# Release Notes for Cisco AsyncOS 8.0.8 for Web

This document is cumulative for all releases of AsyncOS 8.0.x for Cisco Web Security appliances.

**Published: January 27, 2014**

**Revised: October 30, 2015**

## Contents



## New Features in This Release

# New Features in Release 8.0.8 (GD)

Primary changes in this release are related to disabling and enabling SSLv3 and elliptic-curve Diffie-Hellman ephemeral (ECDHE) features.

**Note** Please use the Cisco AsyncOS for Web User Guide v8.0.6, in conjunction with this release.

| Feature | Description |
|---|---|
| SSL configuration | For enhanced security, you can enable and disable SSLv3 for several services. Services with SSLv3 disabled will use TLSv1.0.<br><br>You can enable and disable SSLv3 for Appliance Management Web User Interface, Proxy Services (includes HTTPS Proxy and Credential Encryption for Secure Client), Secure LDAP Services (includes Authentication, External Authentication, SaaS SSO, and Secure Mobility), as well as the Update Service.<br><br>Use the Web interface (System Administration > SSL Configuration), or the CLI (`sslconfig`). |
| ECDHE authentication | Additional ECDH ciphers are supported in successive releases; however, certain named curves provided with some of the additional ciphers cause the appliance to close a connection during secure LDAP authentication and HTTPS traffic decryption.<br><br>If you experience these issues, use the `sslconfig` command, `ECDHE` option, command to disable or enable ECDHE cipher use for either or both features. Here is a snippet of the CLI for this:<br><br>`Choose the operation you want to perform:`<br>`- SSLV3 - Enable or disable SSL v3.`<br>`- ECDHE - Enable or disable ECDHE Authentication.`<br>`[]> ECDHE`<br><br>`ECDHE cipher status is enabled in Proxy & enabled in LDAP`<br><br>`Please select an option to change ECDHE cipher status:`<br>`- 1 - Toggle ECDHE cipher status in Proxy`<br>`- 2 - Toggle ECDHE cipher status in LDAP`<br>`- 3 - Enable ECDHE cipher in both Proxy & LDAP`<br>`- 4 - Disable ECDHE cipher in both Proxy & LDAP`<br>`[]>` |

# New Features in Release 8.0.7

This is a maintenance release; no new features were added.

# New Features in Release 8.0.6

All new features in this release are related to the file reputation and file analysis features.

| Feature | Description |
|---|---|
| Verdict Updates Report Change | Clicking a SHA-256 link in the Verdict Updates report now displays in Web Tracking all available transactions that included that SHA-256. |
| Reputation Score Threshold Customization | You can override the reputation threshold for Advanced Malware Protection provided by the cloud with a custom value. |
| SSL Certificate Retrieval | AsyncOS gets the latest SSL certificates automatically. |
| Support for Port 443 | Port 443 is now supported for Advanced Malware Protection file reputation queries. |
| Proxy Support | The appliance can now communicate with the cloud reputation service via an upstream proxy. Configure this in the Advanced Malware Protection settings, Advanced section.<br>Note that a proxy is not currently supported for the connection with the File Analysis server. |
| Improved Logging for Advanced Malware Protection | AsyncOS logs file analysis failures in the AMP log. |

# New Features in Release 8.0.5

| Feature | Description |
|---|---|
| File Reputation Filtering and File Analysis | Advanced Malware Protection (AMP) is an additionally licensed feature available to all Cisco Web Security appliance customers. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis, and retrospective alerting. It takes advantage of the vast Cisco cloud security intelligence networks.<br>AMP augments the anti-malware detection and blocking capabilities already offered by Cisco Web Security appliances with enhanced file reputation capabilities, detailed file behavior reporting, continuous file analysis, and retrospective verdict alerting.<br>For requirements and other details, see the File Reputation Filtering and File Analysis chapter in the online help or user guide. |

