Release Notes for AsyncOS 10.0 for Cisco Email Security Appliances

Published: June 20, 2016
Revised: October 6, 2016

Contents

What's New In This Release

Feature	Description
Office 365 Mailbox Auto Remediation	A file can turn malicious anytime, even after it has reached user's mailbox. AMP can identify this as new information emerges and push retrospective alerts to your appliance. With this release you get more than just alerting. If your organization is using Office 365 to manage mailboxes, you can configure your appliance to perform auto-remedial actions on the messages in user mailbox when the threat verdict changes. See the "Automatically Remediating Messages in Office 365 Mailboxes" chapter in the user guide or online help.

Cisco Systems, Inc.
www.cisco.com

Detecting Forged Messages (also known as spoofing, CEO fraud, or business email compromise)	Cisco Email Security appliance can detect fraudulent messages with forged sender address (From: header) and perform actions on such messages. See the "Email Authentication" chapter in the user guide or online help.
Support for On-Premises File Reputation Server	If you have deployed a Cisco AMP Virtual Private Cloud appliance on your network, you can now query the file reputation of message attachments without sending them to the public reputation cloud. To configure your appliance to use an on-premises file reputation server, see the "File Reputation Filtering and File Analysis" chapter in the user guide or online help.
Cloud Updatable Advanced Malware Protection Engine	• The Advanced Malware Protection engine is now cloud updatable. • You can use the `ampstatus` command in CLI to view the version of various Advanced Malware Protection components. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Virtual Appliance Enhancement	Cisco Email Security virtual appliances can now be deployed on VMware vSphere Hypervisor (ESXi) 6.0. For more information, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from: http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.
Duplicate Boundaries Verification	Cisco Email Security appliance can now detect messages with duplicate MIME boundaries and perform actions on them. Use the Duplicate Boundaries Verification content filter condition or the `duplicate_boundaries` message filter rule to detect messages with duplicate MIME boundaries. See the "Content Filters" chapter or the "Using Message Filters to Enforce Email Policies" chapter in the user guide or online help.
Cisco Email Submission and Tracking Portal Registration	Cisco Email Submission and Tracking Portal is a web-based tool that allows email administrators to track the spam submissions from their organization and to report new misclassified messages to Cisco. This portal requires all your appliances to have a common registration ID. Use the **System Administration > Email Submission and Tracking Portal Registration** page in web interface or the `portalregistrationconfig` command in CLI to set the registration ID. If your appliances are not part of a cluster, you must set a common registration ID on all your appliances. See the "Anti-Spam" chapter in the user guide or online help.

Enhanced AMP Reports	**Advanced Malware Protection** page includes the following enhancements: • A new graph that shows the incoming files handled by AMP in percentage based on the verdicts (Clean, Malicious, Unknown, Unscannable). • A new graph that shows the top incoming malware files based on the file types. • A new table that shows the number of incoming files handled by AMP based on the verdicts (Clean, Malicious, Unknown, Unscannable). Click on the file count to view the related messages in Message Tracking. • Incoming Malware Threat Files Report – Incoming Malware Threat Files report now shows the name of the file(s) associated with a SHA-256 hash. – If you click on a SHA-256 hash, a new page that shows file reputation and analysis summary for the specified SHA-256 hash is displayed. – Click on the number of infected messages to view the related messages in Message Tracking. **File Analysis** page includes the following enhancements: • Completed Analysis Requests from This Appliance and Pending Analysis Requests from This Appliance reports include the following enhancements: – Reports now show the name of the file(s) associated with a SHA-256 hash. – Click on **Details** to view the related messages in Message Tracking. • A new report that shows the number of files uploaded for file analysis. **AMP Verdict Updates** page includes the following enhancements: • Files with Retrospective Verdict Changes report now shows the name of the file(s) associated with a SHA-256 hash. • Files with Retrospective Verdict Changes report now shows the old disposition for a given SHA-256 hash. • If you click on a SHA-256 hash, a new page that shows file analysis summary for the specified SHA-256 hash is displayed. • Click on **Details** to view the related messages in Message Tracking.
Spam Quarantine Enhancement	You can now send notifications to end users that list new quarantined messages without displaying the message subject. To view the message subject, end users must click the link and view the message in the spam quarantine. You can achieve this using the new notification variable **`New Message Table without Subject`**. See the "Spam Quarantine" chapter in the user guide or online help.

