Release Notes for AsyncOS 13.0.2 for Cisco Email Security Appliances

Published: November 9, 2020

Revised: February 5, 2024

Contents

What's New In This Release

What's New in AsyncOS 13.0.2

This release contains a Behavior Change and Bug Fixes; see the Changes in Behavior, page 8 and Known and Fixed Issues, page 28 for additional information.

What's New in AsyncOS 13.0.1

This release contains Behavior Changes and Bug Fixes; see the Changes in Behavior, page 8 and Known and Fixed Issues, page 28 for additional information.

What's New in AsyncOS 13.0

Feature	Description
Mailbox Auto Remediation on Microsoft Exchange online, Microsoft Exchange on-premise, hybrid, and multi-tenant deployments	A file can turn malicious anytime, even after it has reached user's mailbox. AMP can identify this as new information emerges and push retrospective alerts to your appliance. You can configure your appliance to perform auto-remedial actions on the messages in user mailbox when the threat verdict changes. The appliance can perform auto-remedial actions on the messages in the following mailbox deployments: • Microsoft Exchange online – mailbox hosted on Microsoft Office 365 • Microsoft Exchange on-premise – a local Microsoft Exchange server • Hybrid/Multiple tenant configuration – a combination of mailboxes configured across Microsoft Exchange online and Microsoft Exchange on-premise deployments For more information, see the "Automatically Remediating Messages in Mailboxes" chapter in the user guide.
Single Sign-On (SSO) using SAML 2.0	The Cisco Email Security appliance now supports SAML 2.0 SSO to allow users to log in to the web interface (both legacy and new web interface) of the appliance using the same credentials used to access other SAML 2.0 SSO enabled services within the organization. For more information, see the "Single Sign-On (SSO) Using SAML 2.0" section in the user guide.
Support for Unified Common Event Format (CEF)-based Logging	The Cisco Email Security appliance now supports a new type of log subscription – 'Consolidated Event Logs' that summarizes each message event in a single log line. Using this log subscription, you can reduce the number of bytes of data (log information) sent to a Security Information and Event Management (SIEM) vendor or application for analysis. The Consolidated Event Logs are in the Common Event Format (CEF) log message format that is widely used by most SIEM vendors. For more information, see the "Logging" chapter in the user guide.

Ability to safe print message attachments	You can configure your email gateway to provide a safe view (safe-printed PDF version) of a message attachment detected as malicious or suspicious. The safe view of the message attachment is delivered to the end user and the original attachment is stripped from the message.
	You can use the 'Safe Print' content filter action to safe print all message attachments that match a configured content filter condition.
	The ability to safe print message attachments in the email gateway helps an organization to:
	• Prevent message attachments with malicious or suspicious content from entering an organization network.
	• View malicious or suspicious message attachments without being affected by the malware.
	• Deliver the original message attachment based on the end-user request.
	For more information, see the "Configuring Email Gateway to Safe Print Message Attachments" chapter in the user guide.
Integrating the Appliance with Cisco Threat Response Portal	You can integrate your appliance with Cisco Threat Response portal, and perform the following actions in Cisco Threat Response portal:
	• View the message tracking data from multiple appliances in your organization.
	• Identify, investigate, and remediate threats observed in the message tracking.
	• Resolve the identified threats rapidly and provide recommended actions to take against the identified threats.
	• Document the threats in the portal to save the investigation, and enable collaboration of information among other devices on the portal.
	For more information, see the "Integrating with Cisco Threat Response Portal" chapter in the user guide.
Performing Threat Analysis using Casebooks	The Cisco Email Security appliance now includes the casebook and pivot menu widgets.
	✎
	Note If you are using the Microsoft Internet Explorer browser to access your appliance, you will not be able to use the casebook widget.
	You can perform the following actions in your appliance using the casebook and pivot menu widgets:
	• Add an observable to a casebook to investigate for any threat analysis.
	• Pivot an observable to a new case, an existing case, or other devices registered in the Cisco Threat Response portal (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis.
	For more information, see the "Integrating with Cisco Threat Response Portal" chapter in the user guide.

