Release Notes for AsyncOS 9.8.1 for Cisco Email Security Appliances

Published: October 25, 2016
Revised: November 14, 2017

Contents

What's New In This Release

- What's New in AsyncOS 9.8.1, page 2
- What's New in AsyncOS 9.8.0, page 2

Cisco Systems, Inc.
www.cisco.com

What's New in AsyncOS 9.8.1

Feature	Description
CRL check for web interface login	You can configure CRL check for web interface login using one of the following ways: • Network > CRL Sources > Edit Settings > CRL check for WebUI option in the web interface • `certconfig > crl` command in the CLI If you enable this option and the certificate is revoked: • You will receive an alert indicating that the certificate is revoked. • You will not be able to access the web interface of your appliance. However, you can still log in to your appliance using the CLI. You must import and configure a valid certificate through the CLI to be able to access the web interface of your appliance. See *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.

What's New in AsyncOS 9.8.0

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). See the "FIPS Management" chapter in the user guide or online help.
Support for 90-Series Hardware	Support for new appliance models: • C190 • C390 • C690

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 or online help.
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 or online help.

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 or online help. • **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 or online help. • **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 or online help. • **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 or online help. • **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 or online help.
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 Changes May Require Configuration Changes, page 15. 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.
Enhanced Credit Card Number Smart Identifier	The credit card number smart identifier can now identify JCB card numbers.
View File Analysis result details from all appliances in your organization	You can now view detailed file analysis results in the cloud for all files uploaded from any content security appliance in your organization. To configure this functionality, see the "File Reputation Filtering and File Analysis" chapter in the user guide or online help.
URL Filtering Enhancement	You can now configure the appliance not to replace the URLs within HREF tags with secure proxy URLs. However, if an end user clicks on these URLs, the end user will be redirected to the secure proxy. You can configure this option using the `websecurityadvancedconfig` command in the CLI. See *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Option to Send Potentially Malicious File Types for File Analysis	Cisco periodically checks for potentially malicious file types to prevent zero day threats. If new threats are identified, details of such file types are sent to your appliance through updater servers. If you enable this functionality, your appliance will send such file types for analysis in addition to the file types you have selected. Select the **Other potentially malicious file types** option on the File Reputation and Analysis Settings page (**Security Services** > **File Reputation and Analysis** > **Edit Global Settings** > **File Analysis** section) to enable this functionality. For information about the new file types that are analyzed, see *File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*, available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html. **Note** 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.
Content Scanning Engine Update	The content scanning engine is updated in this release. Going forward, all the content scanning engine updates are automatically available through the update server.
Image Analysis Scanning Engine Update	The image analysis scanning engine is updated in this release.

Cloudmark Anti-spam Engine Update	The Cloudmark anti-spam engine is updated in this release.
Non-Spam Quarantines	You can now specify a retention time in minutes for all policy, virus, and outbreak quarantines including the File Analysis quarantine.
LDAP	LDAP queries that return certain error codes such as Unavailable, Busy, or Operations Error, now fall back to a subsequent LDAP server listed for failover. Previously, failover occurred only if the connection to the LDAP server failed.
Option to accept or reject ARP replies with a multicast address	While configuring ethernet media settings using the `etherconfig` command in CLI, you can now specify whether to accept or reject ARP replies with a multicast address.
Support for RAR 5.0 Archive Format	Cisco Email Security appliance now supports scanning of RAR 5.0 files.
Changes in SMTP Call-Ahead Server Profile Settings	While setting up an SMTP Call-Ahead Server Profile, you can now configure the appliance to reject a connection with custom SMTP response (code and text) for validation failures.
Using From Header for DKIM Signing	You can now use the DKIM Global Settings (**Mail Policies** > **Signing Profiles**) to choose whether to use From header for DKIM signing. For DMARC verification of DKIM signed messages, you must use the From header during DKIM signing.
Duplicate Boundaries Verification	Cisco Email Security appliance can now detect messages with duplicate MIME boundaries and perform actions on them. Use the Duplicate Boundaries Verification content filter condition or the `duplicate_boundaries` message filter rule to detect messages with duplicate MIME boundaries.
Message Filter Rule to Detect Malformed MIME Headers(CSCuw03606)	You can now take actions on messages with malformed MIME headers using the new message filter rule: "`malformed-header`." See the "Using Message Filters to Enforce Email Policies" chapter in the user guide or online help.