# New Features in Release 8.0.0

| Feature | Description |
|---|---|
| **New Features** | |
| Cloud Web Security Connector | This release introduces a new configuration mode, which allows you to connect to and direct traffic to Cisco Cloud Web Security for policy enforcement and threat defense.<br><br>Cloud Web Security Connector mode is available through the Cisco Web Security Virtual Appliance as well as the physical Web Security appliance.<br><br>Documentation for the Cloud Connector is in Chapter 3 of the User Guide, "Connect the Appliance to a Cloud Web Security Tower." To put the Web Security appliance in Cloud Connector mode, begin with "Configuring the Cloud Connector."<br><br>**Note** Kerberos authentication and IPv6 addresses are not supported in Cloud Connector mode.<br><br>**Note** After upgrading to this release, if you plan to use the appliance in Cloud Connector mode, do not put the appliance into Standard mode using the System Setup Wizard. Put the appliance directly into Cloud Connector mode. |
| Kerberos Authentication | Kerberos is a "pass through" authentication protocol for Windows, Mac OS X, and other operating systems. Due to many operating systems today that no longer support NTLM or NTLM SSO, Kerberos has become a very popular authentication protocol. This feature supports Kerberos Version 5 (MS KRB5 and KRB5), and AD servers such as 2003, 2008, 2008R2, and 2012. We also support the following Internet browsers : IE, Chrome, Firefox and Safari.<br><br>**Note** Active Directory realms created prior to this release will not have the Kerberos scheme available. |

| Feature | Description |
|---|---|
| Cisco Web Security Virtual Appliance | Cisco offers the Cisco Web Security appliance as a virtual machine that you can host on your own network.<br><br>The virtual appliance requires a separate license for the virtual appliance purchased from Cisco and a Cisco UCS Server (Blade or Rack-Mounted) hardware platform running VMware ESXi version 4.x, 5.0, or 5.1.<br><br>The Cisco Security Virtual Appliance Installation Guide includes more information on the requirements for the virtual appliance.<br><br>The new Web Security virtual appliance models and configurations are:<br>• S000V (250 GB disk space, 50 GB cache space, 1 core, 4 GB memory)<br>• S100V (250 GB disk space, 50 GB cache space, 2 cores, 6 GB memory)<br>• S300V (1024 GB disk space, 200 GB cache space, 4 cores, 8 GB memory)<br><br>This feature includes the following changes to AsyncOS for Web:<br>• The Web Security virtual appliance license allows you to clone and run multiple virtual appliances on your network.<br>• The loadlicense CLI command for installing the virtual appliance license.<br>• You can use the same license for multiple virtual appliances.<br><br>Feature keys are included as part of the virtual appliance license. The feature keys will expire at the same time as the license. Purchasing new feature keys will require downloading and installing a new virtual appliance license.<br><br>Due to feature keys being included in the virtual appliance license, there are no 30-day evaluations for AsyncOS features.<br><br>You cannot open a Technical Support tunnel before installing the virtual appliance license.<br><br>The version and supportrequest CLI commands have also been updated to included virtual appliance information.<br><br>There are new alerts and logs for mis-configured virtual appliances.<br><br>For more information, see Deploying a Virtual Appliance, page 10. |
| IPv6 Support | IPv6 is supported in both explicit and transparent deployment modes. The IPv6 feature is designed to have the same familiar configuration interface as IPv4. Existing features such as HTTP/HTTPS/FTP, L4TM, Proxy bypass, URL categorization, AVC, among many others all are IPv6 ready. Logs and reports are largely unchanged but offer additional visibility into IPv6 traffic.<br><br>See Functional Support for IPv6 Addresses for additional information. |

| Feature | Description |
|---|---|
| **Enhancements** | |
| User Interface | AsyncOS 8.0.0 introduces an easier-to-use interface that allows “drag and drop” capabilities. The “view reports” page, favorites page, and other interfaces allow user to drag and drop to rearrange items on the screen, such as ordering a list or moving components of the reports dashboard to a different location.<br>The following pages support drag and drop:<br>• Identities<br>• Access Policies<br>• Decryption Policies<br>• Routing Policies<br>• Cisco Data Security<br>• Outbound Malware Scanning<br>• External Data Loss Prevention<br>Also:<br>• Users can now create their own favorites list and customize and schedule My Reports. These features are available from the My Favorites menu.<br>• Users can now adjust web reputation and categorization settings separately using either the web or command line interface.<br>• Users now have the option preserve network settings when resetting the configuration. |

# Upgrade Paths



## Upgrading to Release 8.0.8-113

To ensure a successful upgrade, prepare for the upgrade process as described in Pre-upgrade Requirements, page 8 and Installation and Upgrade Notes, page 8.

