



Release Notes for Cisco AsyncOS 8.5 for Email

Updated: March 14, 2014

Contents

- [What's New, page 2](#)
- [Changes in Behavior, page 5](#)
- [Upgrade Paths, page 6](#)
- [Installation and Upgrade Notes, page 6](#)
- [Documentation Updates, page 9](#)
- [Resolved Issues, page 9](#)
- [Known Issues, page 10](#)
- [Finding Information about Known and Resolved Issues, page 11](#)
- [Related Documentation, page 12](#)
- [Service and Support, page 12](#)



What's New

Feature	Description
New Features	
URL filtering	<p>URL filtering obtains the reputation and category of URLs in incoming and outgoing messages to allow several new functionalities:</p> <ul style="list-style-type: none"> • Anti-spam and outbreak filters now use the reputation and category of URLs in messages to help determine if a message is spam or malicious. This additional data improves the filtering accuracy for messages that contain URLs. • You can further reduce the threat from potentially malicious sites by modifying URLs in delivered messages. You can make URLs unclickable, replace them with text, or redirect them to a proxy that evaluates the safety of a site if and when the recipient clicks the link, and blocks transactions it deems unsafe. You can create content and message filters to modify URLs based on categories of URL that are likely to be problematic. • You can create content and message filters to enforce acceptable use policies based on the category of URLs in messages. For example, you can drop messages that include links in the Illegal Activities category. <p>For more information, see the Documentation Updates section below and the new URL Filtering chapter in the user guide or online help.</p>
DMARC Verification	<p>You can now:</p> <ul style="list-style-type: none"> • Verify incoming emails using DMARC. • Define policies to override (accept, quarantine, or reject) domain owners' policies. • Send DMARC aggregate feedback reports to domain owners that helps to strengthen their authentication deployments. • Send delivery error reports to the domain owners if the DMARC aggregate report size exceeds 10 MB or the size specified in the RUA tag of DMARC record.
Rule for detecting high volume mail attacks	<p>AsyncOS now includes a new rule, Header Repeats (<code>header-repeats</code>) rule, for detecting high volume mail attacks. When used in message filters, the Header Repeats rule evaluates to <code>true</code> if at a given point in time, a specified number of messages:</p> <ul style="list-style-type: none"> • With same subject are detected in the last one hour. • From same envelope sender are detected in the last one hour.
Upgrade notification	<p>A notification now appears at the top of the web interface when a new AsyncOS upgrade is available.</p>

Feature	Description
Virtual appliance support	<ul style="list-style-type: none"> The following deployment options are now supported: <ul style="list-style-type: none"> Deployments with VMWare ESXi5.1 hypervisor Deployment as part of a FlexPod solution For general information about FlexPod, see http://www.cisco.com/en/US/netsol/ns1137/index.html. Feature keys for individual features can have earlier expiration dates than the virtual appliance license, which expires on the date of the latest-expiring feature key. Virtual license expiration now includes a 180-day grace period, during which the appliance continues to deliver mail without security services.
Option to drop an email with corrupt attachment	You can now configure your content and message filters to drop emails containing corrupt attachments.
Envelope language	<p>If you are using Cisco Registered Envelope Service for email encryption, you can change the locale of the envelope to any one of the following locales:</p> <ul style="list-style-type: none"> English French German Spanish Portuguese Japanese <p>Note This feature will not be available at FCS, but will be available some time thereafter.</p>
Provision and activate Cisco Registered Envelope Service administrator from the appliance	<p>For physical hardware appliances, you can now provision and activate Cisco Registered Envelope Service administrator. The appliance prompts you to enter the email address of the encryption account administrator. When you provision an Encryption Profile, this email address is registered automatically with the encryption server.</p> <p>For virtual appliances, see Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances, page 6.</p>
Stochastic sampling	If IronPort Anti-Spam or Intelligent Multi-Scan feature keys are active and SenderBase Network Participation is enabled, AsyncOS sends a random sample of messages normally dropped by poor reputation to CASE for Antispam scanning. CASE scans these messages and uses the results to improve the efficacy of the product.
No Operation message filter action	<p>AsyncOS now includes a new message filter action, No Operation (<code>no-op</code>). The No Operation action performs a no-op, or no operation.</p> <p>You can use this action in a message filter if you do not want to use any of the other actions such as Notify, Quarantine, or Drop. For example, to understand the behavior of a new message filter that you created, you can use the No Operation action. After the message filter is operational, you can monitor the behavior of the new message filter using the Message Filters report page, and fine-tune the filter to match your requirements.</p>

