Release Notes for AsyncOS 9.0 for Cisco Email Security Appliances

Published: January 28, 2015

Revised: December 21, 2015

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

Feature	Description
New Features	
Release and Support Notifications	You can now receive software release and critical support notifications from Cisco Support (in the form of alerts).
S/MIME Security Services	AsyncOS for Email now allows organizations to communicate securely using S/MIME without requiring that all end-users possess their own certificates. Organizations can handle message signing, encryption, verification, and decryption at the gateway level using certificates that identify the organization rather than the individual. AsyncOS provides the following S/MIME security services: • Sign, encrypt, or sign and encrypt messages using S/MIME • Verify, decrypt, or decrypt and verify messages using S/MIME
Cisco AsyncOS API for Email	The Cisco AsyncOS API for Email (or AsyncOS API) is a Representational StateTransfer (REST)-based set of operations that provide secure and authenticated access to the Email Security appliance reports and report counters. You can retrieve the Email Security appliance reporting data using this API. See *Cisco AsyncOS API for Email - Getting Started Guide*.
File Analysis Quarantine	AsyncOS for Email now includes an Advanced Malware Protection-specific quarantine. You can configure the appliance to quarantine messages with attachments sent for analysis. Before upgrading to this release, see an important caveat at File Analysis Quarantine, page 10.
Enhancements	
Virtual Appliance enhancements	• Support for thin provisioning • Support for ESXi 5.5 • Access to more than 2 TB of disk space However, when upgrading a virtual appliance, an important caveat applies. See Upgrading a Virtual Appliance, page 8.
Customizable disk space	You can now allocate disk space on the appliance based on the functionality your organization uses (spam and system quarantines, reporting and tracking data, etc.) Previous limits on quarantine size have been removed. For virtual appliances, you can use VMWare tools to increase the disk space available to Email Security appliance instances. However, in order to access more than 2 TB of disk space on upgraded virtual appliances, see Upgrading a Virtual Appliance, page 8. If you are upgrading, see also Optimize Disk Space Allocations, page 11.

Feature	Description
More flexibility for choosing users for an incoming or outgoing policy	Prior to this release, an incoming or outgoing policy matches if any of the specified values (sender, receiver domains, or LDAP group names) in the policy matches. Cisco AsyncOS 9.0 for Email provides you more flexibility for choosing users for an incoming or outgoing policy. You can set the policy to match if, • The message is from any sender, one or more of the specified senders, or none of the specified senders. • The message is sent to any recipient, one or more of the specified recipients, or all of the specified recipients and none of the specified recipients. **Note** From Cisco AsyncOS 9.0 for Email onwards, you must set at least one sender and recipient.
Advanced Malware Protection Improvements	• You can now use the Advanced Malware Protection feature to detect malware in archived or compressed email attachments. For a list of supported archive and compressed formats, see the document referenced in Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?, page 7. • When you configure the file analysis feature, you choose which file types are sent for analysis. For a list of supported file types, see the document referenced in Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?, page 7. • New types are added dynamically; you will receive an alert when the list of uploadable file types changes, and can select added file types to upload. • You will receive an alert if analysis of some file types is temporarily unavailable. • You will receive an alert if analysis of all supported file types is restored after a temporary outage. • Cisco AsyncOS for Email now includes a new message filter action (`skip-ampcheck`) that allows messages to bypass File Reputation Filtering and File Analysis configured on the system.
Virtual gateway improvement	The number of Virtual Gateway addresses available on all Email Security appliance models is now 255.
Per-user spam notifications	You can specify which users receive spam notifications, based on LDAP groups.
Customizable end user notification page for URL filtering	You can customize the appearance of the end user notification page used for URL filtering and display your organization's branding such as logo, name of the organization, contact information, and so on.
Enhanced password options	When creating user accounts or changing passwords, there is now an option to auto-generate a password that meets the configured requirements.