Message Tracking Details for URLs in Messages	Users can now view finer details about URLs caught by content and outbreak filters. Administrators can configure which users can see this information. See the "Message Tracking" chapter in the user guide or online help.
Content Filter Condition and Message Filter Rule to Detect Message Language	You can now use the content and message filters to detect the language of the message (subject and body) and take different actions based on the message language. See the "Content Filters" chapter or the "Using Message Filters to Enforce Email Policies" chapter in the user guide or online help.
Custom Bounce and Delay Warning Messages Based on Language of the Message	While configuring a bounce profile (**Network > Bounce Profiles**), you can now configure custom bounce and delay warning messages based on the language of the original message. See the "Configuring Routing and Delivery Features" chapter in the user guide or online help.
Support for 90-Series Hardware	Support for new appliance models: • C190 • C390 • C690
Enhanced Verdict Update Alert	Alert for file reputation verdict changes is now enhanced to include additional details such as details of the message, spyname, and so on.
Using From Header for DKIM Signing	You can now use the DKIM Global Settings (Mail Policies > Signing Profiles) to choose whether to use From header for DKIM signing. For DMARC verification of DKIM signed messages, you must use the From header during DKIM signing. See the "Email Authentication" chapter in the user guide or online help.
Message Filter Rule to Detect Malformed MIME Headers	You can now take actions on messages with malformed MIME headers using the new message filter rule: "`malformed-header`." See the "Using Message Filters to Enforce Email Policies" chapter in the user guide or online help.

Changes in Behavior

Advanced Malware Protection Behavior Changes	• If a message has malformed headers, the appliance will attempt to extract the attachments from the message. If the extracted messages are found to be malicious, the file reputation verdict is set to "malicious." If the appliance is unable to extract the attachments, the file reputation verdict is set to "unscannable." • The file reputation verdict for a message without any attachments is set to "skipped."
Advanced Malware Protection and File Analysis Reports Prior to the Upgrade	Advanced Malware Protection, File Analysis, and Verdict Updates reports are enhanced to display additional fields, graphs, and so on. The reports displayed after the upgrade do not include the reporting data prior to the upgrade. To view the reports prior to the upgrade, click on the hyperlink (`Click here to view reports prior to AsyncOS 10.0`) at the top of the report page.
Change in Report Page Name	File Analysis report page is renamed to Advanced Malware Protection File Analysis.
DKIM Signing of System Generated Messages	**DKIM Signing of System Generated Messages** option is now available under Mail Policies > Signing Profiles > DKIM Global Settings.
Graymail Changes	Prior to this release, if a message is graymail and outbreak filter positive, the actions configured for graymail are not applied after the message is released from the outbreak quarantine. The safe unsubscribe banner (if configured) is not added in this scenario. After upgrading to this release, the actions configured for graymail are applied after the message is released from the outbreak quarantine. The safe unsubscribe banner (if configured) is added in this scenario.
Advanced Malware Protection File Detail - Report Changes	• The content of Matching Signatures report on the Advanced Malware Protection File Analysis > File Detail page is merged with the Classification / Threat Score report. • The Classification / Threat Score report on the Advanced Malware Protection File Analysis > File Detail page is renamed to Behavioral Indicators. Also, this report now includes only the following details: – Indicators (formerly shown as Matching Signatures) – Category (formerly shown as Factor) – Threat Level
Change in SPF Verification Content and Message Filter Behavior	If you have configured an SPF verification content or message filter rule without an SPF identity and if a message contains different SPF identities with different verdicts, the rule is triggered if one of the verdicts in the message matches the rule.

Mail Policy Matching Logic Changes	Prior to this release, while matching a message to a mail policy, the envelope sender (RFC821 MAIL FROM address) and the sender header (address found in the RFC822 From and Reply-To) had the same priority. As a result, if you had configured a mail policy to match a specific user, the messages were classified into that mail policy based on the sender header. After upgrading to this release, when you match a message to a mail policy, the envelope sender and the envelope recipient have a higher priority over the sender header. If you configure a mail policy to match a specific user, then the messages are automatically classified into the mail policy based on the envelope sender and the envelope recipient.
Miscellaneous Disk Usage	After upgrading to this release, when Miscellaneous disk usage reaches 75 percent of the quota, the appliance immediately recalculates the disk usage to ensure that the usage has actually reached 75 percent and adds the following entry to the Mail Logs at Debug level: **`Disk quota for Miscellaneous services (logs, configuration file, and so on) is reaching its limit. Recomputing disk usage to double-check disk quota`**. After the recalculation, if the disk usage has reached 75 percent, an alert is sent. This process is repeated when Miscellaneous disk usage reaches 100 percent of the quota.
New Alert for Message Filter Crashes	When a message filter crashes, the appliance sends a system alert with a critical severity.
Password to Passphrase Change	The term “password” is changed to “passphrase” in web interface and command line interface.