Feature	Description
Enhancements	
Spam quarantine improvements	<ul style="list-style-type: none"> • You can now choose whether to require end users to log in when they access the end user quarantine via a link in a notification. • You have more flexibility in scheduling the frequency and timing of notifications sent to end users about possible spam they receive. For example, you can now send notifications any day or days of the week and any hour or hours of the day. • Administrators can now view, search, add, edit, and delete safelist and blocklist entries.
Reporting and Tracking enhancement	Click links in reports to view the Message Tracking data for messages that are included in the report. This enhancement will simplify identification of problems, investigation of patterns, and testing of system and configurations.
Graphical User Interface for configuring Scan Behavior and SSL Settings	Prior to this release, Scan Behavior and SSL Settings could be configured only using CLI. You can now configure Scan Behavior and SSL Settings using web interface and CLI.
Outbreak Filter Enhancements	<p>Using the enhanced Outbreak Filter, you can:</p> <ul style="list-style-type: none"> • Add the following additional email headers to the Outbreak Filters: <ul style="list-style-type: none"> – X-IronPort-Outbreak-Status – X-IronPort-Outbreak-Description • Filter emails using the new email headers. • Perform a content filter-based scan on the Outbreak Filter processed messages by configuring Outbreak Filters to send the processed emails to an alternate destination mail host, Email Security Appliance. • Alter email subject line and body using the following Outbreak Filters variables: <ul style="list-style-type: none"> – \$threat_verdict – \$threat_category – \$threat_type – \$threat_description – \$threat_level • Configure Outbreak Filters to deliver emails immediately without adding them to quarantine. • Use the following new reports: <ul style="list-style-type: none"> – Hit Messages from Incoming Messages – Hit Messages by Threat Level – Messages resided in Outbreak Quarantine – Top URLs Rewritten

Feature	Description
Suspend and resume mail delivery to specific domains and subdomains	You can now suspend and resume mail delivery to specific domains and subdomains.
Password security enhancements	You can set the following options for administrative user passwords: <ul style="list-style-type: none"> • Show a password strength indicator to a user entering a new password. (Password strength is enforced by the other password requirements that you specify.) • Disallow certain words in passwords. (You upload a list of forbidden words to the appliance.)
Loading configuration in clustered appliances	You can now load configuration in clustered appliances in the following scenarios: <ul style="list-style-type: none"> • If you are migrating from on-premise environment to hosted environment and you want to migrate the on-premise cluster configuration to the hosted environment. • If an appliance in a cluster is down or needs to be retired and you want to load the configuration from this appliance to a new appliance that you plan to add to the cluster. • If you want to load a backed up configuration to a cluster.

Changes in Behavior

- [Accessing the Sender Group Report, page 5](#)
- [Feature Key for Centralized Management, page 5](#)
- [Revised Threshold Levels for Entering Resource Conservation Mode, page 5](#)

Accessing the Sender Group Report

You can now access the Sender Group report directly from the Monitor menu; the link has been removed from the bottom of the Incoming Mail report page.

Feature Key for Centralized Management

Feature key is no longer required to enable Centralized Management feature. By default, Centralized Management feature is enabled on your appliance.

Revised Threshold Levels for Entering Resource Conservation Mode

Prior to this release, Email Security appliance enters resource conservation mode when the RAM utilization exceeds 75% and the allowed injection rate is gradually decreased as RAM utilization approaches 85%.

From version 8.0 onwards, AsyncOS for Email is a 64-bit software. As a result of this changed memory model, the threshold values are revised in this release. Appliance enters resource conservation mode when the RAM utilization exceeds 45% and the allowed injection rate is gradually decreased as RAM utilization approaches 60%. This change does not affect the memory utilization on the appliance and all the components in the appliance continue to use the memory as earlier.

**Caution**

Appliances with large memory utilization, especially with large system quarantine, can enter resource conservation immediately after upgrading to AsyncOS 8.5 for Email. To avoid this scenario, make sure that you reduce the system quarantine to a few thousand messages before upgrading.

Upgrade Paths

You can upgrade to release 8.5.0-473 from the following versions:

- 7.6.3-019
- 7.8.0-360
- 8.0.1-023

To ensure a successful upgrade, you must complete some steps before you start the upgrade process. For details on these prerequisites, see [“Installation and Upgrade Notes” section on page 6](#).

Installation and Upgrade Notes

Read through and consider the installation and upgrade impacts listed in this section.

When you upgrade AsyncOS for Email 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.

You must be logged in as the admin to upgrade. Also, you must reboot the appliance after upgrading.

Deploying a Virtual Appliance

If you are deploying a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*.

If you are switching from a physical appliance to a virtual appliance, you will need to convert your configuration file to an AsyncOS 8.0 virtual appliance configuration file. For information, see the *Release Notes for Configuration Migration Tool 1.0 for Cisco Content Security Virtual Appliances*. You can import the AsyncOS 8.0 virtual appliance configuration file into a virtual appliance running AsyncOS 8.5.

Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances

Please contact Cisco TAC for information required to provision your virtual appliance.

Pre-upgrade Notes

Please be aware of the following upgrade impacts:

- [Email Authentication, page 7](#)
- [Configuration Files, page 7](#)
- [Received Headers, page 7](#)
- [Feature Keys, page 7](#)
- [Resource Conservation Mode, page 8](#)

Email Authentication

For DKIM Authentication, Cisco currently supports version 8 of the Draft Specification of 'Authentication-Results:' header.

For SPF/SIDF verification, the `spf-passed` rule is no longer available in content filters. To maintain backwards compatibility, the **spf-passed** content filter rule will be accepted from XML configuration files but it will be converted to the **spf-status** rule with corresponding arguments. **spf-passed** will be changed to **spf-status == "Pass"** and **NOT spf-passed** to **spf-status != "Pass"**. You can, however, still use the `spf-passed` message filter.

Configuration Files

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.

Received Headers

When you configure AsyncOS to use received headers, you can specify that the header reflects one of the following hostnames:

- The hostname of the Virtual Gateway used for delivering the message
- The hostname of the interface the message is received on

You specify the hostname from the CLI command **listenerconfig-> setup**. You cannot configure the hostname from the web interface.

If you configure the received header to display the hostname of the interface the message is received on, a **strip-header** filter action configured to strip received headers will strip the received header inserted by AsyncOS.

Feature Keys

The AsyncOS appliance checks for and applies feature keys at one minute intervals. Therefore, when you add a feature key, it may take up to a minute to view the changes.

Resource Conservation Mode

From AsyncOS 8.5 for Email, Email Security appliance will enter resource conservation mode when the RAM utilization exceeds 45% and the allowed injection rate is gradually decreased as RAM utilization approaches 60%. Appliances with large memory utilization, especially with large system quarantine, can enter resource conservation immediately after upgrading to AsyncOS 8.5 for Email. To avoid this scenario, make sure that you reduce the system quarantine to a few thousand messages before upgrading.

Upgrading to Cisco AsyncOS 8.5 for Email Release

Before You Begin

Review the [Known Issues, page 10](#) and [Installation and Upgrade Notes, page 6](#).

Procedure

Use the following instructions to upgrade your Email Security appliance.

-
- Step 1** Save the XML configuration file off the IronPort appliance.
 - Step 2** If you are using the Safelist/Blocklist feature, export the Safelist/Blocklist database off the appliance.
 - Step 3** Suspend all listeners.
 - Step 4** Wait for the queue to empty.
 - Step 5** From the System Administration tab, select the System Upgrade page.
 - Step 6** Click the **Available Upgrades** button. The page refreshes with a list of available AsyncOS upgrade versions.
 - Step 7** Click the **Begin Upgrade** button and your upgrade will begin. Answer the questions as they appear.
 - Step 8** When the upgrade is complete, click the **Reboot Now** button to reboot your IronPort appliance.
 - Step 9** Resume all listeners.
-

Performance Advisory

RSA Email DLP - Enabling RSA Email DLP for outbound traffic on an appliance that is also running anti-spam and anti-virus scanning on inbound traffic can cause a performance decrease of less than 10%. Appliances that are only running outbound messages and are not running anti-spam and anti-virus may experience a significant performance decline.

DomainKeys - DomainKeys signing outgoing email can cause a decrease in the message throughput capacity. Using smaller signing keys (512 byte or 768 byte) can mitigate this.

SBNP - SenderBase Network Participation now uses the Context Adaptive Scanning Engine (CASE) to collect data to power IronPort Information Services. In some configurations customers may experience a moderate performance decline.

Outbreak Filters - Outbreak Filters uses the Context Adaptive Scanning Engine to determine the threat level of a message and scores messages based on a combination of Adaptive Rules and Outbreak Rules. In some configurations, you may experience a moderate performance decline.

IronPort Spam Quarantine - Enabling the IronPort Spam Quarantine on-box for a C-Series or X-Series appliance causes a minimal reduction in system throughput for nominally loaded appliances. For appliances that are running near or at peak throughput, the additional load from an active quarantine may cause a throughput reduction of 10-20%. If your system is at or near capacity, and you desire to use the IronPort Spam Quarantine, consider migrating to a larger C-Series appliance or an M-Series appliance.

If you change your anti-spam policy from dropping spam to quarantining it (either on-box or off-box), then your system load will increase due to the need to scan additional spam messages for virus and content security. For assistance in properly sizing your installation please contact your authorized IronPort support provider.

Documentation Updates

Opening Required Firewall Ports for URL Filtering Features

The following information supplements the information in the Firewall topic in the online help and appears in the Firewall appendix in the User Guide PDF.