Improving User Experience by Collecting Feature Usage Statistics	The Cisco Email Security appliance now collects feature/interface usage statistics on the new web interface of the appliance that helps Cisco improve overall user experience. All data collected is anonymized. If you want to opt-out of this feature, navigate to **System Administration > General Settings > Usage Analytics** page of the web interface to disable it. For more information, see the "Collecting Usage Statistics of the Appliance on the New Web Interface" section in the user guide.
FIPS Certification	Cisco Email Security Appliance will be FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #2984). See the "FIPS Management" chapter in the user guide.
Message Tracking Enhancement	You can now search for messages based on the "Reply-To" header of the message. For more information, see "Tracking Messages" chapter of the user guide.
The *trailblazerconfig* CLI Command	You can use the *trailblazerconfig* command to route your incoming and outgoing connections through HTTPS ports on the new web interface. ✎ **Note** By default, trailblazerconfig CLI command is enabled on your appliance. You can see the inline help by typing the command: help trailblazerconfig. For more information, see "trailblazerconfig" section of the CLI Reference guide.
Metrics Bar Widget	The Metrics Bar widget enables you to view the real time data of the file analysis done by the Cisco Threat Grid appliance on the Advanced Malware Protection report page. For more information, see "Advanced Malware Protection Page" section of the user guide.
Ability to categorize IP addresses as persistent allowed list or blocked list	You can categorize the IP address that you use to access the appliance using SSH as a persistent allowed list or blocked list. If the appliance or the ipblockd service is restarted, the IP address in the persistent blocked list or allowed list is retained. You can use the sshconfig > access control sub command in the CLI to categorize the IP address as a persistent allowed list or blocked list. For more information, see the sshconfig section of the *CLI Reference Guide for AsyncOS 13.0 for Email Security Appliances*.
Forged Email Detection Enhancement	You can now create an exception list consisting of only full email addresses to bypass the Forged Email Detection content filter in **Mail Policies > Address Lists**. You can use this exception list in the Forged Email Detection rule if you want the appliance to skip email addresses from the configured content filter.

New Web Interface for Reporting, Quarantine, and Tracking	The appliance now has a new web interface to search and view: • **Email Reports.** You can now view email reports from the Reports drop-down based on the following categories: – Email Threat Reports – File and Malware Reports – Connection and Flow Reports – User Reports – Filter Reports For more information, see the "Email Security Monitor Pages on the New Web Interface" chapter in the user guide. • **Spam Quarantine** – You can now view and search for spam and suspected spam messages in **Quarantine** > **Spam Quarantine** > **Search** page in the web interface. – You can view, add, and search for domains added in the safelist and blocklist in **Quarantine** > **Spam Quarantine** > **Safelist** or **Blocklist** page in the web interface. For more information, see the "Spam Quarantine" chapter in the user guide. • **Policy, Virus and Outbreak Quarantines.** You can view and search for policy, virus and outbreak quarantines in Quarantine > Other Quarantine > Search page in the web interface. For more information, see the "Centralized Policy, Virus, and Outbreak Quarantines" chapter in the user guide. • **Message Tracking.** You can search for messages or a group of messages depending on your search criteria in **Tracking** > **Search** page in the web interface. For more information, see the "Tracking Messages" chapter in the user guide. **Important!** • Make sure that you have enabled AsyncOS API on the appliance. • Make sure that AsyncOS HTTPS API port is not enabled on multiple interfaces. • By default, `trailblazerconfig` is enabled on the appliance. – Make sure that the configured HTTPS port is opened on the firewall. The default HTTPS port is 4431. – Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance. For more information, see Accessing the New Web Interface, page 17.

Advanced Malware Protection Report Enhancement	The Advanced Malware Protection Report page has the following enhancements: • A new section - **Incoming Malware Files by Category** to view the percentage of blocked file SHAs received from the AMP for Endpoints console that are categorized as **Custom Detection**. The threat name of a blocked file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report. • A new section - **Incoming Malware Files by Category** to view the percentage of blocked file SHAs based on the threshold settings that are categorized as **Custom Threshold**. • You can click on the link in the More Details section of the report to view the file trajectory details of a blocked file SHA in the AMP for Endpoints console. • A new verdict - **Low Risk** is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the Incoming Files Handed by AMP section of the report. For more information, see the "Email Security Monitor pages on the New Web Interface" chapter in the user guide.

Anti-Spam Scanning Configuration Enhancement	A new 'Aggressive' scanning profile is added to the Anti-Spam global settings. You can use this profile to assign a higher priority on incoming or outgoing messages detected as spam, and to accept a higher chance of false positives.
	✎ **Note**	**Note**: If aggressive scanning profile option is enabled, the mail policy adjustments to Anti-Spam thresholds have a larger impact than when a Normal profile scanning is used. Therefore, you must review the existing Anti-Spam mail policy thresholds settings for the best balance of spam catch rate versus false positive potential.
	You can enable this option in any one of the following ways: • **Security Services** > **IronPort Anti-Spam** > **Edit Global Settings** in the web interface. See the "Managing Spam and Graymail" chapter in the user guide. • `antispamconfig` command in the CLI. See the *CLI Reference Guide for AsyncOS 13.0 for Email Security Appliances*.
New Walkthroughs available on the How-Tos Widget	The How-Tos is a contextual widget that provides in-app assistance to users in the form of walkthroughs to accomplish complex tasks on your appliance. The following are the walkthroughs that are added in this release: • Single Sign-On Using SAML 2.0 • Remediate Malicious Messages in the Mailboxes Using Mailbox Auto Remediation • Provide a Safe View of Malicious or Suspicious Message Attachments • Configure Unified Common Event Format (CEF) Logging
	✎ **Note**	The list of walkthroughs is cloud updateable. Make sure that you clear your browser cache to view an updated version of the How-Tos widget and pop-up window.
	For more information, see the "Accessing the Appliance" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*. To view the complete list of walkthroughs supported in each release, see Walkthroughs Supported in AysncOS for Cisco Email Security Appliances.

