Release Notes for AsyncOS 8.5.x for Cisco Web Security Appliances

This document is cumulative for all releases of AsyncOS 8.5.x for Cisco Web Security appliances.

Published: November 12, 2014

Revised: February 14, 2017

Contents

New Features

- New Features in Release 8.5.4-038 (MD), page 2
- New Features in Release 8.5.3-069 (GD), page 2
- New Features in Release 8.5.2-027 (MD), page 2
- New Features in Release 8.5.1, page 3

Cisco Systems, Inc.
www.cisco.com

- New Features in Release 8.5.0, page 4

New Features in Release 8.5.4-038 (MD)

This release contains a number of bug fixes; see the “Fixed issues” search in Known and Fixed Issues in Release 8.5.4-038 (MD), page 17 for additional information.

New Features in Release 8.5.3-069 (GD)

This release contains a number of bug fixes; see the “Fixed issues” search in Known and Fixed Issues in Release 8.5.3-069 (GD), page 17 for additional information.

New Features in Release 8.5.2-027 (MD)

Primary changes in this release are related to disabling and enabling SSLv3, as well as elliptic-curve Diffie-Hellman ephemeral (ECDHE) features, and for configuring update server certificate validation.

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>SSL configuration</td><td>

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`).

</td></tr>
<tr><td>ECDHE authentication</td><td>

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.

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:

```
Choose the operation you want to perform:
- SSLV3 - Enable or disable SSL v3.
- ECDHE - Enable or disable ECDHE Authentication.
[]> ECDHE

ECDHE cipher status is enabled in Proxy & enabled in LDAP

Please select an option to change ECDHE cipher status:
- 1 - Toggle ECDHE cipher status in Proxy
- 2 - Toggle ECDHE cipher status in LDAP
- 3 - Enable ECDHE cipher in both Proxy & LDAP
- 4 - Disable ECDHE cipher  in both Proxy & LDAP
[]>
```

</td></tr>
</table>

Feature	Description
Updater certificate verification	Two new certificate-related subcommands were added to the CLI command `updateconfig` to let you manage the certificates used by the update client to verify the issuer of the server certificate. The update client validates the update server certificate before downloading updates. If certificate validation fails, alert notifications will be sent at regular intervals with the reason for failure and update will be aborted. The default generation of alerts will be at five minutes, 15 minutes, 35 minutes, and finally at 60 minutes repeating interval (present behavior). When the server certificate is finally validated, the update process will continue. If the update server points to `update-manifests.ironport.com` or `update-manifests.sco.cisco.com` and that server's root signing certificate is not flagged as "not trusted," the updates/upgrades process will operate without any issues. For other update servers, you must explicitly upload the appropriate certificate for update/upgrade purposes. The new `updateconfig` subcommands are: • `validate_certificates` Lets you turn off or on update server certificate validation (enter `yes` or `no`); it is on by default. • `trusted_certificates` Available options are: – `list` – Display a list of current trusted certificates used for updates. – `add` – Upload new trusted certificates for updates. Provide the certificate text (PEM format) and then enter a . (dot, full stop, period) to indicate the end of the certificate. Repeat this process to add another certificate. To exit certificate-upload mode, press the Enter key. – `delete` – Delete a current update certificate, as identified by its name or number in the `list` output. **Note** `UPDATER.UPDATERD.SERVER_CERT_ERROR` is a new updater log entry that will be recorded upon a server certificate-validation failure.

New Features in Release 8.5.1

Release 8.5.1-021 (GD)

This release includes a specific bug fix; see the "Fixed issues" search in Known and Fixed Issues in Release 8.5.1-021 (GD), page 17 for details.

Release 8.5.1-019 (MR)

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

New Features in Release 8.5.0

The following new features and enhancements have been added in this release.

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" chapter in 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 thin provisioning • Support for ESXi 5.5 • 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
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.

Feature	Description
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.

Upgrade Paths

Upgrading to Release 8.5.4-038 (MD)

Caution Before you start the upgrade process, see Installation and Upgrade Notes, page 10 and Known and Fixed Issues in Release 8.5.4-038 (MD), page 17.

You can upgrade to release 8.5.4-038 for AsyncOS for Cisco Web Security appliances from the following versions:

- 8.0.6-119
- 8.0.7-142
- 8.0.8-118
- 8.5.1-104
- 8.5.2-027
- 8.5.3-069

Upgrading to Release 8.5.3-069 (GD)

Before you start the upgrade process, see Installation and Upgrade Notes, page 10.

You can upgrade to release 8.5.3-069 for AsyncOS for Cisco Web Security appliances from the following versions; “multi-hop” upgrade paths are also provided.

Note You cannot upgrade from AsyncOS 8.5.3 to AsyncOS 9.0.

