Release Notes for AsyncOS 8.8 for Cisco Web Security Appliances - ED

Published: July 6, 2015

Revised: January 26, 2016

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

What's New in Cisco AsyncOS 8.8

Feature	Description
ISE failover	Integration with Identity Services Engine (ISE), versions 1.3 and later, is complete. Enhancements include the option to connect to two individual ISE servers, which provides failover capability.
Secure ICAP	You can now secure the channel between the appliance and an external DLP (ICAP) server.
Support for on-premises File Analysis	If you deploy a Cisco AMP Threat Grid appliance on your network, you can analyze downloaded files for threats without sending them to the public cloud. For more information, see the "File Reputation Filtering and File Analysis" user guide PDF.
Cognitive Threat Analytics (CTA) Integration	You can now push custom SCP-formatted W3C logs to a cloud-based CTA analysis and reporting service.

What's New in Cisco AsyncOS 8.7

Feature	Description
ISE integration	AsyncOS can now access additional user-identity information from an Identity Services Engine (ISE) version 1.3 server deployed in the same network.
SSL configuration	For enhanced security, you can enable and disable SSLv3 for several services. Services with SSLv3 disabled will use TLSv1.0. 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. Use the Web interface (System Administration > SSL Configuration), or the CLI (`sslconfig`).

Requirements and Restrictions for AsyncOS 8.7

Please be aware of the following requirements and restrictions for AsyncOS 8.7:

- AsyncOS 8.7 supports only version 1.3 of the Identity Services Engine.
- This release of AsyncOS does not support Connector mode; however, when operating in Connector mode, ISE-specific options remain visible and apparently available. To reiterate, Connector mode is not supported, and if your system is operating in that mode, **you should not upgrade** to this release.

Release Classification

Each release is identified by the release type (ED - Early Deployment, GD - General Deployment, etc.) For an explanation of these terms, see http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - S170
  - S370
  - S670
  - S680
  - S380

Some hardware models require a memory upgrade before you can install or upgrade to this AsyncOS release. For more information, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html

Upgrade Paths

Before you start the upgrade process, see Pre-Upgrade Requirements, page 5 and Installation and Upgrade Notes, page 5.

Upgrading to AsyncOS 8.8

You can upgrade to release 8.8.0-085 for AsyncOS for Cisco Web Security appliances from the following version:

- 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
- 7.7.0-764

- 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

- 8.0.7-142
- 8.0.7-149

- 8.0.8-113

- 8.1.0-235
- 8.1.0-245

- 8.5.0-389
- 8.5.0-390
- 8.5.0-476
- 8.5.0-497
- 8.5.0-518

- 8.5.1-019
- 8.5.1-021
- 8.5.1-022

- 8.5.2-027

- 8.7.0-141
- 8.7.0-172

- 8.8.0-21
- 8.8.0-33

Upgrading to AsyncOS 8.7

You can upgrade to release 8.7.0-172 for AsyncOS for Cisco Web Security appliances from the following versions:

- 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
- 8-0-7-142
- 8-1-0-235
- 8-1-0-245
- 8-5-0-389
- 8-5-0-390
- 8-5-0-476
- 8-5-0-518
- 8-5-1-019
- 8-5-1-021
- 8-6-0-025
- 8-7-0-141

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*.

Check Post-Upgrade Requirements Before Upgrading

Some existing functionality will not work after upgrade until you make changes. To minimize downtime, familiarize yourself with and prepare for those requirements before upgrading. See Important! Actions Required After Upgrading.

Installation and Upgrade Notes

- Compatibility Details
- Deploying a Virtual Appliance
- Configuration Files
- Demo Security Certificate Encryption Strength
- Post-Upgrade Reboot

Compatibility Details

- Compatibility with Cisco AsyncOS for Security Management
- IPv6 and Kerberos Not Available in Cloud Connector Mode
- Functional Support for IPv6 Addresses
- Availability of Kerberos Authentication for Operating Systems and Browsers

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/c/en/us/support/security/content-security-management-appliance/products-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 with 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 a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance with this AsyncOS release using the documentation described in Deploying a Virtual Appliance, page 7.

Step 2 Upgrade your hardware appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded hardware appliance.

Step 4 Load the configuration file from the hardware appliance onto the virtual appliance.

If your hardware and virtual appliances have different IP addresses, deselect Load Network Settings before loading the configuration file.

Step 5 Commit your changes.

Step 6 Go to **Network > Authentication** and join the domain again. Otherwise identities won’t work.

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 from earlier AsyncOS releases are incompatible with later AsyncOS releases and vice-versa.

Demo Security Certificate Encryption Strength

The encryption strength of the demo security certificate is 1024 bits both before and after upgrade to AsyncOS 8.5 and later.

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.

List of Available Upgrades

Beginning in AsyncOS 8.5, all available releases appear in the list of available upgrades, including releases that would previously have been provisioned only to a limited number of customers as a limited release.

Each release in the list is identified by the release type (ED - Early Deployment, GD - General Deployment, MD - Maintenance Deployment, etc.) For an explanation of these terms, see http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf.

Support Requests Require CCO ID and Support Contract

Beginning in AsyncOS 8.5, in order to open a support request from the appliance, you must enter a CCO ID and a support contract ID.