Changes in Behavior

Changes in Behavior in AsyncOS 13.0.2

File Reputation Service Configuration Changes	There is no option to enable or disable SSL communication when you configure the File Reputation service in your appliance. The appliance uses the SSL protocol by default to communicate with the File Reputation service using firewall port 443 only.
	The following options to configure SSL communication settings for the File Reputation service in your appliance are removed:
	• The **Use SSL (Port 443)** checkbox in Security Services > File Reputation and Analysis page in the web interface of your appliance.
	• The `Do you want to enable SSL communication (port 443) for file reputation? [Y]>` statement in `ampconfig > advanced` sub command in the CLI.

Changes in Behavior in AsyncOS 13.0.1

Content Scanner Changes	The Content Scanner in your appliance can now extract file names at the first nested level of password-protected attachments (.zip format) for messages.
SSL Cipher Configuration Changes	The @STRENGTH parameter is now added to the default SSL cipher strings for Inbound SMTP, Outbound SMTP, and GUI connections.
	Now, all connection requests sent from your appliance (acting as a client) to a remotely configured MTA (acting as a server) will get rejected if the MTA supports only weak ciphers and older TLS methods. The @STRENGTH parameter sorts the cipher list and displays the strongest ciphers at the top of the list. Based on the selected TLS method, the cipher list will not contain all the weak ciphers.
Changes in Sophos Anti-Virus Configuration Settings on Appliance	Prior to this release, the StrongPDF option was automatically enabled by default in the Sophos Anti-Virus engine in your appliance. The Sophos Anti-Virus engine used the StrongPDF option to categorize clean PDF files that were corrupted as "unscannable" because of EOF (End-of-File) missing, and so on.
	After you upgrade to this release, the StrongPDF option is disabled by default. The Sophos Anti-Virus engine now automatically categorizes clean PDF files that were corrupted as "clean" because of EOF (End-of-File) missing, and so on.
	You can use the `antivirusconfig > PDF` sub command in the CLI to enable the StrongPDF option on the Sophos Anti-Virus engine in your appliance.
File Reputation Query Timeout Changes	The appliance now adds extra buffer time of 2 seconds to the total timeout period during the file reputation query process.

Changes in Behavior in AsyncOS 13.0

Change in Report Pages	The following reports are changed on the new web interface, in this release: • My Dashboard page is renamed to My Reports. • Incoming Mail page is renamed to Mail Flow Summary. • Outbreak Filters report page is renamed to Outbreak Filtering. • Virus Types report page is renamed to Virus Filtering. • Advanced Malware Protection, AMP File Analysis, AMP Verdict Updates and Mailbox Auto Remediation report pages are merged as Advanced Malware Protection. • Incoming Mail and Outgoing Senders report pages are merged as Mail Flow Details. • TLS Connections report page is renamed to TLS Encryption. • Geo-Distribution report page is renamed to Connection by Country. • Internal Users report page is renamed to User Mail Summary. • Web Interaction Tracking report page is renamed to Web Interaction. For more information, see "Understanding the Email Reporting Pages" section in the user guide.
Changes in Accessing the Spam Quarantine	• The administrative users can now access the Spam Quarantine page on the new web interface of the appliance. You can navigate to **Quarantine** > **Spam Quarantine** > **Search** page on the new web interface to access the Spam Quarantine page. • The end-users can now access the Spam Quarantine portal on the new web interface, For more information, see Accessing the New Web Interface, page 17. **Important!** Only end users can log in to the end-user spam quarantine portal. Local and externally-authenticated users cannot log in to the end-user spam quarantine portal. • You will now receive spam notification with a link to view the quarantined messages on the new web interface. Make sure that you have enabled AsyncOS API HTTP/HTTPS ports and HTTPS service on the appliance. • If you are using spam quarantine on the any other interface (Data 1), then you must set it as the default interface. **Important!** If the `trailblazerconfig` is enabled, then you must enable the AsyncOS API ports (HTTP/HTTPS) and HTTP/HTTPS service on the (Data 1) interface. If the `trailblazerconfig` is disabled, then you must enable the AsyncOS API ports (HTTP/HTTPS) on the (Data 1) interface.