Changes in Behavior

- Changes in Behavior in AsyncOS 9.8.1, page 7
- Changes in Behavior in AsyncOS 9.8.0, page 7

Changes in Behavior in AsyncOS 9.8.1

Changes in Importing Certificate Authority list	Prior to this release, you could import the certificate authority list on your appliance when the CA flag is set to either 'true' or 'false'. After you upgrade to this release, you can import the custom certificate authority list on your appliance only when the CA flag is set to 'true'.
Changes in Uploading Device Certificate	Prior to this release, you could upload the device certificate on your appliance without importing the custom certificate authority list. After you upgrade to this release, you need to import the custom certificate authority list before you upload the device certificate on your appliance.
Malformed-Header Message Filter Rule Changes	The `malformed-header` message filter rule now also checks for the value of the Content-Transfer-Encoding header.

Changes in Behavior in AsyncOS 9.8.0

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 9.8 or later, • 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.
Content Dictionary Changes	For efficient processing, the following content dictionary entries are treated as words: • Entries containing only alphanumeric characters • Email addresses containing the following characters: 0-9, A-Z, a-z, dot, underscore, hyphen, and at symbol • Domain names containing the following characters: 0-9, A-Z, a-z, dot, underscore, hyphen, and at symbol If you want the appliance to treat such a word as a regular expression, enclose the word in parenthesis, for example, `(user@example.com)`.
File Analysis	File Analysis changes may require action from you. See File Analysis Changes May Require Configuration Changes, page 15.

DKIM Signing-related Logging Changes	• If the log level is set to Trace, the mail log will now include additional log entries to identify errors that occur during the DKIM signing process. • The mail log will now include two separate log entries for DKIM signing: one for displaying the signing profile that will be used for the signing and the other for the signing event.
AMP-related Mail Log and Message Tracking Changes	Prior to this release, if the threat verdict of a file is unknown, the verdict was shown as "clean" in the mail log and message tracking. After upgrading to this release, if the threat verdict of a file is unknown, the mail log and message tracking will show the verdict as "unknown."
Graymail Changes	Prior to this release, if a message is graymail and outbreak filter positive, the actions configured for graymail are not applied after the message is released from the outbreak quarantine. The safe unsubscribe banner (if configured) is not added in this scenario. After upgrading to this release, the actions configured for graymail are applied after the message is released from the outbreak quarantine. The safe unsubscribe banner (if configured) is added in this scenario.
Mail Policy Matching Logic Changes	Prior to this release, while matching a message to a mail policy, the envelope sender (RFC821 MAIL FROM address) and the header sender (address found in the RFC822 From and Reply-To) had the same priority. As a result, if you had configured a mail policy to match a specific user, the messages were classified into that mail policy based on the header sender. After upgrading to this release, while matching a message to a mail policy, the envelope sender has higher priority over the header sender. If you have configured a mail policy to match a specific user, the messages will be classified into that mail policy based on the envelope sender.
Changes in Outbreak Filter Settings	While enabling Outbreak Filter on mail policies, you can now configure the appliance to modify the message subject even when the URL Rewriting is disabled or the Threat Disclaimer is not set.
Representation of the CPU utilization	For better representation of the CPU utilization, the parameter Total CPU Utilization is now changed to Overall CPU Load Average (Monitor > System Status > CPU Utilization on web interface or `system status` command in CLI). Overall CPU Load Average is the average of the appliance's CPU load in the last one minute.
Changes in Authentication-Results Header	Authentication-Results header now includes authentication results for SPF, DKIM, and DMARC verifications. Also, to be compliant to RFC5451, if DKIM verification is enabled and a message is not DKIM signed, the appliance now adds "none" in the Authentication-Result header.
Changes in URL Filtering	URLs that were formerly labeled "Suspicious" are now labeled "Neutral." Only the labeling has changed; the underlying logic and processing have not changed.
Receive and process messages from domains with malformed DMARC records	Cisco Email Security appliance will now be able to receive and process messages from domains with malformed DMARC records. However, the appliance will not perform DMARC verification of such messages.