You can upgrade to release 8.0.8-113 for AsyncOS for Cisco Web Security appliances from the following versions:

- 7-5-0-703
- 7-5-0-727
- 7-5-0-810
- 7-5-0-825
- 7-5-0-833
- 7-5-0-834
- 7-5-0-836
- 7-5-0-838
- 7-5-0-840
- 7-5-0-850
- 7-5-0-860
- 7-5-0-861
- 7-5-1-074
- 7-5-1-079
- 7-5-1-085
- 7-5-1-201
- 7-5-1-223
- 7-5-1-230
- 7-5-1-245
- 7-5-2-118
- 7-5-2-202
- 7-5-2-303
- 7-5-2-304
- 7-5-2-322
- 7-5-2-501
- 7-5-7-048
- 7-7-0-500
- 7-7-0-608
- 7-7-0-706
- 7-7-0-710
- 7-7-0-725
- 7-7-0-736
- 7-7-0-744
- 7-7-0-753
- 7-7-0-757
- 7-7-0-760
- 7-7-0-761
- 7.7.5-190
- 7.7.5-194
- 7.7.5-195
- 7.7.5-302
- 7.7.5-311
- 8-0-0-408
- 8-0-0-503
- 8-0-5-075
- 8-0-5-079
- 8-0-5-082
- 8-0-6-053
- 8-0-6-078
- 8-0-6-081
- 8-0-6-101
- 8-0-6-119
- 8-0-6-121
- 8-0-6-142
- 8-0-7-142

# Upgrading to Release 8.0.7-142

To ensure a successful upgrade, prepare for the upgrade process as described in Pre-upgrade Requirements, page 8 and Installation and Upgrade Notes, page 8.

You can upgrade to release 8.0.7-142 for AsyncOS for Cisco Web Security appliances from the following versions:

- 7-5-0-703
- 7-5-0-727
- 7-5-0-810
- 7-5-0-825
- 7-5-0-833
- 7-5-0-834
- 7-5-0-836
- 7-5-0-838
- 7-5-0-840
- 7-5-0-850
- 7-5-0-860
- 7-5-0-861
- 7-5-1-074
- 7-5-1-079
- 7-5-1-085
- 7-5-1-201
- 7-5-1-223
- 7-5-1-230
- 7-5-1-245
- 7-5-2-118
- 7-5-2-202
- 7-5-2-303
- 7-5-2-304
- 7-5-2-322
- 7-5-2-501
- 
- 
- 7-5-7-048
- 7-7-0-500
- 7-7-0-608
- 7-7-0-706
- 7-7-0-710
- 7-7-0-725
- 7-7-0-736
- 7-7-0-744
- 7-7-0-753
- 7-7-0-757
- 7-7-0-760
- 7-7-0-761
- 7.7.5-190
- 7.7.5-194
- 7.7.5-195
- 7.7.5-302
- 7.7.5-311
- 8-0-0-408
- 8-0-0-503
- 8-0-5-075
- 8-0-5-079
- 8-0-5-082
- 
- 8-0-6-053
- 8-0-6-078
- 8-0-6-101
- 8-0-6-119

# Pre-upgrade Requirements

## Update RAID Controller Firmware

Before upgrading the AsyncOS software, update the RAID controller firmware as described in *Cisco Update for RAID Controller Firmware (For S360/S370/S660/S670 only, reboot required) Release Notes*.

## Log In to the Administrator Account

You must be logged in as the admin to upgrade.

## Preserve Pre-upgrade Data from the System Capacity Report

Pre-upgrade data for CPU usage for Web Reputation and Web Categorization (as shown in the CPU Usage by Function chart on the System Capacity report page) will not be available after upgrade. If you need to preserve this historic data, export or save the data for the CPU Usage by Function chart as CSV or PDF before you upgrade.

In this release, Web Reputation and Web Categorization data have been combined into a single collation called “Acceptable Use and Reputation.”

### Known Issues

Before you upgrade AsyncOS for Web, see “Current Information about Known and Resolved Issues” section on page 16.

# Installation and Upgrade Notes



## Compatibility Details

## Compatibility with Cisco AsyncOS for Security Management

For compatibility between this release and AsyncOS for Cisco Content Security Management releases, see the compatibility matrix at: http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html.

## IPv6 and Kerberos Not Available in Cloud Connector Mode

When the appliance is configured in Cloud Connector mode, unavailable options for IPv6 addresses and Kerberos authentication appear on pages of the web interface. Although the options appear to be available, they are not supported in Cloud Connector mode. Do not attempt to configure the appliance to use IPv6 addresses or Kerberos authentication when in Cloud Connector mode.