Cluster Support on the New Web Interface	In case of a cluster configuration, you can view the reporting data and viewing and searching of quarantine data of only the login host on the new web interface.
Context Adaptive Scanning Engine (CASE) Improvements	The following are the CASE improvements: • Additional message metadata and information about URLs in the message attachments are available to the CASE. • Improvements in the utilization of URL intelligence in the Outbreak Filters quarantine exit scan provide greater detection of Phishing and other URL-based threats.
Changes when scanning attachments with long file names	If the file name of the attachment contains more than 255 characters, the attachment and files within the attachment are marked as unscannable and not processed further in the email pipeline. The Message Tracking page and the AMP log display the truncated file name in the following format: `<First 225 characters of original filename+'~too_long_name~'+the last ten characters of original filename>`
Enhancements to Mailbox Auto Remediation feature	Prior to this release, when you configure a delete remedial action on a malicious message, the message does not deleted from certain folders such as Deleted Items. After you upgrade to this release, the message is deleted permanently from all folders in the mailbox.
Changes to API version support in AsyncOS 13.0	After you upgrade to this release, AsyncOS 13.0 supports only API version 2.0 instead of version 1.0.
Changes to LDAP connection settings	While creating LDAP server profile on the appliance, you can now configure the maximum time (in seconds) for which the connections to the LDAP server must persist before the connections reset. Choose a value between 60 and 86400. You can configure the value in any one of the following ways: • **System Administration** > **LDAP** > **Add LDAP Server Profile** in the web interface. See the "Creating LDAP Server Profiles to Store Information About the LDAP Server" section in the user guide. • `ldapconfig` command in the CLI. See the "CLI Reference Guide for AsyncOS for Cisco Email Security Appliances."
Changes while loading the configuration file for File Analysis	The following are the behavior changes when you load the configuration file for File analysis using **Configuration File > Load Configuration** option in the web interface: • The file types under the file groups are selected as per the configuration file and the other file types remain unselected. • You cannot add a new file type or change the group for the file type using the Load Configuration option.
Changes in Self-Signed Certificates	Prior to this release, the appliance used SHA-1 signature hash algorithm to create a self-signed certificate. After you upgrade to this release, the appliance uses the SHA-256 signature hash algorithm to create self-signed certificates.

Username Length Changes	Prior to this release, the username length was limited to 16 characters. After you upgrade to this release, the username length is limited to 32 characters.
Changes in Demo Certificates	Prior to this release, the appliance was pre-configured with a demonstration certificate to enable the TLS connections. After you upgrade to this release, the appliance generates a unique certificate to enable TLS connection. The existing demonstration certificate that is used in the following configurations are replaced with the new certificate: • Mail Delivery • LDAP • •Networking • URL Filtering • SMTP Services
Changes to Cross-Site Scripting Attack Protection configuration	Prior to this release, the Cross-Site Scripting Attack Protection (XSS) is disabled by default. After you upgrade to this release, XSS is enabled by default. You can use the adminaccessconfig command in the CLI to change the configuration.
Changes in Attachment File Info content or message filter	When you configure an 'Attachment File Info' content or message filter in your appliance based on any one of the following conditions: • Select the 'Filename' option, choose either 'Does Not Equal,' 'Does Not Contain,' 'Does Not End With,' or 'Does Not Begin With' options, and enter a file name. • Select the 'File type' option, choose the 'Is not' option and choose the file type from the drop-down list. • Select the 'MIME type' option, choose the 'Is Not' option, and enter the MIME type. The appliance now performs the configured action on messages with attachments and matches any one of the above conditions.
Changes in LDAP Server Profiles using SSL	After you upgrade to this release, LDAP server profiles do not use SSL by default. This happens when you upgrade your appliance from an AsyncOS version where the secure LDAP is disabled.
DMARC Aggregate Reports Changes	You can now use the dmarcconfig command in the CLI to configure the maximum limit of DMARC aggregate reports that can be generated per day. The default value for the number of DMARC aggregate reports generated per day is 1000, and the maximum value is 50K. It is recommended that you schedule the generation of DMARC aggregate reports during non-peak hours to avoid impact on mail flow. If you generate a higher number of DMARC aggregate reports, you might experience a slight delay in email delivery during non-peak hours for a longer duration.

