Release Notes for AsyncOS 8.7 for Cisco Web Security Appliances (LD)

Published: April 1, 2015

Revised: October 15, 2015

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

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.

What's New in Cisco AsyncOS 8.6

Feature	Description
Virtual Appliance enhancements	• Virtual appliances can now be deployed on a KVM hypervisor running on the following Linux platforms: – Red Hat Enterprise Linux Server 7.0 – Ubuntu Server 14.04.1 LTS Thin provisioning for disk storage is supported. • You can configure the Cisco appliance license and configuration files to load automatically upon initial startup, on either VMWare ESXi or KVM deployments. For details, 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 **Important!** See Virtual Appliance Running on KVM Hangs on Reboot, page 10.

What's New in Cisco AsyncOS 8.5

Feature	Description
High Availability	This release provides a built-in high availability option suitable for deployments in which the appliance runs in explicit mode with a proxy. For more information, see the "Connect, Install, and Configure" chapterin the User Guide.
2048-bit certificates	The key length for SSL certificates generated or processed by the appliance is now 2048 bits.
LDAP authentication	LDAP protocol is now supported for authenticating administrative users of the appliance.
Volume and Time Quotas	You can apply time and volume quotas to access policies and decryption policies. Quotas allow individual users to continue accessing an Internet resource (or a class of Internet resources) until they exhaust the data volume or time limit imposed.
Web Security Virtual Appliance enhancements	• Support for VMWare ESXi 5.5 • Support for thin provisioning in ESXi • Now, after the virtual appliance license expires, there is a six-month grace period during which the appliance continues to process web transactions, but without security services You can configure the appliance to send you alerts when the license expiration date approaches. • Evaluation feature keys can now be deployed on virtual appliances

Feature	Description
Authentication by machine ID	For deployments in Connector mode with Active Directory, this release introduces the option to authorize access based on device ID.
Advanced Malware Protection enhancements	• Advanced Malware Protection can now detect malware in archived or compressed files. • You can now select the interface used to communicate with an AMP server. • File analysis now supports analysis of additional file types. Supported file types are determined by the cloud service and can change at any time. When you configure the File Analysis feature, you can choose which file types to send for analysis, and you can choose to receive alerts when the options change. For more information, see "Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?" in the Release Notes, and the chapter "File Reputation and File Analysis" in the on-line help or User Guide for information about supported file types and alerts.
AAA Audit logging	AsyncOS is enhanced to standardize AAA-related logging across multiple logs, and to centralize them into a central log subscription. This new log subscription will be exportable via syslog.
Password security enhancements	The following password enhancements have been introduced for locally-defined administrative users: • Show a password strength indicator to a user entering a new password. Password strength is enforced by the password requirements that you specify. • Disallow certain words in passwords. (You upload a list of forbidden words to the appliance.) • The option to generate a password by clicking a button. For more information, see the "Setting Password Requirements for Administrative Users" and "Adding Local User Accounts" sections in the User Guide.
Web Tracking enhancement	There is a new "All Malware" option when you filter web tracking results by Malware Threat.
Cisco Content Security Management Virtual Appliance	You can now manage multiple Web Security appliances with a virtual content security management appliance that has the same functionality as a physical hardware appliance.
Trusted Root Certificate management	Trusted Root Certificate management was moved from Security Services > HTTPS Proxy to Network > Certificate Management.
DNS server failover	If the primary DNS server is non-responsive for a user-specified number of queries, it is considered to have failed and queries are automatically directed to the secondary server.

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 Installation Notes, page 6.

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

Installation Notes

- Upgrading from non-ISE Releases and AsyncOS 8.5 with ISE Preview
- Compatibility Details
- Deploying a Virtual Appliance
- Configuration Files

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**).

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

There is no migration path from hardware appliances to this release.

Configuration Files

Generally, configuration files from earlier AsyncOS releases are incompatible with later AsyncOS releases and vice-versa.

Known and Resolved Issues

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

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

Known issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.7.0&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV
Fixed issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.7.0-172&sb=fr&svr=3nH&srtBy=byRel&bt=custV

Finding Other Bugs

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

Step 2 Log in with your Cisco account credentials.

Step 3 Enter search criteria.

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/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

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.

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.