Release Notes for Cisco AsyncOS 8.0.2 for Email

Published: May 9, 2014
Revised: September 2, 2015

Caution Cisco AsyncOS 8.0.2 for Email is intended for the customers who are planning to use Common Criteria or FIPS compliance modes. If you do not need a Common Criteria or a FIPS compliant build, do not upgrade to Cisco AsyncOS 8.0.2 for Email.

Contents

Cisco Systems, Inc.
www.cisco.com

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).
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. **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`
More Secure AsyncOS Updates and Upgrades	For enhanced security, Cisco AsyncOS now uses a stronger hashing algorithm, SHA-384, to verify the received updates and upgrades.

Feature	Description
Configurable CLI Session Timeout	You can now specify how long a user can be logged into the Email Security appliance's CLI before Cisco 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, Cisco 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.
Updater Enhancements	From **AsyncOS 8.0.2-074**: • 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 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 to configure this option.

Note For more information about the features and enhancements that were added in the previous releases (Cisco AsyncOS for Email version 8.0 and 8.0.1), see http://www.cisco.com/c/dam/en/us/td/docs/security/esa/esa8-0/release_notes/ESA_8-0-1_Release_Notes.pdf.

Changes in Behavior

Revised Threshold Levels for Entering Resource Conservation Mode

Prior to this release, Email Security appliance enters resource conservation mode when the RAM utilization exceeds 75% and the allowed injection rate is gradually decreased as RAM utilization approaches 85%.

From version 8.0 onwards, Cisco AsyncOS for Email is a 64-bit software. As a result of this changed memory model, the threshold values are revised in this release. Appliance enters resource conservation mode when the RAM utilization exceeds 45% and the allowed injection rate is gradually decreased as RAM utilization approaches 60%. This change does not affect the memory utilization on the appliance and all the components in the appliance continue to use the memory as earlier.

Caution Appliances with large memory utilization, especially with large system quarantine, can enter resource conservation immediately after upgrading to Cisco AsyncOS 8.0.2 for Email. To avoid this scenario, make sure that you reduce the system quarantine to a few thousand messages before upgrading.

Additional TLS Support Option

Prior to this release, TLS verification against hosted cloud email services fails when:

- Cloud provider presents a common certificate for all hosted domains.
- The destination controls for these domains have TLS Support set to **Required-Verify**.

Cisco AsyncOS for Email now supports a new TLS Support option - **Required - Verify Hosted Domains**. This option allows you to perform TLS verification against hosted cloud email services where the cloud provider presents a common certificate for all hosted domains. Using this option, you can now send emails over TLS for such domains, as well as domains that are not hosted on cloud.

The new TLS support option is available on Add or Edit Destination Controls page (**Mail Policies > Destination Controls**).

The presented identity of a cloud email server or a destination is either a SubjectAltName (SAN) of type DNSName or a Common Name (CN) of a X.509 public key certificate. Note that CN is checked only if SAN is empty, as SAN has higher priority than CN. Cisco AsyncOS performs an exact or wildcard matching in the following order:

1. Presented identity with recipient email domain.
2. Presented identity with email server hostname configured in Cisco AsyncOS for Email (under **Network > SMTP Routes**).
3. Presented identity with email server hostname derived from a DNS or MX query against the recipient's email domain name.

To verify the server identity, one of the above parameters must match.

Note If you have existing destination controls for hosted cloud email services (where the cloud provider presents a common certificate for all hosted domains), make sure that you set TLS Support to **Required - Verify Hosted Domains**.

Upgrade Paths

Upgrading to AsyncOS 8.0.2-074 for Cisco Email Security Appliances (Maintenance Deployment)

You can upgrade to release 8.0.2-074 from the following versions:

- 8.0.2-066
- 8.0.2-069

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 5.

Upgrading to AsyncOS 8.0.2-055 for Cisco Email Security Appliances (Limited Deployment)

You can upgrade to release 8.0.2-055 from the following versions:

- 7.3.2-024
- 7.6.3-019
- 8.0.1-023

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 5.