Changes in Character Encoding supported for Data Loss Prevention (DLP)	Data Loss Prevention (DLP) now supports the following character encodings for multi-byte plain text files in Chinese, Japanese and Korean languages: • Traditional Chinese (Big5) • Simplified Chinese (GB2312) • Korean (KS-C-5601/EUC-KR) • Japanese (Shift-JIS(X0123)) • Japanese (EUC). However, Data Loss Prevention (DLP) does not support the following character encodings: • Japanese (ISO-2022-JP) • Korean (ISO2022-KR) • Simplified Chinese (HZGB2312)
Changes in Threshold Value for Memory Page Swapping	Prior to this release, the default threshold level for memory page swapping was measured based on the number of pages. After you upgrade to this release, you can now configure your appliance to measure the threshold value for memory page swapping in percentage. The default threshold value for memory page swapping is set to 10%.
SSL Configuration Changes	After you upgrade to this release, you cannot enable TLS v1.0 and v1.2 methods simultaneously. However, you can enable these methods in conjunction with the TLS v.1.1 method, when you configure SSL settings.
Changes in configuring Domain Keys/DKIM Verification	Prior to this release, if your appliance is in the FIPS mode, you could only use 2048-bit DKIM keys to verify incoming messages. After you upgrade to this release, if your appliance is in the FIPS mode, you can verify your incoming messages using 1024, 1536, or 2048-bit DKIM keys.
Changes to Passphrase Settings	The option to automatically generate a login passphrase is removed. You must now manually enter a passphrase of your choice.

Changes to URL Defang Action	Prior to this release, when you apply the defang action for a URL, the URL becomes unclickable, but you could view and copy the URL.
	After you upgrade to this release, when you apply the defang or replace action for a URL, the URL matching the condition is completely removed from the hyperlink.
	Note Make sure that you have disabled the auto-format settings on your email client to make the URLs unclickable.
Changes in Mail Policy Settings	After you upgrade to this release, you can set the priority in which the appliance checks for message headers in the incoming and outgoing messages. The appliance first checks for the message header with the highest priority for all the mail policies. If there is no header match in any of the mail policies, the appliance looks for the next message header in the priority list for all the mail policies. If none of the message headers match in any of the mail policies, the default mail policy settings are used.

Comparison of Web Interfaces, New Web Interface vs. Legacy Web Interface

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Landing Page	After you log in to the appliance, the Mail Flow Summary page is displayed.	After you log in to the appliance, the My Dashboard page is displayed.
Reports Drop-down	You can view reports for your appliances from the Reports drop-down.	You can view reports for your appliance from the **Monitor** menu.
My Reports	Choose **My Reports** from the Reports drop-down.	You can view the My Reports page from **Monitor > My Dashboard**.
Mail Flow Summary	The **Mail Flow Summary** page includes trend graphs and summary tables for incoming and outgoing messages.	The **Incoming Mail** includes graphs and summary tables for the incoming and outgoing messages.
Advanced Malware Protection Report Pages	The following sections are available on the **Advanced Malware Protection** report page of the Reports drop-down menu: • Summary • AMP File Reputation • File Analysis • File Retrospection • Mailbox Auto Remediation	The appliance has the following Advanced Malware Protection report pages under **Monitor** menu: • Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Mailbox Auto Remediation
Outbreak Filters Page	The Past Year Virus Outbreaks and Past Year Virus Outbreak Summary are not available in the **Outbreak Filtering** report page of the new web interface.	The **Monitor > Outbreak Filters** page displays the Past Year Virus Outbreaks and Past Year Virus Outbreak Summary.
Spam Quarantine (Admin and End-User)	Click **Quarantine > Spam Quarantine > Search** on the new web interface to access the Spam Quarantine page. For more information on the end-users access to the Spam Quarantine portal on the new web interface, see Accessing the New Web Interface, page 17.	-You can view spam quarantine from the **Monitor > Spam Quarantine** menu.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Policy, Virus and Outbreak Quarantines	Click **Quarantine** > **Other Quarantine** on the new web interface. You can only view Policy, Virus and Outbreak Quarantines on the appliance.	You can view, configure and modify the Policy, Virus and Outbreak Quarantines on the appliance using the **Monitor** > **Policy, Virus and Outbreak Quarantines**.
Select All action for Messages in Quarantine	You can select multiple (or all) messages in a quarantine and perform a message action, such as, delete, delay, release, move, etc.	You cannot select multiple messages in a quarantine and perform a message action.
Maximum Download Limit for Attachments	The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.	-
Rejected Connections	To search for rejected connections, click **Tracking** > **Search** > **Rejected Connection** tab on the appliance.	-
Query timeout field	The **Query timeout** field of the Message Tracking feature is not available on the appliance.	You can set the query timeout in the Query Settings field of the Message Tracking feature.
Message Tracking Data Availability	Click the gear icon on the upper right side of the page the web interface to access Message Tracking Data Availability page.	You can view the missing-data intervals for your appliance.
Verdict Charts and Last State Verdicts	Verdict Chart displays information of the various possible verdicts triggered by each engine in your appliance. Last State of the message determines the final verdict triggered after all the possible verdicts of the engine.	Verdict Charts and Last State Verdicts of the messages are not available.
Message Attachments and Host Names in Message Details	Message attachments and host names are not displayed in the Message Details section of the message on the appliance.	Message attachments and host names are displayed in the Message Details section of the message.
Sender Groups, Sender IP, SBRS Score and Policy Match in Message Details	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is displayed in the Message Details section of the message on the appliance.	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is not available in the Message Details section of the message.
Direction of the Message (Incoming or Outgoing)	Direction of the messages (incoming or outgoing) is displayed in the message tracking results page on the appliance.	Direction of the messages (incoming or outgoing) is not displayed in the message tracking results page.

