Release Notes for AsyncOS 8.0 for Email

Published: June 10, 2013

Revised: August 25, 2015

Contents

Cisco Systems, Inc.
www.cisco.com

What's New in Cisco AsyncOS 8.0 for Email

Feature	Description
New Features	
Cisco Email Security Virtual Appliance	Cisco offers the Cisco Email Security appliance as a virtual machine that you can host on your own network. The virtual appliance requires a separate license purchased from Cisco and a Cisco UCS Server (Blade or Rack-Mounted) hardware platform running VMware ESXi version 4.x and 5.0. The *Cisco Content Security Virtual Appliance Installation Guide* includes more information on the requirements for the virtual appliance. The new Email Security Virtual appliance models and configurations are: • C000V (200 GB disk space, 10 GB queue space, 1 core, 4 GB memory) • C100V (200 GB disk space, 10 GB queue space, 2 cores, 6 GB memory) • C300V (500 GB disk space, 70 GB queue space, 4 cores, 8 GB memory) • C600V (500 GB disk space, 70 GB queue space, 8 cores, 8 GB memory) **Note** The C000V appliance is for evaluation purposes only. This feature includes the following changes to AsyncOs for Email: • The Email Security virtual appliance license allows you to clone and run multiple virtual appliances on your network. • The `loadlicense` CLI command for installing the virtual appliance license. You can use the same license for multiple virtual appliances. • Feature keys are included as part of the virtual appliance license. The feature keys will expire at the same time as the license. Purchasing new feature keys will require downloading and installing a new virtual appliance license. • Due to feature keys being included in the virtual appliance license, there are no 30-day evaluations for AsyncOS features such as Cisco Anti-Spam or Outbreak Filters. • You cannot open a Technical Support tunnel before installing the virtual appliance license. • The `version`, `ipcheck`, and `supportrequest` CLI commands have also been updated to included virtual appliance information. • There are new alerts and logs for misconfigured virtual appliances. Other differences between the physical and virtual appliances will be noted in this guide when necessary.

Feature	Description
Centralized Policy, Virus, and Outbreak Quarantines	The following quarantines can now be collectively centralized on a Security Management appliance: • anti-virus • outbreak • Policy quarantines used for messages that are caught by – message filters – content filters – data loss prevention policies Centralizing these quarantines offers the following benefits: • Administrators can manage quarantined messages from multiple Email Security appliances in one location. • Quarantined messages are stored behind the firewall instead of in the DMZ, reducing security risk. • Centralized quarantines can be backed up using the standard backup functionality on the Security Management appliance.
SMTP Session Authentication Using Client Certificates	Supports the use of client certificates to authenticate SMTP sessions between the Email Security appliance and users' mail applications. Organizations that require their users to use a Common Access Card (CAC) for their mail applications can use this feature to configure the Email Security appliance to request a certificate that the CAC and ActivClient middleware application then provides to the appliance. This feature includes the following updates: • A new LDAP query checks the validity of a client certificate in order to authenticate an SMTP session between the user's mail client and the Email Security appliance. • An update to the SMTP Authentication LDAP Query that allows the appliance to check whether the user's mail application is allowed to use the SMTP AUTH command to connect to the appliance. • Anew Certificate type of SMTP authentication profile. • A new TLS parameter has been added to mail flow policies: Verify Client Certificate. • A list of revoked certificates (called a Certificate Revocation List) that the appliance checks as part of its certificate verification to make sure that the user's certificate hasn't been revoked.

