Release Notes for Cisco AsyncOS 8.5.7 for Email

Published: June 15, 2015
Revised: July 4, 2017

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

Feature	Description
Updater Enhancements	Cisco AsyncOS 8.5.7 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 configure this option and the verification fails, updates are not downloaded and the details are logged in Updater Logs. Use the `updateconfig > VALIDATE_CERTIFICATES` command in the CLI to configure this option. • 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. Use the `updateconfig > TRUSTED_CERTIFICATES` command in the CLI to configure this option.

Note For a list of all the new features and enhancements in the earlier AsyncOS 8.5.x for Email releases, see *Cisco AsyncOS 8.5.6 for Email Release Notes*.

Upgrade Paths

Upgrading to AsyncOS 8.5.7-043 for Cisco Email Security Appliances (General Deployment—Refresh)

You can upgrade to release 8.5.7-043 from the following versions:

- 8-0-1-023
- 8-5-6-106
- 8-5-7-042

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.

Upgrading to AsyncOS 8.5.7-042 for Cisco Email Security Appliances (General Deployment)

You can upgrade to release 8.5.7-042 from the following versions:

- 8-0-1-023
- 8-5-6-092
- 8-5-6-106
- 8-5-6-116

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.

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.

Change in URL Reputation Feature Servers

Important! The server pool used by the URL Reputation feature servers has changed. As a result, when you enable the URL Filtering feature, you may observe one of the following symptoms:

- Work queue on your appliance backs up
- A large number of 'Request already expired' entries in the web_client logs
- Alerts indicating that your appliance is unable to connect to the Cisco Web Security Service

To fix this issue, you must reduce the number of URLs sent for verification at the same time.

Procedure

Step 1 Use SSH to access the command-line interface.

Step 2 Enter `websecurityadvancedconfig`.

Step 3 Change the value of **Enter the threshold value for outstanding requests** from default value to 5.

Note Make sure that you do not change any other settings.

Step 4 Commit your changes.

Deploying a Virtual Appliance

If you are deploying a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*.

If you are migrating from a hardware appliance, upgrade your hardware appliance to this AsyncOS release, then import the configuration file from the upgraded hardware appliance into your virtual appliance.

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

Please be aware of the following upgrade impacts:

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.

Upgrading to This Release

Before You Begin

Review the Installation and Upgrade Notes, page 3.

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 Upgrade

Update the URL Lookup Timeout Value for Cisco Web Security Services

If you are upgrading from Cisco AsyncOS 8.5.X for Email, it is recommended that you set the default URL Lookup Timeout value to five seconds using the `websecurityadvancedconfig` command in CLI.

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.

Documentation Updates

Additional Information

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 online help and the User Guide PDF.

Certificates for URL Filtering Features

AsyncOS is designed to automatically deploy and update the certificates needed for communications with cloud services used for URL filtering features. However, if for any reason the system is unable to update these certificates, you will receive an alert that requires action from you.

To ensure that you receive these alerts (System type, Warning severity), see information in the online help or user guide about adding alert recipients.

If you receive an alert about an invalid certificate, contact Cisco TAC, which can provide the required replacement certificate. Instructions for installing the certificate are in the URL Filtering chapter in the online help or user guide.

For details about the connection between the appliance and the cloud URL reputation and category services, see the URL Filtering chapter of the user guide or online help.

Changes in Behavior

Note For a list of changes in behavior in the earlier AsyncOS 8.5.x for Email releases, see *Cisco AsyncOS 8.5.6 for Email Release Notes*.

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 new `sslv3config` command in CLI to disable SSLv3 for the above services.

Resolved Issues

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=8.5.7&sb=fr&mDt=1&sts=fd&srtBy=byRel&bt=custV

Note For a list of known and fixed issues in the earlier AsyncOS 8.5.x for Email releases, see *Cisco AsyncOS 8.5.6 for Email Release Notes*.

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 **8.5.7**.

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.

Related Documentation

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.
Cisco Email Security	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 Content Security Management	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.