Accessing the New Web Interface

The new web interface provides a new look for monitoring reports, quarantines and searching for messages.

Prerequisites

- The new web interface of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the `trailblazerconfig enable <port number>` command in the CLI to enable trailblazer on a custom port other than 4431.

- You must also change the corresponding firewall rules and proxy rules so that the port is accessible. Make sure that the trailblazer HTTPS port is opened on the firewall.

- Ensure that the AsyncOS API HTTP and AsyncOS API HTTPS ports on **Network** > **IP Interfaces** are enabled. The default AsyncOS API HTTP/HTTPS port is 6080/6443.

You can access the new web interface in any one of the following ways:

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/ng-login`

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

- Log into the appliance and click **Email Security Appliance is getting a new look. Try it !** to navigate to the new web interface.

The new web interface opens in a new browser window and you must log in again to access it. If you want to log out of the appliance completely, you need to log out of both the new and legacy web interfaces of your appliance.

For a seamless navigation and rendering of HTML pages, Cisco recommends using the following browsers to access the new web interface of the appliance (AsyncOS 13.0 and later):

- Google Chrome (Latest Stable Version)
- Mozilla Firefox (Latest Stable Version)

You can access the legacy web interface of the appliance on any of the supported browsers.

The supported resolution for the new web interface of the appliance (AsyncOS 13.0 and later) is between 1280x800 and 1680x1050. The best viewed resolution is 1440x900, for all the browsers.

> **Note** Cisco does not recommend viewing the new web interface of the appliance on higher resolutions.

The end-users can now access the Spam Quarantine on the new web interface in any one of the following ways:

> **Note** The end-users cannot log in to the Spam Quarantine portal on the new web interface using the interface ports 82/83.

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/euq-login`.

where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

Upgrade Paths

Upgrading to Release 13.0.2-030- MD (Maintenance Deployment)

You can upgrade to release 13.0.2-030 from the following versions:

- 11-0-3-242
- 11-0-3-251
- 11-1-0-135
- 11.1.1-108
- 11.1.2-023
- 12.0.0-419
- 12.1.0-071
- 12.1.0-087
- 12.1.0-091
- 12.5.1-037
- 12.5.2-011
- 13.0.0-392
- 13.0.0-403
- 13.0.1-030

Upgrading to Release 13.0.1-030- MD (Maintenance Deployment)

You can upgrade to release 13.0.1-030 from the following versions:

- 11-0-3-242
- 11-1-0-135
- 11-1-1-108
- 11-1-2-023
- 12-0-0-419
- 12-1-0-071

- 12-1-0-087
- 12-5-1-037
- 12-5-2-011
- 13-0-0-392
- 13-0-0-403
- 13-0-1-018

Upgrading to Release 13.0.0-392- GD (General Deployment)

You can upgrade to release 13.0.0-392 from the following versions:

- 11.0.3-238
- 11.0.3-242
- 11.0.3-251
- 11.1.0-135
- 11.1.2-023
- 11.1.3-009
- 11.5.0-076
- 12.0.0-419
- 12.1.0-071
- 12.1.0-087
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-031
- 12.5.1-037
- 13.0.0-314
- 13.0.0-375

Upgrading to Release 13.0.0-375- LD (Limited Deployment) Refresh

You can upgrade to release 13.0.0-375 from the following versions:

- 11.0.0-274
- 11.1.3-009
- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059

- 12.5.0-066
- 12.5.1-031
- 12.5.1-037
- 13.0.0-314

Upgrading to Release 13.0.0-314 - LD (Limited Deployment)

You can upgrade to release 13.0.0-314 from the following versions:

- 11.1.3-009
- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 13.0.0-252
- 13.0.0-285
- 13.0.0-305

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 a user with administrator privileges to upgrade. Also, you must reboot the appliance after upgrading.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models - C190, C195, C390, C395, C690, C695, and C695F.

  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
- C170, C370, C370D, C670 and X1070
- C380 and C680 appliances

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 21.

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 30, 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:

- Upgrading from Previous AsyncOS Version in FIPS Mode to AsyncOS 13.0 in FIPS Mode, page 22
- Upgrading from AsyncOS 11.x to AsyncOS 13.x, page 22
- Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels, page 24

Upgrading from Previous AsyncOS Version in FIPS Mode to AsyncOS 13.0 in FIPS Mode

If you are upgrading your appliance that is in FIPS mode with Centralized Policy, Virus, and Outbreak Quarantines enabled, the Centralized Policy, Virus, and Outbreak Quarantines is disabled after the upgrade. The Centralized Policy, Virus, and Outbreak Quarantines is disabled because to a FIPS-related change in AsyncOS 13.0 for Email. From AsyncOS 13.0 for Email onwards, the appliance in FIPS mode uses a certificate of size 2048 bits to enable Centralized Policy, Virus, and Outbreak Quarantines. The earlier AsyncOS versions have certificates of size 1024 bits.

