensor_name*** **> Sensor Management > Licensing**.

Step 11 Under Update License, click the **License File** radio button.

Step 12 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 13 Browse to the license file and click **Open**.

Step 14 Click **Update License**.

Using the CLI

Note You cannot install an older license key over a newer license key.

Use the **copy** *source-url license_file_name* **license-key** command to copy the license key to your sensor.

The following options apply:

- *source-url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination-url*—The location of the destination file to be copied. It can be a URL or a keyword.
- **license-key**—The subscription license file.
- *license_file_name*—The name of the license file you receive.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- ftp:—Source URL for an FTP network server. The syntax for this prefix is:

  ftp://[[username@]location][/relativeDirectory]/filename

  ftp://[[username@]location][//absoluteDirectory]/filename

  Note You are prompted for a password.

- scp:—Source URL for the SCP network server. The syntax for this prefix is:

  scp://[[username@]location][/relativeDirectory]/filename

  scp://[[username@]location][//absoluteDirectory]/filename

  Note You are prompted for a password. You must add the remote host to the SSH known hosts list.

- http:—Source URL for the web server. The syntax for this prefix is:

  http://[[username@]location][/directory]/filename

  Note The directory specification should be an absolute path to the desired file.

- https:—Source URL for the web server. The syntax for this prefix is:

  https://[[username@]location][/directory]/filename

  Note The directory specification should be an absolute path to the desired file. The remote host must be a TLS trusted host.

Installing the License Key

To install the license key, follow these steps:

Step 1 Apply for the license key at this URL: www.cisco.com/go/license.

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

Step 2 Fill in the required fields. Your Cisco IPS Signature Subscription Service license key will be sent by e-mail to the e-mail address you specified.

Note You must have the correct IPS device serial number because the license key only functions on the device with that number.

Step 3 Save the license key to a system that has a Web server, FTP server, or SCP server.

Step 4 Log in to the CLI using an account with administrator privileges.

Step 5 Copy the license key to the sensor.

```
sensor# copy scp://user@10.89.147.3://tftpboot/dev.lic license-key
Password: *******
```

Step 6 Verify the sensor is licensed.

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABCDEFGHIJK
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