The hostname for the web security service is available via the command-line interface. Run the `websecurityadvancedconfig` command and accept all defaults. Look for the "Web security service" hostname.

Certificates for URL Filtering Features

AsyncOS is designed to automatically deploy and update the certificates needed for communications with cloud services used for URL filtering features. However, if for any reason the system is unable to update these certificates, you will receive an alert that requires action from you.

To ensure that you receive these alerts (System type, Warning severity), see information in the online help or user guide about adding alert recipients.

If you receive an alert about an invalid certificate, contact Cisco TAC, which can provide the required replacement certificate. Instructions for installing the certificate are in the URL Filtering chapter in the online help or user guide.

For details about the connection between the appliance and the cloud URL reputation and category services, see the URL Filtering chapter of the user guide or online help.

Resolved Issues

**Note**

To view a complete list of resolved issues in this release, see [Finding Information about Known and Resolved Issues, page 11](#).

Reference Number	Description
CSCui89551	When clicking on links rewritten by non-viral threat Outbreak Filters, secure-web.cisco.com returns a 403 Forbidden response intermittently.
CSCul44164	When non-viral threat Outbreak Filters rewrites a URL, the special character - ampersand is not translated correctly. As a result, the rewritten URL will not work as expected.
CSCzv06682	SNMP traps are not sent out for RAID status changes.
CSCzv12021	Using a single backslash in LDAP filter causes an application fault.
CSCzv38250	IP addresses are lost when reconfiguring network settings.
CSCzv57037	Some emails sent from Email Security appliance have empty headers.
CSCzv63347	Firewall rule for numerically lowest IP address of Email Security appliance fails.
CSCzv91451	Unable to establish a secure support tunnel if the host is not DNS resolvable.
CSCzv97281	AsyncOS creates an unwanted process after every SenderBase upload.

Known Issues



Note

To view a complete list of known issues in this release, see [Finding Information about Known and Resolved Issues](#), page 11.

Reference Number	Description
CSCuj71189	Inline images are shown as attachments on CRES encrypted messages. Workaround: Not available
CSCul76921	Cisco Web Security Services connection status on URL Filtering page does not show the connection status of the cluster. Workaround: Not available
CSCul77260	URL on the first line of the message body is not detected by URL Filter in Trace. Workaround: Add a newline or a text before the URL.
CSCum64395	On Overview report page, the Message with Malicious URLs is subsumed under other message categories and is not considered in the Total Attempted Messages count. Workaround: Not available
CSCun02358	Auto provision of encryption profiles does not work on virtual Email Security appliances. Workaround: Contact the customer support to add the serial number of the Virtual appliance to the CRES server.

Reference Number	Description
CSCun06341	Some of the Outbreak Filter rewritten URLs are not working. Workaround: Not available
CSCun27984	Grace period for incoming mail handling does not work after upgrading from AsyncOS 8.0.x for Email to AsyncOS 8.5.0 for Email. Workaround: After upgrading to AsyncOS 8.5.0 Email, reload the VLN XML license file by running the CLI command <code>loadlicense</code> .
CSCun30538	Unable to load the cluster configuration using Internet Explorer. When loading the cluster configuration, you are prompted to save a <code>.json</code> file or the next window does not appear. Workaround: Use other supported browsers such as Mozilla Firefox or Google Chrome to load the cluster configuration.
CSCun33155	The final message in trace contains 'http://' instead of rewritten URLs. This problem occurs when you run a trace with a message that contains URLs in the body that belong to the URL category selected in the content or message filter and this filter has a redirect action to Cisco Security Proxy. Workaround: Not available
CSCzv15563	AsyncOS for Email sends out an alert to the user stating that the Sophos Engine has expired. This occurs when you upgrade to the latest version of AsyncOS for Email with an expired Sophos Engine. Workaround: You can ignore this alert. After the upgrade, auto-update will download and update the Sophos Engine to the latest available version.

Finding Information about Known and Resolved Issues

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

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 > Email Security > Cisco Email Security Appliance**, and click **OK**.
 - Step 4** In Releases field, enter **8.5.0**.
 - 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



Note

For the most current and complete documentation, see the PDF version of the user guide. Online help may not include the most current and complete information.

The documentation for the Email Security appliance includes the following books:

- Cisco AsyncOS for Email User Guide*
- Cisco Content Security Virtual Appliance Installation Guide*
- Cisco AsyncOS CLI Reference Guide*

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.
Cisco Email Security	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco Web Security	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
Cisco Content Security Management	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
CLI reference guide for Cisco Content Security appliances	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco IronPort Encryption	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

Service and Support

Use the following methods to obtain support:

U.S.: Call 1 (408) 526-7209 or Toll-free 1 (800) 553-2447

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

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2014 Cisco Systems, Inc. All rights reserved.