Release Notes for AsyncOS 9.7 for Cisco Email Security Appliances

Published: October 26, 2015

Contents

- What’s New, page 1
- Changes in Behavior, page 2
- Upgrade Paths, page 3
- Installation and Upgrade Notes, page 3
- Known and Fixed Issues, page 6
- Documentation Updates, page 7
- Related Documentation, page 8
- Service and Support, page 8

What’s New

Feature	Description
Content Scanning Engine Update	The content scanning engine is updated in this release. Going forward, all the content scanning engine updates are automatically available through the update server.
Image Analysis Scanning Engine Update	The image analysis scanning engine is updated in this release.
Cloudmark Anti-spam Engine Update	The Cloudmark anti-spam engine is updated in this release.
Non-Spam Quarantines	You can now specify a retention time in minutes for all policy, virus, and outbreak quarantines including the File Analysis quarantine.

LDAP	LDAP queries that return certain error codes such as Unavailable, Busy, or Operations Error, now fall back to a subsequent LDAP server listed for failover. Previously, failover occurred only if the connection to the LDAP server failed.
Option to accept or reject ARP replies with a multicast address	While configuring ethernet media settings using the `etherconfig` command in CLI, you can now specify whether to accept or reject ARP replies with a multicast address.
Support for RAR 5.0 Archive Format	Cisco Email Security appliance now supports scanning of RAR 5.0 files.
Changes in SMTP Call-Ahead Server Profile Settings	While setting up an SMTP Call-Ahead Server Profile, you can now configure the appliance to reject a connection with custom SMTP response (code and text) for validation failures.

Changes in Behavior

Changes in Outbreak Filter Settings	While enabling Outbreak Filter on mail policies, you can now configure the appliance to modify the message subject even when the URL Rewriting is disabled or the Threat Disclaimer is not set.
Representation of the CPU utilization	For better representation of the CPU utilization, the parameter Total CPU Utilization is now changed to Overall CPU Load Average (Monitor > System Status > CPU Utilization on web interface or `system status` command in CLI). Overall CPU Load Average is the average of the appliance's CPU load in the last one minute.
Changes in Authentication-Results Header	Authentication-Results header now includes authentication results for SPF, DKIM, and DMARC verifications. Also, to be compliant to RFC5451, if DKIM verification is enabled and a message is not DKIM signed, the appliance now adds “none” in the Authentication-Result header.
Changes in URL Filtering	URLs that were formerly labeled “Suspicious” are now labeled “Neutral.” Only the labeling has changed; the underlying logic and processing have not changed.
Receive and process messages from domains with malformed DMARC records	Cisco Email Security appliance will now be able to receive and process messages from domains with malformed DMARC records. However, the appliance will not perform DMARC verification of such messages.
Character limit for SMTP Routes Destination Hostnames removed	While setting up SMTP Routes, you can now specify destination hostnames of more than 45 characters.
Content Scanner Behavior	For enhanced performance, if the Image Analysis Feature is not enabled, content scanner will not extract images embedded in attachment files.

Upgrade Paths

You can upgrade to release 9.7.0-125 from the following versions:

- 8.5.7-043
- 9.1.0-032
- 9.1.1-023
- 9.1.1-025
- 9.6.0-042
- 9.6.0-051
- 9.7.0-041
- 9.7.0-119

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 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 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 3.

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 8, 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:

- FIPS Compliance, page 4
- Upgrading Deployments with Centralized Management (Clustered Appliances), page 5
- Upgrading From a Release Other Than the Immediate Previous Release, page 5
- Configuration Files, page 5

FIPS Compliance

AsyncOS 9.7 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 9.7.

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.

Upgrading to This Release

Before You Begin

- Review the Known and Fixed Issues, page 6 and Installation and Upgrade Notes, page 3.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 4.

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 6.

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 6
- Lists of Known and Fixed Issues, page 7
- Finding Information about Known and Resolved Issues, page 7

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&rls=9.7.0&sb=anfr&sts=fd&srtBy=byRel&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.7.0&sb=anfr&sts=open&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 the version of the release, for example, 9.7.

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.

Documentation Updates

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 8.

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

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.