## Functional Support for IPv6 Addresses

Features and functionality that support IPv6 addresses:

- Command line and web interfaces. You can access WSA using http://[2001:2:2::8]:8080 or https://[2001:2:2::8]:8443
- Performing Proxy actions on IPv6 data traffic (HTTP/HTTPS/SOCKS/FTP)
- IPv6 DNS Servers
- WCCP 2.01 (Cat6K Switch) and Layer 4 transparent redirection
- Upstream Proxies
- Authentication Services
  - Active Directory (NTLMSSP, Basic, and Kerberos)
  - LDAP
  - SaaS SSO
  - Transparent User Identification through CDA (communication between WSA and CDA is IPv4 only)
  - Credential Encryption
- Web Reporting and Web Tracking
- External DLP Servers (communication between WSA and DLP Server is IPv4 only)
- PAC File Hosting

Features and functionality that require IPv4 addresses:

- Internal SMTP relay
- External Authentication
- Log subscriptions push method: FTP, SCP, and syslog
- NTP servers
- Local update servers, including Proxy Servers for updates
- Authentication services
- AnyConnect Security Mobility
- Novell eDirectory authentication servers
- Custom logo for end-user notification pages

- Communication between the Web Security appliance and the Security Management appliance
- WCCP versions prior to 2.01
- SNMP

### Availability of Kerberos Authentication for Operating Systems and Browsers

You can use Kerberos authentication with these operating systems and browsers:

- Windows servers 2003, 2008, 2008R2 and 2012
- Latest releases of Safari and Firefox browsers on Mac (OSX Version 10.5+)
- IE (Version 7+) and latest releases of Firefox and Chrome browsers on Windows 7 and XP.

Kerberos authentication is not available with these operating systems and browsers:

- Windows operating systems not mentioned above
- Browsers not mentioned above
- iOS and Android

## Deploying a Virtual Appliance

To deploy a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

### Migrating from Hardware to Virtual Appliance

To migrate your configuration from physical hardware:

**Step 1** Upgrade your hardware appliance to this AsyncOS release.

**Step 2** Save the configuration file.

**Step 3** Set up your virtual appliance with this AsyncOS release.

**Step 4** Import the configuration file from your hardware appliance into the virtual appliance.

## Configuration Files

When you upgrade AsyncOS for Web from the web interface or Command Line Interface (CLI), the configuration is saved to file in the /configuration/upgrade directory. You can access the upgrade directory using an FTP client. Each configuration file name is appended with the version number, and passwords in the configuration file are masked so they are not human readable.

Generally, configuration files are not compatible between different AsyncOS releases.

## Post-upgrade Reboot

You must reboot the Web Security appliance after you upgrade AsyncOS for Web.

## Changes in Behavior

This section describes changes in behavior from previous versions of AsyncOS for Web that may affect the appliance configuration after you upgrade to the latest version.

### X-Authenticated-Groups Header Format

With LDAP authentication and External Data Loss Prevention configured on the appliance, AsyncOS now sends the X-Authenticated-Groups header in this format:

LDAP://(*LDAP server name*)/(*groupname*).

Previously, the format was LDAP://(*groupname*). This software change may require changes to policies or other automation relying on the X-Authenticated-Groups header. [Defect: CSCum91801]

# Upgrading AsyncOS for Web

**Before You Begin**

- Perform preupgrade requirements, including updating the RAID controller firmware. Pre-upgrade Requirements, page 8.

**Step 1** On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

**Step 2** On the System Administration > System Upgrade page, click **Available Upgrades**.

The page refreshes with a list of available AsyncOS for Web upgrade versions.

**Step 3** Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.

**Step 4** When the upgrade is complete, click **Reboot Now** to reboot the Web Security appliance.

**Note** To verify the browser loads the new online help content in the upgraded version of AsyncOS, you must exit the browser and then open it before viewing the online help. This clears the browser cache of any outdated content.

New features are typically not enabled by default.

# Documentation Updates

The following section is missing from the User Guide and online Help, as is a link to it from the `%Xr` description in the access-logs table.

# Interpreting Access Log Scanning Verdict Entries

The access log file entries aggregate and display the results of the various scanning engines, such as URL filtering, Web Reputation filtering, and anti-malware scanning. The appliance displays this information in angled brackets at the end of each access log entry.