ips-ssp#
```

Traffic Flow Stopped with Fail-Open Policy on IPS Switchports

Problem Traffic on any port located on the ASA 5585-X IPS SSP (1/x) no longer passes through the adaptive security when the ASA 5585-X IPS SSP is reset or shut down. This affects all traffic through these ports regardless of whether or not the traffic would have been monitored by the IPS. The link on the ports will link down when the ASA 5585-X IPS SSP is reset or shut down.

Possible Cause Using the ports located on the ASA 5585-X IPS SSP (1/x), and resetting or shutting down the ASA 5585-X IPS SSP via any mechanism.

Solution Use the ports on the adaptive security appliance (0/x) instead because those ports do not lose their link when the ASA 5585-X IPS SSP is reset or shut down.

ASA IPS 5585-X and Jumbo Packet Frame Size

Refer to the following URL for information about the jumbo packet frame size for the ASA modules:

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/interface_start.html#wp1328869

Note A jumbo frame is an Ethernet packet that is larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS).

ASA IPS 5585-X and Jumbo Packets

The jumbo packet count in the **show interface** command output from the lines `Total Jumbo Packets Received` and `Total Jumbo Packets Transmitted` for ASA IPS modules may be larger than expected due to some packets that were almost jumbo size on the wire being counted as jumbo size by the IPS. This miscount is a result of header bytes added to the packet by the ASA before the packet is transmitted to the IPS. For IPv4, 58 bytes of header data are added. For IPv6, 78 bytes of header data are added. The ASA removes the added IPS header before the packet leaves the ASA.

Importing a New SSL Certificate

Import the new SSL certificate for the new sensor to each tool being used to monitor the new sensor.

For More Information

For the procedures for configuring TLS/SSL, for the CLI refer to Configuring TLS, for the IDM refer to Configuring Trusted Hosts, and for the IME refer to Configuring Trusted Hosts.

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 IPS 7.1(1)E4 software and the products that run it:

- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- Bypass mode is not supported.
- CDP mode is not supported.
- Alternate TCP resets are not supported.
- The ASA 5585-X IPS SSP is supported in ASA 8.2(4.4) and higher as well as ASA 8.4(2) and higher. It is not supported in ASA 8.3(*x*).
- Anomaly detection does not support IPv6 traffic; only IPv4 traffic is directed to the anomaly detection processor.
- IPv6 does not support the following event actions: Request Block Host, Request Block Connection, or Request Rate Limit.
- Global correlation does not support IPv6.
- ICMP signature engines do not support ICMPv6, they are IPv4-specific, for example, the Traffic ICMP signature engine. ICMPv6 is covered by the Atomic IP Advanced signature engine.
- The ASA 5585-X IPS SSP can support both promiscuous and inline monitoring at the same time on its single physical back plane interface inside the adaptive security appliance. The configuration on the main adaptive security appliance can be used to designate which packets/connections should be monitored by the ASA 5585-X IPS SSP as either promiscuous or inline.
- 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 the IDM, they are turned into something unrecognizable and you will not be able to delete or edit the resulting object through the IDM or the CLI.

  This is true for any string that is used by CLI as an identifier, for example, names of time periods, inspect maps, server and URL lists, and interfaces.

- When SensorApp is reconfigured, there is a short period when SensorApp cannot respond to any queries. Wait a few minutes after reconfiguration is complete before querying SensorApp for additional information.
- 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 and the IME launch 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.

Caveats

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

Resolved Caveats

The following issues have been resolved in IPS 7.1(1)E4 release:

- CSCsg09619—IPS accepts RSA keys with exponent 3 which are vulnerable to forgery
- CSCsj82458—global-block-timeout allows values outside supported range
- CSCsq18457—Unauthenticated Ntp settings lost after recover application-partition
- CSCsq53214—IPS reports different sig version in CT and CLI
- CSCsw86555—5582 false positve
- CSCsx20458—Sig 1300.0 firing incorrectly
- CSCtc18038—SensorApp mismanages buffers when TX queue full
- CSCtc43996—Engine P2P may not properly check boundaries
- CSCtc61972—Ares P2P signature does not fire
- CSCtd91982—Crash mainAPP aborted parsing CT name and idapi parameters
- CSCte55319—Sensor returns ERROR for custom IOS LWE signatures on appliances
- CSCtf04150—Promiscuous mode stream normalizer incorrect handling of TO_WEB traffic
- CSCtf04660—IPS: crash in Anomaly Detection getLearnedKnowledgeBase
- CSCtf09280—Unable to delete custom sigs created for IOS Lightweight engines