Character limit for SMTP Routes Destination Hostnames removed	While setting up SMTP Routes, you can now specify destination hostnames of more than 45 characters.
Content Scanner Behavior	For enhanced performance, if the Image Analysis Feature is not enabled, content scanner will not extract images embedded in attachment files.
Change in SPF Verification Content and Message Filter Behavior	If you have configured an SPF verification content or message filter rule without an SPF identity and if a message contains different SPF identities with different verdicts, the rule is triggered if one of the verdicts in the message matches the rule.
DKIM Signing of System Generated Messages	**DKIM Signing of System Generated Messages** option is now available under Mail Policies > Signing Profiles > DKIM Global Settings.
New Alert for Message Filter Crashes	When a message filter crashes, the appliance sends a system alert with a critical severity.
Change in SPF Verification Content and Message Filter Behavior	If you have configured an SPF verification content or message filter rule without an SPF identity and if a message contains different SPF identities with different verdicts, the rule is triggered if one of the verdicts in the message matches the rule.
Change in host key verifications during cluster communication.	Prior to this release, during cluster communication, host key verifications were performed based on SSH-DSS and SSH-RSA. After upgrading to this release, during cluster communication, host key verifications are now performed based on SSH-RSA only.
Changes in Authentication Logs	If you enter an invalid username during login through the web interface or CLI, the username is masked in the authentication logs.

Upgrade Paths

Upgrade Paths for Release 9-8-1-021

You can upgrade to release 9.8.1-021 from the following versions:

- 9-8-0-112
- 9-8-1-015

Upgrade Paths for Release 9-8-1-015

You can upgrade to release 9.8.1-015 from the following versions:

- 9-8-0-112
- 9-8-0-102

- 9-1-2-036

Note You cannot upgrade from 9.8.0.x version to10.0.x release.

Upgrade Paths for Release 9.8.0-112

You can upgrade to release 9.8.0-112 from the following versions:

- 9.1.2-036
- 9.7.2-131
- 9.8.0-102

Note You cannot upgrade from 9.8.0.x version to10.0.x release.

Upgrade Paths for Release 9.8.0-102

You can upgrade to release 9.8.0-102 from the following versions:

- 9.1.1-023
- 9.1.2-036
- 9.7.2-131
- 9.8.0-092

Note You cannot upgrade from 9.8.0.x version to10.0.x release.

Installation and Upgrade Notes

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

When you upgrade AsyncOS 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.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - C190, C390, C690
  - 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

Migrating from Older Hardware to x90 Hardware Appliances

Migration of configurations from x60 hardware is not supported.

Instructions in this topic apply only to configuration migration from x70 or x80 hardware.

Note In order to migrate your configuration, both the old hardware and the new hardware must be running the identical AsyncOS version, including build number. The AsyncOS version you choose must be supported on both hardware models.

Step 1 Upgrade your new 90-series hardware to the latest supported version of AsyncOS (build number is important.)

Step 2 Upgrade your old appliance to the same AsyncOS release, including build number.

Step 3 Save the configuration file from your upgraded hardware appliance.

Step 4 Load the configuration file from the old appliance onto the new appliance.

If your old and new appliances have different IP addresses, deselect Load Network Settings before loading the configuration file.

Step 5 Commit your changes.

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 your current Virtual Appliance release does not support more than 2TB of disk space, and you want to use more than 2 TB of disk space with this release, you cannot simply upgrade your virtual appliance.

Instead, you must deploy a new virtual machine instance for this release.

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 12.

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.

See also Service and Support, page 18, below.

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:

Cisco Content Security Management Appliance Compatibility

You can connect AsyncOS 9.8 to a Security Management appliance only if the AsyncOS version of the Security Management appliance is 9.6.0-077.