Upgrade Paths

You can upgrade to release 10.0.0-203 from the following versions:

- 9.1.0-032
- 9.1.1-023
- 9.1.2-028
- 9.1.2-036
- 9.1.2-041
- 9.6.0-042
- 9.6.0-051
- 9.7.0-125
- 9.7.1-066
- 9.7.1-102
- 9.7.1-207
- 9.7.2-047
- 9.7.2-065
- 10.0.0-082

- 10.0.0-125
- 10.0.0-199

Caution If you plan to upgrade to AsyncOS 10.0.0-203, review the Reverting to Previous AsyncOS Versions, page 8.

Installation and Upgrade Notes

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

When you upgrade AsyncOS 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.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - C380, C390, C680, or C690
  - C170 or C190
  - Some C370, C370D, C670 or X1070 appliances

    To determine whether your appliance is supported, and to remedy the situation if it is not currently compatible, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html.

The following hardware is NOT supported for this release:

C160, C360, C660, and X1060

Deploying or Upgrading a Virtual Appliance

If you are deploying or upgrading a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

Upgrading a Virtual Appliance

If your current Virtual Appliance release does not support more than 2TB of disk space, and you want to use more than 2 TB of disk space with this release, you cannot simply upgrade your virtual appliance.

Instead, you must deploy a new virtual machine instance for this release.

When you upgrade a virtual appliance, the existing licenses remain unchanged.

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 or Upgrading a Virtual Appliance, page 7.

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.

Be sure to select an appropriate option related to network settings.

Getting Technical Support for Virtual Appliances

Requirements for obtaining technical support for your virtual appliance are described in the *Cisco Content Security Virtual Appliance Installation Guide* available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

See also Service and Support, page 13, below.

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

Before upgrading, review the following:

Reverting to Previous AsyncOS Versions

The following AsyncOS versions are affected by the Internal Testing Interface Vulnerability (http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa):

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047

- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

If you upgrade to AsyncOS 10.0.0-203 from one of the above versions, you cannot revert to any of the previous versions.

FIPS Compliance

AsyncOS 10.0 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 10.0.

Upgrading Deployments with Centralized Management (Clustered Appliances)

If a cluster includes C160, C360, C660, or X1060 hardware appliances, remove these appliances from the cluster before upgrading.

All machines in a cluster must be running the same version of AsyncOS, and x60 hardware cannot be upgraded to this release. If necessary, create a separate cluster for your x60 appliances.

Upgrading From a Release Other Than the Immediate Previous Release

If you are upgrading from a major (AsyncOS X.0) or minor (AsyncOS X.x) release other than the release immediately preceding this release, you should review the Release Notes for major and minor releases between your current release and this release.

Maintenance releases (AsyncOS X.x.x) include only bug fixes.

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.

IPMI Messages During Upgrade

If you are upgrading your appliance using CLI, you may observe messages related to IPMI. You can ignore these messages. This is a known issue.

Defect ID: CSCuz28415

Upgrading to This Release

Before You Begin

- Review the Known and Fixed Issues, page 11 and Installation and Upgrade Notes, page 7.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 7.

Procedure

Use the following instructions to upgrade your Email Security appliance.

Step 1 Save the XML configuration file off the 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 appliance.

Step 9 Resume all listeners.

What To Do Next

Review the Performance Advisory, page 10.

Performance Advisory

RSA Email DLP

- Enabling RSA Email DLP for outbound messages on an appliance that is already having anti-spam and anti-virus scanning running on inbound messages can cause a performance degradation of less than 10%.
- Enabling RSA Email DLP on an appliance that is only running outbound messages and is not running anti-spam and anti-virus can cause higher performance degradation as compared to the previous scenario.

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 support provider.

Known and Fixed Issues

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

- Bug Search Tool Requirements, page 11
- Lists of Known and Fixed Issues, page 11
- Finding Information about Known and Resolved Issues, page 11

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://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=10.0.0&sb=afr&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=10.0.0&sb=fr&bt=custV

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 the version of the release, for example, 10.0.

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 Content Security Management	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 Email Security	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

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

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

Support Site for legacy IronPort: http://www.cisco.com/web/services/acquisitions/ironport.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.