Release Notes for Cisco AsyncOS 9.5 for Cisco Email Security Appliances

Published: May 28, 2015

Last updated: October 27, 2015

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

Feature	Description
Graymail Detection and Safe Unsubscribing	• The Email Security appliance allows you to: – Identify graymail using the integrated graymail engine and apply appropriate policy controls. – Provide a secure and easy mechanism for end users to unsubscribe from unwanted graymail using cloud-based Unsubscribe Service. • You can monitor detected graymail using the following reports: – Overview page > Incoming Mail Summary – Incoming Mail page > Top Senders by Graymail Messages – Incoming Mail page > Incoming Mail Details – Incoming Mail page > Incoming Mail Details > Sender Profile (drill down view) – Internal Users page > Top Users by Graymail – Internal Users page > User Mail Flow Details – Internal Users page > User Mail Flow Details > Internal User (drill down view) • If you have enabled service updates, scanning rules for the graymail management solution are automatically retrieved from the Cisco update servers. See the "Managing Graymail" chapter in the user guide. **Note** In this release, you cannot configure graymail detection and safe unsubscribing using CLI.
Web Interaction Tracking	The web interaction tracking feature provides information about the end users who clicked on rewritten (policy or Outbreak Filter) URLs and the action associated with each user click. Once you enable this feature, you can use the Web Interaction Tracking report to view information such as top malicious URLs clicked, top users who clicked on malicious URLs, and so on. **Note** Web Interaction Tracking report modules are not updated in real-time and are refreshed every 30 minutes. Also, after clicking a rewritten URL, it may take up to two hours for the Web Interaction Tracking report to report this event. See the "Protecting Against Malicious or Undesirable URLs" chapter in the user guide.

Feature	Description
System health monitoring enhancements	The Email Security appliance includes the following system health monitoring enhancements: • **Configurable threshold for system health parameters**. Depending on your organization's requirements, you can configure the threshold for various health parameters of your appliance such as overall CPU usage, number of messages in the work queue, and so on. You can also configure the appliance to send alerts when the specified threshold values are crossed. See the "System Administration" chapter in the user guide. • **Enhanced System Capacity page**. The following reports on the System Capacity page now shows the configured threshold levels for system health parameters: – Workqueue – Overall CPU Usage – Memory Page Swapping See the "Using Email Security Monitor" chapter in the user guide. • **Upgrade Guidance**. While performing an upgrade using web interface or CLI, the system analyzes the Status Logs to determine whether the appliance is ready for an upgrade. Depending on the result of the analysis, you will get guidance on whether to upgrade or perform additional tasks before upgrading. See the "System Administration" chapter in the user guide. • **On-demand Health Check**. You can now check the health of your appliance using the Health Check feature whenever required. The system analyzes historical data in the Status Logs to determine the health of the appliance. Based on the analysis, you can take remediation actions. See the "System Administration" chapter in the user guide. • **Resource Conservation Activity graph.** This graph shows the number of times the appliance entered resource conservation mode. You can access this graph from **Monitor > System Capacity > System Load**. See the "Using Email Security Monitor" chapter in the user guide.

Feature	Description
Support for On-Premises File Analysis	If you have deployed a Cisco AMP Threat Grid appliance on your network, you can analyze message attachments for malware without sending them to the cloud. For information about upgrades, see File Analysis Server Change, page 8. To configure an on-premises file analysis server, see the "File Reputation Filtering and File Analysis" chapter in the user guide or online help.
Support for TLS v1.2	Cisco Email Security appliance now supports an additional SSL method: TLS v1.2. Keep in mind that: • If you were using TLS v1 prior to the upgrade, TLS v1.2 is also negotiated after the upgrade. • If you weren't using TLS v1 prior to the upgrade, the SSL methods are not automatically set to TLS v1.2 after the upgrade. You can use the SSL Configuration page on web interface or the `sslconfig` command in CLI to view or modify the existing SSL configuration. **Note** The highest supported TLS or SSL method in the client advertisement is always selected during the negotiation.

Changed Behavior

Marketing Email Settings	If you had enabled anti-spam scanning and had configured Marketing Email Settings under anti-spam settings for a mail policy, after upgrading to AsyncOS 9.5 for Email, • Graymail will be enabled globally by default. • Marketing Email Settings under anti-spam settings will be moved under graymail settings of the same policy. • While using graymail-related reports, keep in mind that: – The number of marketing messages is a sum of marketing messages detected before and after the upgrade. – The total number of graymail messages does not include the number of marketing messages detected before the upgrade. – The total number of attempted messages also includes the number of marketing messages detected before the upgrade.

Upgrade Paths

You can upgrade to release 9.5.0-201 from the following versions:

- 8.5.6-106
- 9.1.0-032
- 9.5.0-144

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 5.

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.

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:

- File Analysis Quarantine, page 6
- FIPS Mode, page 6
- Upgrading Deployments with Centralized Management (Clustered Appliances), page 7
- Upgrading From a Release Other Than the Immediate Previous Release, page 7
- Configuration Files, page 7

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.

FIPS Mode

AsyncOS 9.5 for Email is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to version 9.5.

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 9 and Installation and Upgrade Notes, page 5.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 5.

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 8.

After Upgrading

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.

File Analysis Server Change

The File Analysis cloud server URL has changed. In order to ensure smooth transition of service, perform the following tasks:

- You may need to adjust your firewall settings to allow this traffic to pass. To see the new URL, select **Security Services > File Reputation and Analysis**, then select **Advanced Settings for File Analysis**.
- The file types that can be analyzed may have changed after upgrade. You should receive an alert if there are changes. To verify the file types selected for analysis, select **Security Services > File Reputation and Analysis**.

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&rls=9.5.0&sb=fr&srtBy=byRel&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.5.0&sb=afr&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 **9.5**.

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 10.

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.