Direct Upgrade Paths

- 7.7.0-764
- 7.7.0-809
- 7.7.5-311
- 8.0.7-152
- 8.0.7-154
- 8.0.8-113
- 8.0.8-118
- 8.0.8-401
- 8.1.0-235
- 8.1.0-245
- 8.5.1-021
- 8.5.2-027[1]
- 8.5.3-051
- 8.5.3-064
- 8.5.3-068

[1] You cannot upgrade to 8.5.3-069 from 8.5.2-027 with the CLI command if you want to use either the save-password or email-configuration options. We recommend using the Web interface. [CSCuu81990]

Multi-hop Upgrade Paths

- 7.5.0-517 -> 7.5.0-703 -> 8.0.8-113
- 7.5.0-586 -> 7.5.0-703 -> 8.0.8-113
- 7.5.0-680 -> 8.0.6-119
- 7.5.0-690 -> 7.5.0-703 -> 8.0.8-113
- 7.5.0-703 -> 8.0.8-113
- 7.5.0-727 -> 8.0.8-113
- 7.5.0-805 -> 7.5.0-833 -> 8.0.8-113
- 7.5.0-825 -> 8.0.8-113
- 7.5.0-826 -> 7.5.0-833 -> 8.0.8-113
- 7.5.0-833 -> 8.0.8-113
- 7.5.0-834 -> 8.0.8-113
- 7.5.0-838 -> 8.0.8-113
- 7.5.0-861 -> 8.0.8-113
- 7.5.1-073 -> 7.5.1-074 -> 8.0.8-113
- 7.5.1-074 -> 8.0.8-113
- 7.5.1-079 -> 8.0.8-113
- 7.5.1-085 -> 8.0.8-113
- 7.5.1-201 -> 8.0.8-113
- 7.5.1-223 -> 8.0.8-113
- 7.5.2-118 -> 8.0.8-113
- 7.5.2-303 -> 8.0.8-113
- 7.5.2-304 -> 8.0.8-113
- 7.5.1-201 -> 8.0.7-142
- 7.5.2-118 -> 8.0.8-113
- 7.5.2-303 -> 8.0.8-113
- 7.5.2-304 -> 8.0.8-113
- 7.5.2-306 -> 7.7.0-761 -> 8.0.7-142
- 7.5.2-351 -> 8.0.6-119
- 7.5.2-501 -> 8.0.7-142
- 7.5.7-040 -> 7.5.7-048 -> 8.0.7-142
- 7.5.7-048 -> 8-0.7-142
- 7.7.0-219 -> 7.7.0-233 -> 8.5.2-027[1]
- 7.7.0-223 -> 7.7.0-500 -> 8.5.2-027[1]
- 7.7.0-327 -> 7.7.0-500 -> 8.5.2-027[1]
- 7.7.0-389 -> 7.7.0-500 -> 8.5.2-027[1]
- 7.7.0-487 -> 7.7.0-500 -> 8.5.2-027[1]
- 7.7.0-500 -> 8.5.2-027[1]
- 7.7.0-608 -> 8.5.2-027[1]
- 7.7.0-706 -> 8.5.2-027[1]
- 7.7.0-710 -> 8.5.2-027[1]
- 7.7.0-725 -> 8.5.2-027[1]
- 7.7.0-736 ->
- 7.7.0-744 8.5.2-027[1]
- 7.7.0-753 -> 8.0.6-119 -> or 8.5.2-027[1]
- 7.7.0-757 -> 8.0.6-119 -> or 8.5.2-027[1]
- 7.7.0-760 -> 8.5.2-027[1]
- 7.7.0-761 -> 8.0.6-119 -> or 8.5.2-027[1]
- 8.0.0-408 -> 8.5.2-027[1]
- 8.0.0-503 -> 8.5.2-027[1]
- 8.0.5-075 -> 8.5.2-027[1]
- 8.0.5-079 -> 8.5.2-027[1]
- 8.0.5-082
- 8.0.6-053 -> 8.5.2-027[1]
- 8.0.6-078 -> 8.5.2-027[1]
- 8.0.6-101 -> 8.5.2-027[1]
- 8.0.6-119 -> 8.5.2-027[1]
- 8.0.6-123 -> 8.5.2-027[1]
- 8.0.6-126 -> 8.5.2-027[1]
- 8.0.7-142 -> 8.5.2-027[1]
- 8.0.7-149 -> 8.5.2-027[1]
- 8.1.0-117 -> 8.1.0-235 -> 8.5.2-027[1]
- 8.1.0-228 -> 8.1.0-235 -> 8.5.2-027[1]
- 8.1.0-235 -> 8.5.2-027[1]
- 8.5.0-333 -> 8.5.0-389
- 8.5.0-389 -> 8.5.2-027[1]
- 8.5.0-497 -> 8.5.2-027[1]
- 8.5.1-019 -> 8.5.2-027[1]
- 8.5.1-021
- 8.5.1-022 -> 8.5.2-027[1]
- 8.5.2-024 -> 8.5.2-027[1]

[1] You cannot upgrade to 8.5.3-069 from 8.5.2-027 with the CLI command if you want to use either the save-password or email-configuration options. We recommend using the Web interface. [CSCuu81990]

Upgrading to Release 8.5.2-027 (MD)

Before you start the upgrade process, see Installation and Upgrade Notes, page 10.