Installation and Upgrade Notes

Read through and consider the installation and upgrade impacts listed in this section.

When you upgrade Cisco 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.

Deploying a Virtual Appliance

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

If you are switching from a physical appliance to a virtual appliance, you will need to convert your configuration file to an AsyncOS 8.0 virtual appliance configuration file. For information, see the *Release Notes for Configuration Migration Tool 1.0 for Cisco Content Security Virtual Appliances*. You can import the AsyncOS 8.0 virtual appliance configuration file into a virtual appliance running Cisco AsyncOS 8.0.2.

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 Cisco 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 Cisco AsyncOS.

Feature Keys

The Cisco 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 Cisco AsyncOS 8.0.2 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 Cisco AsyncOS 8.0.2 for Email. To avoid this scenario, make sure that you reduce the system quarantine to a few thousand messages before upgrading.

DSA Host Keys

Prior to this release, in FIPS mode, Cisco AsyncOS for Email was using a 1024-bit DSA host key. In this release, in FIPS mode, Cisco AsyncOS for Email uses a 2048-bit DSA host key. As a result of this change, any remote clients or servers (Security Management Appliances and clustered machines) that are configured with DSA host keys for identification and authentication will fail to connect to your appliance in the following scenarios:

- You were using FIPS mode before upgrading to Cisco AsyncOS 8.0.2 for Email and continued using FIPS mode after the upgrade.
- You were not using FIPS mode before upgrading to Cisco AsyncOS 8.0.2 for Email and you enabled FIPS mode after the upgrade.

To avoid this scenario, you must update your DSA host key files. Depending on your requirements, after the upgrade, do the following:

- If you are using an SSH client to connect to your Email Security appliance, you must remove your appliance from the `~/.ssh/known_hosts` file.
- If you are using a Security Management Appliance (SMA) to centralize management and reporting functions of your Email Security appliances, you must update the DSA host key by running the `logconfig` > `hostkeyconfig` command on SMA. For instructions, see SMA documentation.
- If you are using a cluster setup, you must update the host keys while reconnecting the machines to the cluster. For instructions, see *Cisco AsyncOS for Email User Guide*.

Upgrading to Cisco AsyncOS 8.0.2 for Email Release

Caution If you upgrade from Cisco AsyncOS for Email version 7.3 to 8.0.2, your appliance will no longer be running in FIPS mode. You will need to import or generate new certificates and keys after the upgrade.

Before You Begin

Review the Known Issues, page 10 and Installation and Upgrade Notes, page 5.

Procedure

Use the following instructions to upgrade your Email Security Appliance.

Step 1 Save the XML configuration file off the IronPort 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 Cisco 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 IronPort appliance.

Step 9 Resume all listeners.

Run the **fipscheck** command in CLI to check whether your appliance contains any non FIPS-complaint. objects. If your appliance has any non-FIPS-compliant objects, you must modify them to meet FIPS requirements. See the FIPS Management chapter in the Cisco AsyncOS 8.0.2 for Email User Guide or Online Help.

Note For Cisco AsyncOS 8.0.2 for Email to be FIPS compliant, the key size of non FIPS-compliant objects must be 2048 bits. Failing to change the key size will cause your appliance non FIPS-compliant.

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 IronPort support provider.

Resolved Issues

Note To view a complete list of resolved issues in this release, see Finding Information about Known and Resolved Issues, page 11.

