



Release Notes for Hot Patch 1 for AsyncOS 8.0.1 for Email

Published: February 19, 2014

Revised: June 2, 2014

Contents

- [Upgrade Paths, page 1](#)
- [Changes in Behavior, page 1](#)
- [Resolved Issues, page 3](#)
- [Known Issues, page 3](#)
- [Additional Information, page 3](#)
- [Service and Support, page 4](#)

Upgrade Paths

You can upgrade to release 8.0.1-107 from the following versions:

- 8.0.1-023

Changes in Behavior

Revised Threshold Levels for Entering Resource Conservation Mode

Defect ID: [CSCu188365](#)



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, 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 Hot Patch 1 for AsyncOS 8.0.1 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

Defect ID: [CSCu190516](#)

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**.

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. 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 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**.

Resolved Issues

Click a Defect ID in the table for more information about the defect.

Defect ID	Description
CSCu166951	When making an LDAP routing query, if the user portion of the original email address is same as that of the user portion of the routed address, the query fails.
CSCu190516	TLS verification against some of the hosted cloud email services fails, where cloud provider presents a common certificate for all hosted domains.

Known Issues

Click a Defect ID in the table for more information about the defect.

Defect ID	Description
CSCuo97941	<p>Some messages are not encrypted as expected.</p> <p>This can occur if "TLS Required - Verify Hosted Domains" is enabled for the Destination Domain and the destination Mail Transfer Agent (MTA) does not offer STARTTLS.</p> <p>Workaround: Do not enable "TLS Required - Verify Hosted Domains."</p>
CSCum92696	<p>Emails are sent to incorrect mailhosts after LDAP routing. This issue occurs when the configured LDAP contains multiple LDAP entries with the same mailLocalAddress field.</p> <p>Workaround: Not available</p>
CSCzv15563	<p>Upgrade to latest AsyncOS which is having Expired Sophos Engine will alert the user stating that it is expired. This issue occurs when user upgrades to latest available AsyncOS which has Expired Sophos Engine. An alert will be sent to user stating that the Sophos engine is expired.</p> <p>Workaround: You can ignore this alert. After the upgrade, auto-update will download and update the Sophos Engine to the latest available version.</p>

Additional Information

For additional information about AsyncOS for Cisco Email Security Appliances, see the Release Notes for your release at http://www.cisco.com/en/US/products/ps10154/prod_release_notes_list.html.

Service and Support

For service and support information for Cisco Content Security appliances, see:

- http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html
- http://www.cisco.com/en/US/products/ps11169/serv_group_home.html#~Support

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

For noncritical questions and issues, you can also submit a customer support request from the appliance. For instructions, see the User Guide or online help.

This document is to be used in conjunction with the documents listed in the “Additional Information” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2014 Cisco Systems, Inc. All rights reserved.