Release Notes for Cisco AsyncOS 9.1 for Cisco Email Security Appliances

Published: March 30, 2015
Revised: December 1, 2015

Contents

What's New

Feature	Description
FIPS Certification	Cisco Email Security Appliance is now FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #1643).
File Analysis quarantine improvements	Messages can now be automatically released or deleted from the *centralized* File Analysis quarantine on the Content Security Management Appliance based on the analysis verdict. For more information, see the documentation for AsyncOS 9.1 for Cisco Content Security Appliances.

Feature	Description
Updater enhancements	Cisco AsyncOS 9.1 for Email includes the following updater enhancements: • Email security appliance can check the validity of the Cisco updater server certificate every time the appliance communicates with the updater server. • If you are using a non-transparent proxy server, you can add the CA certificate used to sign the proxy certificate to the appliance. By doing so, the appliance trusts the proxy server communication. For more information, see *Cisco AsyncOS for Email User Guide*.
Option to disable SSLv3 for enhanced security	For enhanced security, you can disable SSLv3 for the following services: • Updater • URL Filtering • End User Quarantine • LDAP You can use the `sslv3config` command in CLI to disable SSLv3 for the above services. For more information, see *Cisco AsyncOS for Email User Guide*.

Changes in Behavior

While configuring the global settings for listeners, you can now specify whether to accept or reject messages based on the size of the subject. If you specify this parameter, messages having subject size within the specified limit will be accepted and any other messages will be rejected. For more information, see *Cisco AsyncOS for Email User Guide*.

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 3.
- **Virtual appliances**: To ensure that you obtain all of the benefits of this release, see Upgrading a Virtual Appliance, page 4.
- **Cluster configurations (centralized management):** Take action before you upgrade your cluster. See Upgrading Deployments with Centralized Management (Clustered Appliances), page 5.
- **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 3.

You can upgrade to release **9.1.0-032** from the following versions:

- 8.0.1-023
- 8.0.2-066
- 8.5.5-280
- 8.5.6-074
- 8.5.6-092
- 8.5.6-106
- 8.5.6-116
- 9.0.0-500
- 9.1.0-024

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 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.

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.

Pre-upgrade Notes

Before upgrading:

- File Analysis Quarantine, 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

File Analysis Quarantine

- If you have manually created a policy quarantine with the name "File Analysis," you must eliminate this quarantine before upgrading from a release earlier than AsyncOS 9.0.

  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 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.

After Upgrading

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, 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=9.1.0&sb=fr&sts=fd&svr=4nH&srtBy=byRel&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.1.0&sb=afr&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 **9.1.0**.

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.

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.

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

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.

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.

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

Use the following methods to obtain support:

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

Support Site: 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.