RSA Enterprise Manager

RSA Enterprise Manager is not supported on AsyncOS 9.8. If you are using RSA Enterprise Manager, before upgrading to AsyncOS 9.8, perform the following tasks:

1. Disable RSA Enterprise Manager.
2. Enable RSA Email DLP on your appliance(s).
3. Using RSA Email DLP, recreate the DLP policies that were configured in RSA Enterprise Manager.

For instructions, see the “Data Loss Prevention” chapter in the User Guide or the online help.

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.

Deletion of Certificates that Do Not Comply to Common Criteria Specification

After you upgrade to this release, all the certificates that do not comply to the Common Criteria specification are deleted.

Upgrading to This Release

Before You Begin

- Review the Known and Fixed Issues, page 16 and Installation and Upgrade Notes, page 10.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 12.

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

- After the upgrade, review your SSL configuration to ensure that you have selected the correct GUI HTTPS, Inbound SMTP, and Outbound SMTP methods to use. Use the **System Administration** > **SSL Configuration** page or the `sslconfig` command in CLI. For instructions, see the “System Administration” chapter in the User Guide or the online help.
- If you are upgrading from a non-FIPS-compliant release, you must enable FIPS mode on your appliance using the `fipsconfig` command in CLI. For instructions, see the “FIPS Management” chapter in the User Guide or the online help.
- If you plan to switch your appliance to FIPS mode, disable TLS v1.0 method for GUI HTTPS, Inbound SMTP, and Outbound SMTP under **System Administration** > **SSL Configuration**. For instructions, see the “System Administration**”** chapter in the User Guide or the online help.
- To be Common Criteria-compliant, make sure that all the trusted certificate authorities installed (System and Custom Lists) in your appliance have the CA flag set to TRUE. For instructions, see “Encrypting Communication with Other MTAs” chapter > “Ensuring That the List of Trusted Certificate Authorities in Your Appliance are Common Criteria-Compliant” section.
- Review the following topics:
  - Pushing Logs to a Remote Server Using SCP May Require Configuration Changes

Pushing Logs to a Remote Server Using SCP May Require Configuration Changes

If you have configured your appliance to push your subscribed logs to a remote server using Secure Copy (SCP), do the following after upgrading to AsyncOS 9.8:

Step 1 Log in to your appliance's web interface.

Step 2 Click **System Administration** > **Log Subscriptions**.

Step 3 Edit one of the existing log subscriptions and submit the configuration without making any changes.

Step 4 Copy the new SSH key from the success message displayed on top of the page.

Step 5 Log in to the remote server and edit the `authorized_keys` file.

Step 6 Replace the old SSH key with the new SSH key.

Caution If you do not perform this step, the logs will not be pushed to the remote server after the upgrade.

File Analysis Changes May Require Configuration Changes

Viewing Detailed File Analysis Results in the Cloud

If you have deployed multiple content security appliances (email, web, and/or management) and you want to view detailed file analysis results in the cloud for all files uploaded from any appliance in your organization, you must configure an appliance group on each appliance after upgrading.

For details, see information about grouping appliances in the "File Reputation Filtering and File Analysis" chapter in the user guide PDF.

Verify that Analyzed File Types Have Not Changed

CSCut78133 The File Analysis cloud server URL has changed, and as a result, 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**.

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.

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, page 16
- Lists of Known and Fixed Issues, page 17
- Finding Information about Known and Resolved Issues, page 17

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

Known Issues	**AsyncOS 9.8.1-021**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.8.1-021&sb=afr&bt=custV
	AsyncOS 9.8.1-015	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.8.1-015&sb=afr&bt=custV
	AsyncOS 9.8.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.8.0&sb=afr&bt=custV

Fixed Issues	**AsyncOS 9.8.1-021**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.8.1-021&sb=fr&bt=custV
	AsyncOS 9.8.1-015	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.8.1-015&sb=fr&bt=custV
	AsyncOS 9.8.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.8.0&sb=fr&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 the version of the release, for example, 9.8.

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 18.

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

Note To get support for virtual appliances, have your Virtual License Number (VLN) number ready when you call Cisco TAC.

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site for legacy IronPort: http://www.cisco.com/web/services/acquisitions/ironport.html

For non-critical issues, you can also access customer support 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 "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.