Reference Number	Description
CSCug73383	You may intermittently see application faults and alerts when some of the incoming SMTP connections over TLS are closed.
CSCuh88840	Logging into the web interface of a virtual appliance with expired license causes an application fault.
CSCui21883	Commit action on Cisco AsyncOS 8.0 for Email with large number of RAT entries takes longer compared to earlier AsyncOS releases.
CSCui31954	When using the $Headers['string'] action variable within a notification template for a customized header (for example, "X-Some-Header"), the notification is empty.
CSCui32748	When the appliance fails to download a list of available updates, the SNMP counters for failed updates are not incremented and the updateFailure SNMP trap is not sent.
CSCui89551	When clicking on links rewritten by non-viral threat Outbreak Filters, secure-web.cisco.com returns a 403 Forbidden response intermittently.
CSCuj05650	When using the Centralized Policy/Virus/Outbreak Quarantines, an application fault might occur if an email with unusual meta-data is received by the appliance and the appliance attempts to transfer it to the Centralized Quarantines on the Security Management Appliance (SMA). Such emails remain stuck in the queue to be sent to the SMA and continue to generate application faults when delivery is retried.
CSCuj19408	SNMP is not responding after upgrading to Cisco AsyncOS 8.0 for Email.
CSCuj33987	When the certificates configured for both a listener and the relevant IP interface are changed at the same time (used for receiving released Centralized Policy Virus and Outbreak (PVO) Quarantines), the appliance stops listening for released PVO emails.
CSCuj74034	In Cisco AsyncOS 8.0 for Email and above, when an LDAP query with static attributes is sent to the configured LDAP server, all upper case characters in the static attributes are converted to lower case. This might cause problems for boolean attributes as these attributes must be passed in the original uppercase format.

Reference Number	Description
CSCul07902	An application fault occurs when the Time Range is changed on the search result of Incoming Mail Monitoring page.
CSCul88715	Updater client does not verify server certificate
CSCum06266	Delivering an email over a TLS connection fails due to a defective libz library in Cisco AsyncOS for Email.
CSCum30384	If an error occurs while opening a tunnel for remote access in the CLI, the CLI session displays a trace back and ends abruptly.
CSCun21348	Rules from RSA Enterprise Management (EM) Server are not getting applied intermittently, and DLP stops scanning outbound messages. Mail logs do not show any DLP verdicts.
CSCun79713	After importing a configuration file that includes My Reports type Scheduled Report subscriptions, an application fault occurs whenever you access the Monitor > Scheduled Reports page.
CSCuo25329	Machines installed with OpenSSL 1.0.1g patch fail to connect with Cisco Email Security Appliance.
CSCuu19126	CLI timeout is not happening in serial login.
CSCuu19143	SSH login using an invalid key failed, but not logged.
CSCzv12137	When masquerading is enabled on a listener and is looking at the "friendly" FROM header, any message having badly encoded data or an unknown encoding in the "friendly" FROM header that is sent to a user whose address is checked for masquerade causes an application fault and cause the message to bounce.
CSCzv44971	You might see the "Warning: MID ###### '(no name)' DLP content scanning failed (unknown error)" in the mail logs due to DLP errors when certain content blades that require customization are enabled within custom DLP policies.
CSCzv66126	When upgraded to Cisco AsyncOS 7.5 and later releases, service updates through a local updater server stop working.
CSCzv76406	The Reputation Engine service may not start correctly after it is automatically updated.

Known Issues

Note To view a complete list of known issues in this release, see Finding Information about Known and Resolved Issues, page 11.

Reference Number	Description
CSCun47746	You will receive "Configuration conflict detected" error message while trying to commit. **Workaround** Commit changes as soon as they are made.
CSCun91490	RSA Email DLP service restarts intermittently. **Workaround** Not available

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 **8.0.2**.

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

Note For the most current and complete documentation, see the PDF version of the user guide. Online help may not include the most current and complete information.

The documentation for the Email Security appliance includes the following books:

- *Cisco AsyncOS CLI Reference Guide*
- *Cisco AsyncOS for Email User Guide*
- *Cisco Content Security Virtual Appliance Installation Guide*

Note For more information about the features, enhancements, and the fixed and known issues in the previous releases (Cisco AsyncOS for Email version 8.0 and 8.0.1), see http://www.cisco.com/c/dam/en/us/td/docs/security/esa/esa8-0/release_notes/ESA_8-0-1_Release_Notes.pdf.

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/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco Web Security	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
Cisco Content Security Management	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
CLI reference guide for Cisco Content Security appliances	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco IronPort Encryption	http://www.cisco.com/en/US/partner/products/ps10602/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.

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.