Follow these steps to enable the Centralized Policy, Virus, and Outbreak Quarantines:

Step 1 Upgrade the Cisco Security Content Management appliance to AsyncOS 13.0.

Step 2 Upgrade your Cisco Email Security appliance to AsyncOS 13.0.

After the upgrade, the Centralized Policy, Virus and Outbreak Quarantines setting will be disabled.

Step 3 On the upgraded AysncOS 13.0 Cisco Security Content Management appliance, run the `updatepvocert` command on the CLI.
The CA certificate for Centralized Policy, Virus, and Outbreak Quarantines is updated to 2048 bits.

Step 4 On the upgraded AysncOS 13.0 Cisco Email Security appliance, verify if the Centralized Policy, Virus, and Outbreak Quarantines is enabled. For more information, see *Cisco Security Content Management Appliance User Guide*.

Upgrading from AsyncOS 11.x to AsyncOS 13.x

If your appliance is in a clustered environment and if you are using SSH-DSS keys for host key verification, the cluster communication fails after you upgrade from AsyncOS 11.x to 13.x. You need to add the SSH-RSA keys to your appliance for host key verification.

Note The cluster communication will not fail if the cluster machines are using SSH-RSA keys for host key verification.

Step 1 Delete the SSH-DSS keys used in all the appliances in the cluster as follows:

   a. Log in to any one of the appliances in the cluster using the CLI.

b. Type the command, `logconfig`. In the following example, the `logconfig` command is used to delete the SSH-DSS host keys.

```
mail1.example.com: logconfig
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig
Currently installed host keys:
1. 10.10.2.21 ssh-dss AAAAB3NzaC1kc3MAAACBAKW24h8U6GiAu+5...D9D66DqZM=
2. 10.10.2.28 ssh-dss AAAAB3NzaC1yc2EAAAADAQABAAABAQC+bgQ...J2jsmTC2i=
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> delete
Enter the number of the key you wish to delete.
[]> 1
Currently installed host keys:
1. 10.10.2.28 ssh-dss AAAAB3NzaC1yc2EAAAADAQABAAABAQC+bgQ...J2jsmTC2i=
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
```

c. Repeat steps a - b for all the other appliances in the cluster.

Step 2 Save the current configuration of the appliances in the cluster.

Step 3 Disconnect all the machines from the cluster.

Step 4 Upgrade each machine individually from AsyncOS 11.x to 13.x

Step 5 Reconnect any one of the machines to the cluster and add the SSH-RSA host keys as follows:

a. Log in to any one of the appliances in the cluster using the CLI.

b. Type the command, `clusterconfig`.
In the following example, the `clusterconfig` command is used to reconnect the first machine to the cluster and add the SSH-RSA host keys.

```
(Machine mail1.example.com) [Disconnected]> clusterconfig
This command is restricted to "cluster" mode.  Would you like to switch to "cluster"
mode? [Y]> Y
```

```
This machine (mail.example.com) is currently disconnected from the cluster.
Do you want to reconnect to the cluster? [Y]> Y
This machine (mail.example.com) is not able to communicate with the cluster.
Host keys need to be updated
Continue? [Y]> Y
Is this the first machine being connected back into the cluster? [N]> Y
Host keys updated successfully....
Commit sent to 1 of 2 machines.  Use the "commitdetail" command for more information.
```

    c. Repeat steps a - b for all the other appliances in the cluster.

Step 6   Log in to any one of the machines in the cluster and reconnect all the other machines to the cluster.

Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels

Before you upgrade to AsyncOS 13.0, ensure that the Intelligent Multi-Scan and Graymail configurations are at the same cluster level. If not, you must review the Intelligent Multi-Scan and Graymail settings after the upgrade.

FIPS Compliance

AsyncOS 13.0 GD is FIPS certified and has the integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #2984).

Reverting to Previous AsyncOS Versions

The following AsyncOS versions are affected by the Internal Testing Interface Vulnerability (http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa):

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047
- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

Upgrading Deployments with Centralized Management (Clustered Appliances)

If a cluster includes C160, C360, C660, X1060, C170, C370, C670, C380, C680, or X1070 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, x70, and x80 hardware cannot be upgraded to this release. If necessary, create a separate cluster for your x60, x70, and x80 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.

IPMI Messages During Upgrade

If you are upgrading your appliance using CLI, you may observe messages related to IPMI. You can ignore these messages. This is a known issue.

