Release Notes for Cisco AsyncOS 8.1 for Web (All Builds)

This document is cumulative for all releases of AsyncOS 8.1 for Cisco Web Security appliances.

Published: August 13, 2014

Revised: September 26, 2014

Contents

What's New in This Release

Cisco Systems, Inc.
www.cisco.com

What's New in Release 8.1

Feature	Description
Multiple file types can be sent for analysis	This release 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?, page 10 and information about supported file types and alerts in the File Reputation and File Analysis chapter in the online help or user guide.

What's New in Release 8.0.6

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.
	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.

What's New 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.
	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.
	For requirements and other details, see the File Reputation Filtering and File Analysis chapter in the online help or user guide.

What's New 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.
	Cloud Web Security Connector mode is available through the Cisco Web Security Virtual Appliance as well as the physical Web Security appliance.
	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."
	Note Kerberos authentication and IPv6 addresses are not supported in Cloud Connector mode.
	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.
	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.
	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.
	The Cisco Security Virtual Appliance Installation Guide includes more information on the requirements for the virtual appliance.
	The new Web Security virtual appliance models and configurations are: • S000V (250 GB disk space, 50 GB cache space, 1 core, 4 GB memory) • S100V (250 GB disk space, 50 GB cache space, 2 cores, 6 GB memory) • S300V (1024 GB disk space, 200 GB cache space, 4 cores, 8 GB memory)
	This feature includes the following changes to AsyncOS for Web: • The Web Security virtual appliance license allows you to clone and run multiple virtual appliances on your network. • The loadlicense CLI command for installing the virtual appliance license. • You can use the same license for multiple virtual appliances.
	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.
	Due to feature keys being included in the virtual appliance license, there are no 30-day evaluations for AsyncOS features.
	You cannot open a Technical Support tunnel before installing the virtual appliance license.
	The version and supportrequest CLI commands have also been updated to included virtual appliance information.
	There are new alerts and logs for mis-configured virtual appliances.
	For more information, see Deploying a Virtual Appliance, page 8.
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.
	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.
	The following pages support drag and drop:
	• Identities
	• Access Policies
	• Decryption Policies
	• Routing Policies
	• Cisco Data Security
	• Outbound Malware Scanning
	• External Data Loss Prevention
	Also:
	• Users can now create their own favorites list and customize and schedule My Reports. These features are available from the My Favorites menu.
	• Users can now adjust web reputation and categorization settings separately using either the web or command line interface.
	• Users now have the option preserve network settings when resetting the configuration.

Upgrade Paths

Upgrading to Release 8.1.0-235 (FCS - Limited Availability)

Note **This upgrade is needed only for S380 and S680 hardware.** The fix in this release also requires a RAID firmware upgrade. For details, see Resolved Issues in Release 8.1.0-235, page 11.

Before you start the upgrade process, see Preupgrade Requirements, page 6 and Installation and Upgrade Notes, page 7.

You can upgrade to release 8.1.0-235 from the following versions:

• 7.5.0-703	• 7.5.1-074	• 7.5.2-118	• 7.7.0-500	• 7.7.5-190	• 8.0.0-408
• 7.5.0-727	• 7.5.1-079	• 7.5.2-202	• 7.7.0-608	• 7.7.5-194	• 8.0.0-503
• 7.5.0-810	• 7.5.1-085	• 7.5.2-303	• 7.7.0-706	• 7.7.5-195	
• 7.5.0-825	• 7.5.1-201	• 7.5.2-304	• 7.7.0-710	• 7.7.5-302	• 8.0.5-075
• 7.5.0-833	• 7.5.1-223	• 7.5.2-306	• 7.7.0-725	• 7.7.5-311	• 8.0.5-079
• 7.5.0-834	• 7.5.1-230	• 7.5.2-322	• 7.7.0-736		• 8.0.5-082
• 7.5.0-836	• 7.5.1-245	• 7.5.2-501	• 7.7.0-744		
• 7.5.0-838			• 7.7.0-753		• 8.0.6-053
• 7.5.0-840		• 7.5.7-048	• 7.7.0-757		• 8.0.6-078
• 7.5.0-850					
• 7.5.0-860					• 8.1.0-228
• 7.5.0-861					

Upgrading to Release 8.1.0-228 (Deprovisioned 9/10/2014)

It is no longer possible to upgrade to this release.

Preupgrade 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*.

Login 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 .

Installation and Upgrade Notes

- Compatibility Details
- Deploying a Virtual Appliance
- Configuration Files
- Compatibility with Cisco AsyncOS for Security Management
- 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

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 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. Preupgrade Requirements, page 6.

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

A Proxy is Not Supported for Communications with the File Analysis Server

Using a proxy is not supported for communications between the Web Security appliance and the file analysis service in the cloud, even if an upstream proxy is transparent to the Web Security appliance and communications with the File Reputation service use a proxy.

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.

Resolved Issues in This Release

Resolved Issues in Release 8.1.0-235

For S380 and S680 hardware only: This release, in conjunction with the required firmware upgrade described in Field Notice 63877, prevents an issue that can cause the appliance to become permanently inaccessible. If this issue occurs, the only solution is to RMA the appliance; there is no workaround. This issue does not affect any other S-Series hardware model.

For complete information, see:

- Field Notice 63877 at http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63877.html.
- Bug CSCup88211 in the Bug Search Tool at https://tools.cisco.com/bugsearch/bug/CSCup88211.
- Release Notes for the S380/S680 RAID firmware update at http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html.

Current Information about 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=2825213 10&rls=8.1.0&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV
Fixed issues	https://tools.cisco.com/bugsearch/search?pf=sr&pfVal=282521310&prdNam =Cisco%20Web%20Security%20Appliance&rls=8.1.0&sb=fr&bt=custV&srt By=byRel

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/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.