Feature	Description
FIPS 140-2 Level 1 Compliance	The Cisco Email Security appliance uses the CiscoSSL Cryptographic Toolkit, a GGSG-approved cryptography suite, to comply with FIPS 140-2 Level 1 standard. CiscoSSL contains an enhanced version of OpenSSL as well as the FIPS-compliant Cisco Common Cryptography Module. Administrators can turn FIPS mode on or off using the `fipsconfig` CLI command. In addition to using CiscoSSL, AsyncOS 8.0 for Email has the following enhancements to when the appliance is in FIPS mode: • AsyncOS restricts the types of certificates and keys used by the appliance in FIPS mode. • AsyncOS has dropped support for version 1 of the SSH protocol for incoming and outgoing connections, including pushing logs by SCP. • RSA keys for DKIM signing can only be 1024, 1536, and 2048 bits. DKIM verification will return `permfail` for certificates that aren't FIPS-compliant. • Serial port sessions to the Email Security appliance time out 30 minutes after the connection to the port is terminated. • The following communication between the appliance and other servers will be FIPS compliant, including LDAPS, remote mail hosts, Cisco servers, and the web interface. • Features that do not need to use CiscoSSL for communication or do not send customer data do not need to be FIPS-compliant. These features include: other clustered appliances, RSA Enterprise Manager (DLP), Cisco update servers, and encryption. **Note** As part of FIPS compliance, AsyncOS for Email no longer supports SSH version 1. **Warning** **If you have upgraded from AsyncOS 7.3, the appliance will no longer be running in FIPS mode. You will need to import or generate new certificates and keys after the upgrade.** You can use FIPS on both the physical and virtual appliances.
My Favorites list	Add the pages you use most to a quick-access menu of your favorite pages.
`date` command	You can now view the appliance's current date, time, and time zone by using use the `date` command on the CLI.
Enhancements	
Download Upgrades in the Background	You can now download upgrades in the background and install them later, allowing you to minimize interruption of service.
Reporting Enhancements	Reporting enhancements let you: • Create a custom report page with the charts and tables you reference most. • Click links in reports to view the Message Tracking data for messages that violate Data Loss Prevention or Content Filtering policies. This enhancement will simplify investigating patterns and root causes of such violations.

Feature	Description
Message Tracking Enhancements	• You can now search Message Tracking for messages with UTF-8 encoded subjects. • You can now restrict message tracking searches to quarantined messages • Message Tracking search results and message details now include links to the message details page for quarantines that the message resides in • If a Message Tracking query returns more than 1000 messages, you can now export up to 50,000 messages matching your query as a comma-separated values file, for analysis using other tools.
Support for More Flexible Password Lengths	Appliance passwords of any length, including zero characters, are now supported.
SNMP Trap Improvements	The linkUp and linkDown SNMP traps have been replaced with standard RFC implementations (RFC-3418).
DLP Engine Updating Enhancements	The appliance can now download and update both the DLP engine and the content matching classifiers used by your DLP policies either automatically or manually, depending on your settings. The settings for updating the RSA DLP engine and content matching classifiers on your appliance are accessible on the **Security Services > Data Loss Prevention Settings** page.
Spam Quarantine Improvements	Spam quarantine search results are now easier to view. They now include a link to message tracking details.
Maximum Message Size for Encryption Increased	The appliance can now encrypt messages up to 25 MB in size.
Opening Support Cases	When opening a support case using the appliance, the severity level is 3. Previously, you could set the severity level using the appliance. To open a support case at a higher severity level, contact Customer Support.
Changed Behavior	
NIC Pairing Behavior	From AsyncOS 8.0 onwards, if the primary interface is up after a disruption, the appliance switches from backup interface to primary interface automatically.

Upgrade Paths

You can upgrade to release 8.0.0-671 from the following versions:

- 7.1.5-104
- 7.3.2-024
- 7.5.2-203
- 7.6.1-022
- 7.6.1-101
- 7.6.2-014
- 7.6.2-103
- 7.6.2-201

- 8.0.0-618
- 8.0.0-670

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 6.

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.

Pre-upgrade Notes

Please be aware of the following upgrade impacts:

Do Not Upgrade If LDAP Queries Include Uppercase Letters

If your deployment uses uppercase letters in LDAP queries, upgrading to this release is not recommended. For details, visit https://tools.cisco.com/bugsearch/bug/CSCuj74034.

AsyncOS Reversion

If you plan to revert to an earlier version of AsyncOS, such as AsyncOS 7.5.1 or AsyncOS 7.1.5, you must update your network settings to use only IPv4 addresses before performing the reversion. Earlier releases of AsyncOS for Email do not support IPv6 and any settings that use IPv6 addresses will be reset.