Defect ID: CSCuz28415

Changes when configuring Mailbox Auto Remediation (MAR)

If you have already configured MAR on your appliance, make sure that you change the permission from Outlook API to Graph API on your application in the Microsoft Azure portal before you upgrade.

TLS 1.0 Support for Cisco Email Encryption Service

TLS 1.0 support for Cisco Email Encryption service will be disabled by June 2020. If you are using the Easy Open feature of the Cisco Email Encryption service, it is mandatory to upgrade your appliance to AsyncOS 12.5.1 or higher version.

Upgrading to This Release

Before You Begin

- Clear all the messages in your work queue. You cannot perform the upgrade without clearing your work queue.
- Review the Known and Fixed Issues, page 28 and Installation and Upgrade Notes, page 20.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 21.

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 work 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.

- Review the Performance Advisory, page 27.

Post-Upgrade Notes

- Reregistering Appliance with Cisco AMP for Endpoints Console, page 26
- Enabling Centralized Policy, Virus, and Outbreak Quarantines Setting on AsyncOS 13.0 in FIPS Mode, page 26
- Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 13.x, page 27
- Intelligent Multi-Scan and Graymail Global Configuration Changes, page 27

Reregistering Appliance with Cisco AMP for Endpoints Console

After you upgrade to this release, if you have already registered your appliance with the Cisco AMP for Endpoints console, it is recommended to deregister and reregister your appliance with the Cisco AMP for Endpoints console.

Enabling Centralized Policy, Virus, and Outbreak Quarantines Setting on AsyncOS 13.0 in FIPS Mode

When you upgrade from a previous AsyncOS version that is in non-FIPS mode to AsyncOS 13.0, the appliance retains the Centralized Policy, Virus, and Outbreak Quarantines setting. After the upgrade, if you enable FIPS mode, the Centralized Policy, Virus, and Outbreak Quarantines setting will be automatically disabled. The Centralized Policy, Virus, and Outbreak Quarantines setting is disabled because, from AsyncOS 13.0 onwards, the appliance in the FIPS mode uses the CA certificate of 2048 bits to enable Centralized Policy, Virus, and Outbreak Quarantines setting. The earlier AsyncOS versions have CA certificates of 1024 bits.

To enable the Centralized Policy, Virus, and Outbreak Quarantines setting, see Upgrading from Previous AsyncOS Version in FIPS Mode to AsyncOS 13.0 in FIPS Mode, page 22.

Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 13.x

After upgrading to AsyncOS 13.x, if your appliances are in the cluster mode and DLP is configured, inconsistency in the DLP settings is seen when you run the `clustercheck` command using the CLI.

To resolve this inconsistency, force the entire cluster to use the DLP configuration of any of the other machines in the cluster. Use the following prompt "`How do you want to resolve this inconsistency?`" in the `clustercheck` command as shown in the following example:

```
(Cluster)> clustercheck

Checking DLP settings...

Inconsistency found!

DLP settings at Cluster test:

mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com

mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com

How do you want to resolve this inconsistency?

1. Force the entire cluster to use the mail1.example.com version.

2. Force the entire cluster to use the mail2.example.com version.

3. Ignore.

[3]>
```

Intelligent Multi-Scan and Graymail Global Configuration Changes

The following are the changes to the global settings configuration for Intelligent Multi-Scan (IMS) and Graymail after you upgrade to AsyncOS 13.0:

- If the global settings of IMS and Graymail are configured at different cluster levels, the appliance copies the global settings to the lowest configuration level. For example, if you configure IMS at the cluster level and Graymail at the machine level, the appliance copies the IMS global settings to the machine level.

- If the maximum message size and timeout values for scanning messages are different, the appliance uses the maximum timeout and maximum message size values to configure the IMS and Graymail global settings. For example, if the maximum message size values for IMS and Graymail are 1M and 2M respectively, the appliance uses 2M as the maximum message size value for both IMS and Graymail.

Performance Advisory

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

Register for a Cisco account if you do not have one. Go to https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Lists of Known and Fixed Issues

Known and Fixed Issues for AsyncOS 13.0.2

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.0.2&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.0.2-030&prdNam=Cisco%20Secure%20Email%20Gateway

Known and Fixed Issues for AsyncOS 13.0.1

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.0.1&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.0.1-030&prdNam=Cisco%20Secure%20Email%20Gateway

Known and Fixed Issues for AsyncOS 13.0

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.0.0&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.0.0-392&prdNam=Cisco%20Secure%20Email%20Gateway

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://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

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 Secure Email Gateway**, and click **OK**.

Step 4   In Releases field, enter the version of the release, for example, 13.0.2

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

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.
Cisco Secure Email and Web Manager	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email Gateway	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 Secure Email Encryption Service	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.