Feature	Description
Welcome banner to display internal security information or best practice instructions for the appliance	You can configure Cisco AsyncOS for Email to display a welcome banner after a user successfully logs into the appliance through SSH, FTP, or web interface. You can use the welcome banner to display internal security information or best practice instructions for the appliance.
New authorization protocol for outgoing SMTP authentication	Outgoing SMTP authentication now supports the following additional authorization protocol: LOGIN.
Enhanced spam protection capabilities	Cisco AsyncOS now has enhanced capabilities to detect and protect against new spam campaigns, for example, snowshoe spam.
Enhanced logic to detect whether AMP services (File Reputation and Analysis) are reachable	To avoid false alerts, the logic used to detect whether AMP services (File Reputation and Analysis) are reachable is enhanced.
Configurable SSL Settings in FIPS Mode	In FIPS mode, you can now configure the Cipher Suites in the SSL settings, using the `sslconfig` command in CLI. For more information, see *Cisco AsyncOS for Email CLI Reference Guide*. **Note** You cannot change server and client methods in FIPS mode.
Configurable SSH Server Settings	You can now configure the following SSH server settings using the `sshconfig` command in CLI: • Public Key Authentication Algorithms • Cipher Algorithms • KEX Algorithms • MAC Methods • Minimum Server Key Size
Encrypt sensitive data in FIPS mode	In FIPS mode, you can now encrypt: • Critical security parameters in your appliance • Swap space in your appliance. This helps to prevent any unauthorized access or forensic attacks when the physical security of the appliance is compromised. Use the `fipsconfig` command in CLI to enable encryption of sensitive data in the appliance.
Encrypt sensitive data in configuration files	You can now encrypt the critical security parameters in the appliance configuration file while exporting, emailing, or displaying it.
Permanently delete sensitive data in the appliance	You can now permanently delete sensitive data (critical security parameters) in your appliance using one of the following commands in CLI: • `wipedata` • `diagnostic > reload` See *Cisco AsyncOS for Email CLI Reference Guide*.

Feature	Description
More secure AsyncOS updates and upgrades	For enhanced security, AsyncOS now uses a stronger hashing algorithm, SHA-384, to verify the received updates and upgrades.
Configurable CLI Session Timeout	You can now specify how long a user can be logged into the Email Security appliance's CLI before AsyncOS logs the user out due to inactivity. **Note** The CLI session timeout applies only to the connections using Secure Shell (SSH), SCP, and direct serial connection.
Enhanced security for DKIM Signing Keys in FIPS mode	For enhanced security, if encryption of sensitive data in the appliance is enabled in FIPS mode, • Private keys are not displayed in plain text while editing an existing signing key. • Signing keys are encrypted while exporting.
Enhanced security for DSA Host Keys in FIPS mode	For enhanced security, in FIPS mode, AsyncOS for Email uses a 2048-bit DSA host key.
Enhanced security for Demonstration Certificate	The demonstration certificate is updated to use keys of size 2048 bits and 1024 bits for FIPS mode and non-FIPS mode, respectively.
Enhanced URL Defanging	Message and content filters for URL defanging now accounts for DNS spoofing and replaces a "." (dot) in the URL with "[.]". For example, after defanging, www.defangurl.com becomes BLOCKEDwww[.]defangurl[.]comBLOCKED.

Changes in Behavior

Deprecated Commands

The `disk_usage` subcommand under `diagnostics` has been deprecated. To view and configure disk space quotas, use the `diskquotaconfig` command instead.

Disk Space for Quarantines

You must now allocate disk space for quarantines using the **System Administration > Disk Management** menu.

Changes in Password Change Options

When you are enforcing a password change, you can choose whether the users must change the password during the next login or after a specified duration.

If you are enforcing a password change after a specified duration, you can also set a grace period to reset the password after the password expires.

Changes in Local User Account and Password Settings

While configuring Local User Account and Password Settings, you can configure a grace period to reset the password after the password expires.

Opening a Support Case from the Appliance

In order to open a support case from the appliance, you will need your CCOID and support contract number. Previously, this information was collected via other means.

Also, in order to route cases more efficiently, the Technology and Sub-Technology options may differ from previous releases and may change at any time.

New Log for URL Filtering

URL filtering information will be posted to the following logs:

- Mail Logs (`mail_logs`). Information related to the result of scanning a URL (action taken of a message depending on the URL) is posted to this log.
- URL Filtering Logs (`web_client`). Information related to errors, timeouts, network issues, and so on while attempting the URL lookup are posted this log.

Stricter Password Rules

Stricter password rules are enforced immediately after running the System Setup Wizard.

Removal of Option to Enable Telnet for Appliance Access

The option to enable Telnet for access to the appliance has been removed from the Network > IP Interfaces page and from the `interfaceconfig` command.