New Certificate Management Page

Beginning in AsyncOS 8.5, certificate management functionality has been moved from the Security Services > HTTPS Proxy page to a new, stand-alone page: Network > Certificate Management.

Exporting Web Tracking Data

Previously, when exporting web tracking data as CSV, the data was sorted by timestamp. Beginning in AsyncOS 8.5, this data is not sorted.

SNMP Monitoring

Beginning in AsyncOS 8.5, the following functionality is different from previous implementations:

Message authentication and encryption are mandatory when enabling SNMPv3. Passwords for authentication and encryption should be different. The encryption algorithm can be AES (recommended) or DES. The authentication algorithm can be SHA-1 (recommended) or MD5.

X-Authenticated-Groups Header Format

Beginning in AsyncOS 8.5, if LDAP authentication and External Data Loss Prevention are configured on the appliance, AsyncOS 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. See Pre-Upgrade Requirements, page 5.
- Log in as Administrator.

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.

Important! Actions Required After Upgrading

In order to ensure that your appliance continues to function properly after upgrade, you must address the following items:

Virtual Appliances: Required Changes for SSH Security Vulnerability Fix

Requirements in this section were introduced in AsyncOS 8.8.

The following security vulnerability will be fixed during upgrade if it exists on your appliance: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport.

If you did not patch this issue before upgrading, you will see a message during upgrade stating that it has been fixed. If you see this message, the following actions are required to return your appliance to full working order after upgrade:

- Remove the existing entry for your appliance from the known hosts list in your ssh utility. Then ssh to the appliance and accept the connection with the new key.
- If you use SCP push to transfer logs to a remote server (including Splunk): Clear the old SSH host key for the appliance from the remote server.
- If your deployment includes a Cisco Content Security Management Appliance, see important instructions in the Release Notes for that appliance.

File Analysis: Required Changes to View Analysis Result Details in the Cloud

The requirement in this section was introduced in AsyncOS 8.8.

If you have deployed multiple content security appliances (web, email, and/or management) and you want to view detailed file analysis results in the cloud for all files uploaded from any appliance in your organization, you must configure an appliance group on each appliance after upgrading. To configure appliance groups, see the “File Reputation Filtering and File Analysis” chapter in the user guide PDF. (This PDF is more current than the online help in AsyncOS 8.8.)

File Analysis: Verify File Types To Be Analyzed

The File Analysis cloud server URL has changed, and as a result, the file types that can be analyzed may have changed after upgrade. You should receive an alert if there are changes. To verify the file types selected for analysis, select **Security Services > Anti-Malware and Reputation** and look at the Advanced Malware Protection settings.

Upgrading from non-ISE Releases and AsyncOS 8.5 with ISE Preview

All AsyncOS versions that did not include ISE support (that is, all versions prior to 8.5.0-497), and the limited-availability AsyncOS 8.5 “ISE Preview” release, did not require the Admin and pxGrid certificates, which are necessary in all Cisco AsyncOS releases that include ISE support. Therefore, when you upgrade from a non-ISE release, or from an ISE Preview installation with ISE enabled, the ISE feature will not operate correctly until the two additional certificates are provided (go to **Network > Identity Services Engine**).

Unescaped Dots in Regular Expressions

Following upgrades to the regular-expression pattern-matching engine, you may receive an alert regarding unescaped dots in existing pattern definitions after updating your system. Any unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the Velocity pattern-matching engine, and an alert to that effect will be sent to you, and you continue to receive an alert following each update until you correct or replace the pattern. Generally, unescaped dots in a larger regular expression can be problematic and should be avoided.

Documentation Updates

The following information supplements information in the Online Help and/or User Guide for this release

Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?

The criteria for evaluating a file's reputation and for sending files for analysis may change at any time. Criteria are available only to registered Cisco customers. See *File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

In order to access this document, you must have a Cisco customer account with a support contract. To register, visit https://tools.cisco.com/RPF/register/register.do.

Viewing File Analysis Details in the Cloud

The most current instructions for configuring this functionality are in the user guide PDF, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

Additional Information

The User Guide PDF may be more current than the online help. To obtain the User Guide PDF and other documentation for this product, click the **View PDF** button in the online help or visit the URL shown in Related Documentation, page 13.

Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

Bug Search Tool Requirements

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

Lists of Known and Fixed Issues

Fixed Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.8.0-085&sb=fr&svr=3nH&srtBy=byRel&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.8.0&sb=anfr&sts=open&srtBy=byRel&bt=custV

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find the most current information about known and resolved defects in shipping releases.

Before You Begin

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

Procedure

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

Step 2 Log in with your Cisco account credentials.

Step 3 Click **Select from list** > **Security** > **Web Security** > **Cisco Web Security Appliance**, and click **OK**.

Step 4 In Releases field, enter the version of the release, for example, 8.8.

Step 5 Depending on your requirements, do one of the following:

- To view the list of resolved issues, select **Fixed in these Releases** from the Show Bugs drop down.
- To view the list of known issues, select **Affecting these Releases** from the Show Bugs drop down and select **Open** from the Status drop down.

Note If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool. There is also an interactive tour; to view it, click the link in the orange bar above the search fields.

Related Documentation

Documentation for this product is available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html.

Documentation for Cisco Content Security Management Appliances is available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html.

Support

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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.