The following text is the scanning verdict information from an access log file entry. In this example, the Webroot scanning engine found the malware:

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",-,-,
IW_infr,-,"Trojan Phisher","-","Unknown","Unknown","-","-",489.73,0,-,[Local],"-"
,37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d
85829614fba368a421d14e64c426da5e”>
```

**Note** For an example of a whole access log file entry, see “Access Log Files” on page 21-13 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*.

Each element in this example corresponds to a log-file format specifier as shown in the following table:

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 1 | `IW_infr` | %XC | The URL category assigned to the transaction, abbreviated. This field shows “nc” when no category is assigned.<br>For a list of URL category abbreviations, see “URL Category Descriptions” on page 9-23 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*. |
| 2 | `ns` | %XW | Web Reputation filters score. This field either shows the score as a number, “ns” for no score, or “dns” when there is a DNS lookup error. |
| 3 | `24` | %Xv | The malware scanning verdict Webroot passed to the DVS engine. Applies to responses detected by Webroot only.<br>For more information, see “Malware Scanning Verdict Values” on page 21-37 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*. |
| 4 | `“Trojan-Phisher-Gamec”` | “%Xn” | Name of the spyware that is associated with the object. Applies to responses detected by Webroot only. |
| 5 | `0` | %Xt | The Webroot specific value associated with the Threat Risk Ratio (TRR) value that determines the probability that malware exists. Applies to responses detected by Webroot only. |
| 6 | `354385` | %Xs | A value that Webroot uses as a threat identifier. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only. |
| 7 | `12559` | %Xi | A value that Webroot uses as a trace identifier. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 8 | - | %Xd | The malware scanning verdict McAfee passed to the DVS engine. Applies to responses detected by McAfee only.<br><br>For more information, see "Malware Scanning Verdict Values" on page 21-37 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*. |
| 9 | "-" | "%Xe" | The name of the file McAfee scanned. Applies to responses detected by McAfee only. |
| 10 | - | %Xf | A value that McAfee uses as a scan error. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only. |
| 11 | - | %Xg | A value that McAfee uses as a detection type. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only. |
| 12 | - | %Xh | A value that McAfee uses as a virus type. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only. |
| 13 | "-" | "%Xj" | The name of the virus that McAfee scanned. Applies to responses detected by McAfee only. |
| 14 | - | %XY | The malware scanning verdict Sophos passed to the DVS engine. Applies to responses detected by Sophos only.<br><br>For more information, see "Malware Scanning Verdict Values" on page 21-37 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*. |
| 15 | - | %Xx | A value that Sophos uses as a scan return code. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only. |
| 16 | "-" | "%Xy" | The file location where Sophos found the objectionable content. For non-archive files, this value is the file name itself. For an archive file, it is the object in the archive, such as `archive.zip/virus.exe`. Applies to responses detected by Sophos only. |
| 17 | "-" | "%Xz" | A value that Sophos uses as the threat name. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only. |
| 18 | - | %Xl | The Cisco Data Security scan verdict based on the action in the Content column of the Cisco Data Security Policy. The following list describes the possible values for this field:<br><br>• **0.** Allow<br>• **1.** Block<br>• **- (hyphen).** No scanning was initiated by the Cisco Data Security Filters. This value appears when the Cisco Data Security Filters are disabled, or when the URL category action is set to Allow. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 19 | - | %Xp | The External DLP scan verdict based on the result given in the ICAP response. The following list describes the possible values for this field:<br>• **0.** Allow<br>• **1.** Block<br>• **- (hyphen).** No scanning was initiated by the external DLP server. This value appears when External DLP scanning is disabled, or when the content was not scanned due to an exempt URL category on the External DLP Policies > Destinations page. |
| 20 | IW_infr | %XQ | The URL category verdict determined during request-side scanning, abbreviated. This field lists a hyphen ( - ) when URL filtering is disabled.<br>For a list of URL category abbreviations, see "URL Category Descriptions" on page 9-23 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*. |
| 21 | - | %XA | The URL category verdict determined by the Dynamic Content Analysis engine during response-side scanning, abbreviated. Applies to the Cisco Web Usage Controls URL filtering engine only. Only applies when the Dynamic Content Analysis engine is enabled and when no category is assigned at request time (a value of "nc" is listed in the request-side scanning verdict).<br>For a list of URL category abbreviations, see "URL Category Descriptions" on page 9-23 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*. |