You can upgrade to release 8.5.2-027 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
- 8-0-7-149
- 8-1-0-235
- 8-1-0-245
- 8-5-0-389
- 8-5-0-390
- 8-5-0-476
- 8-5-0-497
- 8-5-1-019
- 8-5-1-021
- 8-5-2-024

Upgrading to Release 8.5.1-021 (GD)

Before you start the upgrade process, see Installation and Upgrade Notes, page 10.

You can upgrade to release 8.5.1-021 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
- 8-5-0-497
- 8-5-1-019

Upgrading to Release 8.5.1-019 (MR)

Before you start the upgrade process, see Installation and Upgrade Notes, page 10.

You can upgrade to release 8.5.1-019 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
- 8-5-0-497

Upgrading to Release 8.5.0-497

Before you start the upgrade process, see Installation and Upgrade Notes, page 10.

You can upgrade to release 8.5.0-497 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

- 8-1-0-235
- 8-1-0-245

- 8-5-0-389
- 8-5-0-390
- 8-5-0-476

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."

Installation and Upgrade Notes

- Compatibility Details
- Deploying a Virtual Appliance
- Configuration Files
- 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 12.

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.

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.

Cisco does not generally support the backward compatibility of configuration files with previous major releases. Minor release support is provided. Configuration files from previous versions may work with later releases; however, they may require modification to load. Check with Cisco Customer Support if you have any questions about configuration file support.

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.x.

Post-Upgrade Reboot

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

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.

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.

- McAfee Engine Changes, page 13
- List of Available Upgrades, page 13
- Support Requests Require CCO ID and Support Contract, page 13
- New Certificate Management Page, page 14
- Exporting Web Tracking Data, page 14
- SNMP Monitoring, page 14
- X-Authenticated-Groups Header Format, page 14

McAfee Engine Changes

From AsyncOS 8.5.4-038 and later, 64-bit version of McAfee anti-virus scanning engine is supported.

List of Available Upgrades

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

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

In order to open a support request from the appliance, you must now enter a CCO ID and a support contract ID.

New Certificate Management Page

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

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

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 10.

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.

Next Steps

See Post-Upgrade Notes, page 15.

Post-Upgrade Notes

Log Subscription Changes

If you have configured the retrieval method of a log file as **Syslog Push**, after upgrading to AsyncOS 8.5.4-038, the value of the **Maximum message size** field is reset to `1024`. After the upgrade, reconfigure the value of the **Maximum message size** field to the original value (as configured prior to the upgrade). To configure this field,

1. Go to **System Administration** > **Log Subscriptions**.
2. Click on the log name and modify the value the **Maximum message size** field under the **Syslog Push** section.
3. Submit and commit the changes.

Documentation Updates

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

Adding JavaScript to End-User Notifications

If you need to add standard JavaScript to end-user notifications of any type, follow instructions in the user guide or online help for editing notification page HTML files. (JavaScript entered into the Custom Message box for notifications in the web user interface will be stripped out.) Be sure to test your script first in supported client browsers to ensure that it works as expected.

SOCKS Proxy Notes

The following notes were restored to the AsyncOS 9.0.1 User Guide:

- The SOCKS protocol only supports direct forward connections.
- The SOCKS proxy does not support (will not forward to) upstream proxies.

- The SOCKS proxy does not support scanning services, which are used by Application Visibility and Control (AVC), Data Loss Prevention (DLP), and malware detection.
- The SOCKS proxy does not support policy tracing.
- The SOCKS proxy does not decrypt SSL traffic; it tunnels from client to server.

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.

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

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 8.5.4-038 (MD), page 17
- Known and Fixed Issues in Release 8.5.3-069 (GD), page 17
- Known and Fixed Issues in Release 8.5.2-027 (MD), page 17
- Known and Fixed Issues in Release 8.5.1-021 (GD), page 17
- Fixed Issues in Release 8.5.1-019 (MR), page 17
- Known and Fixed Issues in Release 8.5.0-497, page 17

Known and Fixed Issues in Release 8.5.4-038 (MD)

Known issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.4&sb=afr&sts=open&svr=3nH&bt=custV
Fixed issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.4-038&sb=fr&svr=3nH&bt=empCustV

Known and Fixed Issues in Release 8.5.3-069 (GD)

Known issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.3&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV
Fixed issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.3-069&sb=fr&svr=3nH&srtBy=byRel&bt=custV

Known and Fixed Issues in Release 8.5.2-027 (MD)

Known issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.2&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV
Fixed issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.2-027&sb=fr&svr=3nH&srtBy=byRel&bt=custV

Known and Fixed Issues in Release 8.5.1-021 (GD)

Known issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.1&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV
Fixed issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.1-021&sb=fr&svr=3nH&srtBy=byRel&bt=custV

Fixed Issues in Release 8.5.1-019 (MR)

Fixed issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.1-019&sb=fr&svr=3nH&srtBy=byRel&bt=custV

Known and Fixed Issues in Release 8.5.0-497

Known issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.0&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV
Fixed issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.5.0-497&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

Note To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.

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

Support site for legacy IronPort: 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.