Documentation Updates

Note For the most current and complete documentation, see the PDF version of the user guide for AsyncOS for Cisco Email Security Appliances. Online help may not include the most current and complete information.

- The maximum depth of attachment recursion to scan (configured using Scan Behavior page or scanconfig command in CLI) is 50. In the online help, this value is incorrect.
- References in Online Help to Unsupported Hardware Models. Please disregard references in the online help to any hardware models that are not supported in this release.

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.

Upgrade Paths

Important!

See the following sections before upgrading:

- **Hardware appliances**: This release is supported only on certain models. See Supported Hardware for This Release, page 8.
- **Virtual appliances**: To ensure that you obtain all of the benefits of this release, see Upgrading a Virtual Appliance, page 8.
- **Cluster configurations (centralized management):** Take action before you upgrade your cluster. See Upgrading Deployments with Centralized Management (Clustered Appliances), page 9.
- **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 8.

You can upgrade to release 9.0.0-500 from the following versions:

- 8.0.1-023
- 8.5.6-092
- 8.5.6-106
- 8.6.0-050
- 9.0.0-448

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.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - C380 or C680
  - C170
  - 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 you have a previous Email Security Virtual Appliance release and you want to use more than 2 TB of disk space, you cannot simply upgrade your virtual appliance. Instead, deploy a new virtual machine instance for this release. You can maintain the old instance separately, and optionally manage both instances using a Cisco Content Security Management appliance.

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 8.

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.

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.

Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances

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

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.

Pre-upgrade Notes

Please be aware of the following upgrade impacts:

- Email Authentication, page 9
- Configuration Files, page 10
- Received Headers, page 10
- Feature Keys, page 10
- Resource Conservation Mode, page 10
- DLP Policies on RSA Enterprise Manager, page 10
- File Analysis Quarantine, page 10

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.

DLP Policies on RSA Enterprise Manager

If you are using RSA Enterprise Manager to manage DLP policies, after upgrading to AsyncOS 9.0 for Email, the association of the policies on RSA Enterprise Manager with Mail Policies on AsyncOS breaks. This is because, in AsyncOS 9.0 for Email, Mail Policies are handled differently from the previous releases. To overcome this scenario, you must reassociate the DLP policies on RSA Enterprise Manager with Mail Policies on AsyncOS. For instructions, see Chapter 17, “Data Loss Prevention” of the *Cisco AsyncOS for Email User Guide*.

File Analysis Quarantine

- If you have manually created a policy quarantine with the name "File Analysis," you must eliminate this quarantine before upgrading.

You can do this by creating another quarantine with a different name, moving the messages to this new quarantine, then deleting the existing File Analysis quarantine. For more information about moving messages between policy quarantines, see the user guide or online help.

If you do not do this, the system will not create the File Analysis quarantine that is used to automatically process messages sent for analysis.

- After upgrade, and after you configure the system to send messages to the new system-created File Analysis quarantine, you may want to delete, or disable in your incoming mail policies, any content filters that you previously created to quarantine messages with files sent for analysis.

Upgrading to This Release

Before You Begin

- Review the Known issues in Known and Fixed Issues, page 12 and Installation and Upgrade Notes, page 8.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 8.

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.

Step 10 (Only if DLP Policies are managed using RSA Enterprise Manager) Reassociate the DLP policies on RSA Enterprise Manager with Mail Policies on AsyncOS. See DLP Policies on RSA Enterprise Manager, page 10.

After Upgrading

Optimize Disk Space Allocations

After upgrade is complete, you can go to **System Administration > Disk Management** and optimize disk space allocation for the functionality that your deployment uses.

Note After upgrading, if you receive an alert stating that the Miscellaneous disk usage has approached 75 percent of the quota, you must manually set the disk space for Miscellaneous to 30 GB. This problem occurs if you have upgraded to Cisco AsyncOS 9.0 for Email more than three times.

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 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

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

Fixed Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&prdNam=Cisco%20Email%20Security%20Appliance&rls=9.0.0&sb=fr&srtBy=byRel&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.0.0&sb=anfr&sts=open&svr=3nH&srtBy=byRel&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 **9.0.0**.

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

Documentation For Cisco Content Security Products	Location
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

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.