| 22 | "Trojan Phisher" | "%XZ" | Unified response-side anti-malware scanning verdict that provides the malware category independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. |
| 23 | "-" | "%Xk" | The threat type returned by the Web Reputation filters which resulted in the target website receiving a poor reputation. Typically, this field is populated for sites at reputation of -4 and below. |
| 24 | "Unknown" | "%XO" | The application name as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled. |
| 25 | "Unknown" | "%Xu" | The application type as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled. |
| 26 | "-" | "%Xb" | The application behavior as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled. |
| 27 | "-" | "%XS" | Safe browsing scanning verdict. This value indicates whether either the safe search or the site content ratings feature was applied to the transaction.<br>For a list of the possible values, see "Logging Adult Content Access" on page 9-16 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide*. |
| 28 | 489.73 | %XB | The average bandwidth consumed serving the request, in Kb/sec. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 29 | 0 | %XT | A value that indicates whether the request was throttled due to bandwidth limit control settings, where "1" indicates the request was throttled, and "0" indicates it was not. |
| 30 | [Local] | %l | The type of user making the request, either "[Local]" or "[Remote]." Only applies when AnyConnect Secure Mobility is enabled. When it is not enabled, the value is a hyphen (-). |
| 31 | "-" | "%X3" | Unified request-side anti-malware scanning verdict independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to client request scanning when an Outbound Malware Scanning Policy applies. |
| 32 | "-" | "%X4" | The threat name assigned to the client request that was blocked or monitored due to an applicable Outbound Malware Scanning Policy.<br>This threat name is independent of which anti-malware scanning engines are enabled. |
| 33 | 37 | %X#1# | Verdict from Advanced Malware Protection file scanning:<br>• 0: File is not malicious<br>• 1: File was not scanned because of its file type<br>• 2: File scan timed out<br>• 3: Scan error<br>• Greater than 3: File is malicious |
| 34 | "W32.CiscoTestVector" | %X#2# | Threat name, as determined by Advanced Malware Protection file scanning; "-" indicates no threat. |
| 35 | 33 | %X#3# | Reputation score from Advanced Malware Protection file scanning. This score is used only if the cloud reputation service is unable to determine a clear verdict for the file.<br>For details, see information about the Threat Score and the reputation threshold in Chapter 14, "File Reputation Filtering and File Analysis," of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide* |
| 36 | 0 | %X#4# | Indicator of upload and analysis request:<br>"0" indicates that Advanced Malware Protection did not request upload of the file for analysis.<br>"1" indicates that Advanced Malware Protection did request upload of the file for analysis. |
| 37 | "WSA-INFECTED-FILE.pdf" | %X#5# | The name of the file being downloaded and analyzed. |
| 38 | "fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e | %X#6# | The SHA-256 identifier for this file. |

Refer to "Log File Fields and Tags" on page 21-28 of the *AsyncOS 8.7 for Cisco Web Security Appliances User Guide* for a description of each format specifier's function.

# Current Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find current information about known and fixed defects.

## Requirements for Accessing the Cisco Bug Search Tool

Register for a Cisco account if you do not have one: https://tools.cisco.com/RPF/register/register.do.

## Lists of Known and Fixed Issues

**Note** Issues that were open in previous releases may also be open in this release. These searches find issues and fixes that are new in this release.

### Known and Fixed Issues in Release 8.0.8-113 (ED)

| | |
|---|---|
| **Known issues** | https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.0.8&sb=anfr&sts=open&srtBy=byRel&bt=custV |
| **Fixed issues** | https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.0.8-113&sb=fr&svr=3nH&srtBy=byRel&bt=custV |

## Other Bug Searches

**Step 1** Go to https://tools.cisco.com/bugsearch/.

**Step 2** Log in with your Cisco account credentials.

**Step 3** Enter search criteria.

For example, enter a Bug ID number in the “Search for” field.

**Note** The 5-digit bug numbers used in previous AsyncOS releases cannot be used with this tool.

**Step 4** If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool.

# Related Documentation

Documentation for this product is available from http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html.

Documentation for Cisco Content Security Management Appliances is available from http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

# Support

## Knowledge Base

You can access the Cisco Knowledge Base on the Cisco Customer Support site at the following URL:

http://www.cisco.com/web/ironport/knowledgebase.html

**Note** You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, you can register for one here: `https://tools.cisco.com/RPF/register/register.do`

## Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community for web security and associated management:

https://supportforums.cisco.com/community/5786/web-security

## Customer Support

International: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: Visit http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.