Release Notes for Cisco AsyncOS 8.5.5 for Email

Published: March 20. 2014

Revised: June 2, 2014

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

What's New in Cisco AsyncOS 8.5.5 for Email

Feature	Description
File Reputation Filtering and File Analysis	Advanced Malware Protection identifies emerging and targeted file-based threats in downloaded files based on: • File reputation • File analysis (for certain files with unknown reputations) • Updated verdicts after a file has been released to the network As new information becomes available about files, threat verdicts are updated, providing you with a starting point for investigating threats that were received before they were known even to the Advanced Malware Protection services. New reports identify infected files found by reputation, provide status and outcome of files sent for analysis, and list files for which verdicts have been updated. Existing reports have been updated with new sections or table columns to let you research users, sites, and trends involving infected files.

What's New in Cisco AsyncOS 8.5.0 for Email

Feature	Description
New Features	
URL filtering	URL filtering obtains the reputation and category of URLs in incoming and outgoing messages to allow several new functionalities: • 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. For more information, see Documentation Updates, page 10 and the new URL Filtering chapter in the user guide or online help.

Feature	Description
DMARC Verification	You can now: • 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	AsyncOS now includes a new rule, Header Repeats (`header-repeats`) rule, for detecting high volume mail attacks. When used in message filters, the Header Repeats rule evaluates to `true` if at a given point in time, a specified number of messages: • With same subject are detected in the last one hour. • From same envelope sender are detected in the last one hour.
Upgrade notification	A notification now appears at the top of the web interface when a new AsyncOS upgrade is available.
Virtual appliance support	• The following deployment options are now supported: – 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. • 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	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: • English • French • German • Spanish • Portuguese • Japanese **Note** This feature will not be available at FCS, but will be available some time thereafter.

Feature	Description
Provision and activate Cisco Registered Envelope Service administrator from the appliance	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. For virtual appliances, see Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances, page 7.
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	AsyncOS now includes a new message filter action, No Operation (`no-op`). The No Operation action performs a no-op, or no operation. 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.
Enhancements	
Spam quarantine improvements	• 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 the web interface or the CLI.

Feature	Description
Outbreak Filter Enhancements	Using the enhanced Outbreak Filter, you can: • Add the following additional email headers to the Outbreak Filters: – 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: – `$threat_verdict` – `$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: – Hit Messages from Incoming Messages – Hit Messages by Threat Level – Messages resided in Outbreak Quarantine – Top URLs Rewritten
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: • 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.)

Feature	Description
Loading configuration in clustered appliances	You can now load configuration in clustered appliances in the following scenarios: • 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.

See also Changes in Behavior, page 10.

Upgrade Paths

You can upgrade to release 8.5.5-280 from the following versions:

- 8.5.0.473
- 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 7.

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 8
- Configuration Files, page 8
- Received Headers, page 8
- Feature Keys, page 8
- 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.x 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.x for Email. To avoid this scenario, make sure that you reduce the system quarantine to a few thousand messages before upgrading.

Upgrading to This Release

Before You Begin

Review the Known Issues, page 12 and Installation and Upgrade Notes, page 7.

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.

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

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 15.

Information about other resources, including the knowledge base and Cisco support community, is in the online help and the User Guide PDF.

About Using a Proxy for Communications with Advanced Malware Protection Cloud Services

Using a proxy is not supported for communications between the Email Security appliance and the file reputation and file analysis services in the cloud, even if an upstream proxy is transparent to the Email Security appliance.

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.

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.

Changes in Behavior

- Accessing the Sender Group Report, page 11

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 this release. To avoid this scenario, make sure that you reduce the system quarantine to a few thousand messages before upgrading.

Resolved Issues

Resolved Issues in Release 8.5.5

Reference Number	Description
CSCun27984	Fixed: 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.

Resolved Issues in Release 8.5.0

Note To view a complete list of resolved issues in this release, see Finding Information about Known and Resolved Issues, page 14.

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

Known Issues

Note To view a complete list of known issues in a release, see Finding Information about Known and Resolved Issues, page 14.

Known Issues in Release 8.5.5

Reference Number	Description
CSCuo97941	Some messages are not encrypted as expected. This can occur if "TLS Required - Verify Hosted Domains" is enabled for the Destination Domain and the destination Mail Transfer Agent (MTA) does not offer STARTTLS. **Workaround**: Do not enable "TLS Required - Verify Hosted Domains."
CSCun56438 CSCun76012	Alerts about Python restart. This occurs only on C170 models, and can occur when: • connectivity to the cloud is lost • a large number of files is simultaneously uploaded for analysis Workaround: None
CSCun00532	Some SHA values are not displayed in the Completed section of the file analysis reports page Workaround: None
CSCun76637	If the File analysis feature key is renewed before the File reputation key is renewed, the file reputation service does not function. Workaround: On the Security Services > File Reputation and Analysis page, disable and then Enable Advanced Malware Protection.
CSCun48177	In cluster mode, File analysis should be disabled by default while enabling Advanced Malware Protection. Workaround: None
CSCum93237	In cluster mode, File Analysis settings cannot be edited on an appliance with an expired feature key. Workaround: Login from an Email Security appliance where the feature key is not expired and edit the File Analysis settings.

Known Issues in Release 8.5.0

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.

Reference Number	Description
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.
CSCun06341	Some of the Outbreak Filter rewritten URLs are not working. **Workaround**: Not available
CSCun30538	Unable to load the cluster configuration using Internet Explorer. When loading the cluster configuration, you are prompted to save a `.json` 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

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/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web Security	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Content Security Management	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
CLI reference guide for Cisco Content Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/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.