- CSCtf40209—Signature Obsoletes from "backport" engines are being processed
- CSCsv26568—IPS SNMP InterfaceGroup OID does not show correct Virtual Sensor
- CSCsz19556—7280.0 does not reliably alert
- CSCta96144—sensorApp terminates with core in updateTime (version 7.x)

- CSCtb58224—No mgmt communications after clearing and reconfiguring host config
- CSCtc25895—sensorApp processing (memory) failure under extreme traffic loads
- CSCtc89228—F1 Control Plane error message on SSM
- CSCtd67026—SSL/TLS Vulnerable to a Memory Exhaustion DOS Attack
- CSCtd70757—mainApp terminates in Cid:Log:Drain:appName
- CSCte69138—Simultaneous DNS lookups corrupt collaborationApp
- CSCtg17572—SMB-Advanced engine: some signatures do not fire correctly
- CSCtg83277—improper API usage of IpAddrNode class results in bad vsID callbacks

The following issues have been resolved in IDM 7.1.1:

- CSCsx42999—IDM/Unable to sort Signature by "Action"
- CSCta12522—IDM does not support multiple OS types in configured-os-map list
- CSCso15239—Create a user from IDM with password less than 8 characters
- CSCta56059—IDM doesn't load the auto update password for Cisco.com
- CSCsw91474—IDM Reports inspection load erratically

Caveats

The following known issues are present in the IPS 7.1(1)E4 release:

- CSCtf76151—Regex compile error when using min-match-length with string-xl-tcp
- CSCtg35970—sensorApp not responding to CTs while applying GC updates
- CSCth09619—CLI setup fails if the default-vlan is set to 0
- CSCth25492—Anomaly Detection incorrectly reports received packet count as zero
- CSCth32595 —Signature definition cannot be defaulted after editing some signature
- CSCth36360— Certain fields in IDM for string-xl signatures cannot be set to no
- CSCth76744—No GC warning generated for unlicensed IPS
- CSCti11562—High number of RGX_QUEUE_IS_FULL error messages due to overload
- CSCti23399—Statistics for os-identifications reporting missing os identifications
- CSCti30963—Updating summertime info with improbable values render IPS inoperable
- CSCti34102—Logging fails if cli login attempted before mainApp starts
- CSCti34230—Error regarding no matching interface descriptors
- CSCti38851—Total interface bytes/packets sometimes unexpectedly huge
- CSCti55219—Dataplane goes down temporarily during stress test
- CSCti69203—No alarming on IPv6 traffic in promiscuous mode
- CSCtj07289—Analysis Engine is stuck at "Busy Processing Stage 39"
- CSCtj09754—Sensor requires reboot to recover from LSI Out of Mem on Config issue.
- CSCtj19451—Reputation Filtering incorrectly triggering drops on IPv6 addresses
- CSCtj21083—Some of the CLI sessions are not able to be terminated.
- CSCtj25752—AD packet counters in virtual sensor stats are incrementing unexpectedly

- CSCtj36640—Compile error when un-retiring certain string-xl signatures
- CSCtj59684—ARC leaves many defunct ssh processes without properly terminating
- CSCtj76025—ARC hangs at connecting state when ssh hostkey not configured
- CSCtj77957—SensorApp stops when rapidly adding and deleting virtual sensors
- CSCtj85012—Continuously adding and removing virtual-sensors stops analysis-engine
- CSCtj96139—SensorApp killed by OOM Killer when large number of CLIs Opened
- CSCtj96473—Quick ramp to max concurrent connections causes sensorApp to stop
- CSCtk05905—L3 checksum incorrectly set and reported for IPv6 packets
- CSCtk06541—IPv6 packets being denied incorrectly due to signature 1250.0
- CSCtk16391—Stateful Jumbo TCP HTTP transactions failing on SSP60 at 200Mbps
- CSCtk28911—MPLS Unicast traffic passed through the IPS without being analyzed
- CSCtl09232—SensorApp stops with RGX_INVALID_HW_INSTR_ERR during signature tuning
- CSCtl77656—SensorApp stops after deleting last string-xl-icmp while it's firing
- CSCtn06217—Health status becomes red if the memory usage threshold is enabled
- CSCtn06270—Spyker received interface errors earlier than expected.
- CSCtn25153—TCP connection resets whenever signatures are being tuned
- CSCtn39822—Invalid Base64 encoded text causes CLI session to close
- CSCtn40134—Incorrect statistics displayed for Denied Address Information
- CSCtn59854—SensorApp stops when tracking unusually high number of streams
- CSCtn65840—SensorApp unresponsive due to GC update when out of memory

The following known issues are present in Cisco IDM 7.1.1:

- CSCsv02875—IDM problems after tuning sig to have atomic-ip-advanced engine
- CSCsy52817—IDM index.html has broken image file on IE 7
- CSCsy56695—Top Attackers Dashboard Cuts off long DNS host names
- CSCtf15537—Not able to select a value first time while adding a custom sig
- CSCti26170—IDM incorrect row selection after sig edit
- CSCth79394—Issues with Viewer role configuring aaa service on IDM
- CSCtb96907— SSC-5 default retired signature not grayed out in IDM

Related Documentation

For a complete list of Cisco IPS 7.1 documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/ips/7.1/roadmap/19889_01.html

For a complete list of the Cisco ASA 5500 series documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.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.