Warning **Cisco does not support reverting your appliances to AsyncOS 7.3.x after you have upgraded them to AsyncOS 8.0.**

Re-enable FIPS Mode

If you have upgraded from AsyncOS 7.3, the appliance will not be running in FIPS mode after the upgrade. You will need to import or generate new certificates and keys after the upgrade since the appliance will not be access the private keys on the HSM.

Re-enable SNMP

SNMP does not start when you boot the appliance after upgrading to AsyncOS 7.6. Use **snmpconfig -> setup** and then **commit** to enable it.

Email Authentication

For DKIM Authentication, IronPort 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 IronPort 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.

Caution For important information concerning configuration files and the Email Security virtual appliance, see Configuration Files, page 9.

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 GUI.

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. [Defect IDs: 16254, 25816]

Known Issues

Verify you read the list of known issues and limitations before you upgrade AsyncOS for Email. For a list of all known issues, see "Known Issues" section on page 11.

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. [Defect ID: 29160]

Upgrading to the AsyncOS 8.0 Release

For the AsyncOS 8.0 release, please 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 IronPort 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 IronPort appliance.

Step 9 Resume all listeners.

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.

DomainKeys - DomainKeys signing outgoing email can cause a decrease in the message throughput capacity. Using smaller signing keys (512 byte or 768 byte) can mitigate this.

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.

Cisco Email Security Virtual Appliance Notes

Cisco Email Security Virtual Appliance Installation Instructions

Instructions for installing the Cisco Email Security virtual appliance are available in the *Cisco Content Security Virtual Appliance Installation Guide* at http://www.cisco.com/en/US/products/ps10164/prod_installation_guides_list.html.

Note It is extremely important to configure time and synchronization settings on your virtual machine in order to prevent random failures on your Cisco Web Security Virtual Appliance. Specific instructions are in the "Important! Preventing Random Failures" section of the Install Guide and must be followed precisely.

Configuration Files

Email Security virtual appliances running AsyncOS for Email 8.0 do not directly support backward compatibility with configuration files from previous versions of AsyncOS for Email, such as 7.6.2 or 7.5.2.

However, a Configuration Migration Tool is available to convert a configuration file from select versions of AsyncOS into a new file that can be uploaded to a virtual appliance.

For details, see the *Release Notes for the Configuration Migration Tool for Cisco Content Security Virtual Appliances* at http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html.

Cisco UCS Servers and VMware ESXi 4.x and 5.0

Cisco UCS servers (blade or rack-mounted) are the only supported hardware platform for the virtual appliance. **VMware ESXi version 4.x and 5.0** are the only supported virtualization hypervisors. Any other hardware platform or VMware hypervisor will be supported on a "Best Effort" basis: we will try to help you, but it may not be possible to reproduce all problems, and we cannot guarantee a solution. No other virtualization hypervisor is supported.

Cisco recommends that the server hosting your virtual appliances have a minimum requirement of two 64-bit x86 processors of at least 1.5 GHz each, 8 GB of physical RAM, and a 10k RPM SAS hard drive disk.

VMware ESXi 4 File System Settings

VMware ESXi version 4.x comes with a file system that has a default block-size of 4 MB, which supports a virtual disk image of up to 1 TB. However, the larger Cisco virtual security appliances (e.g., C600V) require more than 1 TB of disk space. In order to run these models, you will need to create a new datastore and format it with an 8 MB or larger block size.

For information on block size and instructions on how to create a new datastore, seeVMware's technical documentation at http://kb.vmware.com/selfservice/microsites/search.do? .

Compatibility with Cisco Content Security Management Releases

Features on AsyncOS 8.0 for Email are supported by AsyncOS for Cisco Content Security Management version 8.1.

Compatibility of this release with AsyncOS for Cisco Content Security Management releases is detailed in the Compatibility Matrix available from http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html.

Note that there is no virtual Cisco Content Security Management appliance at this time.

Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in shipping releases.

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 Enter search criteria.

For example, to find all issues fixed in a release.

a. Click **Select from list**, then navigate to and select your product:

b. For **Releases**, enter the AsyncOS release number, such as `8.0.0`.

c. For **Show Bugs**, select **Fixed in this release**.

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

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

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

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 Managment	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

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.

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.

© 2013-2015 Cisco Systems, Inc. All rights reserved.