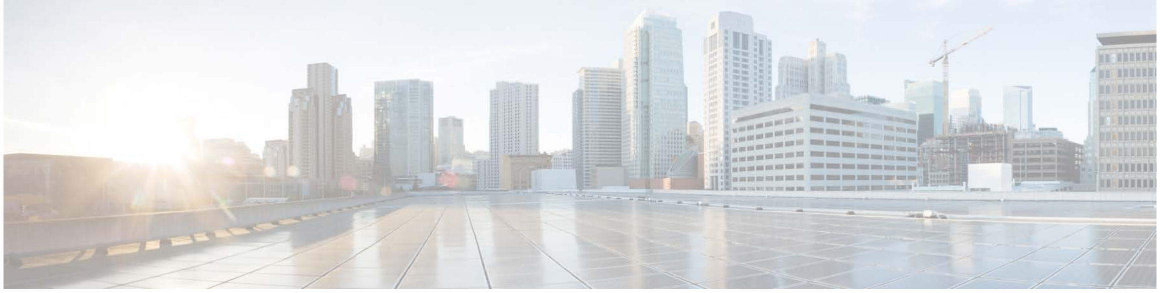

Release Notes for AsyncOS 14.3 for Cisco Secure Email Cloud Gateway

Published: October 11, 2022
Revised: February 16, 2024

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Integrating Secure Email Cloud Gateway with Threat Defense	The Threat Defense Connector client connects the Secure Email Cloud Gateway with the Secure Email Threat Defense to scan messages for Advanced Phishing and Spoofing. When you configure the Threat Defense Connector, the Secure Email Cloud Gateway sends a copy of the actual message as an attachment to the Threat Defense portal's message intake address. The message gets delivered to the user inbox, and advanced scanning completes in the Threat Defense portal. You can enable the Threat Defense Connector in any of the following ways: • From the **Security Services** > **Threat Defense Connector** page of the web interface. • Using the `threatdefenseconfig` command in the CLI. For more information, see the "Integrating Secure Email Cloud Gateway with Threat Defense" chapter in the user guide or the CLI Reference Guide associated with this release.
No Support for Cisco Secure Email Phishing Defense	From this release onwards, as of December 14, 2022, the Cisco Secure Email Phishing Defense (formerly known as Cisco Advanced Phishing Protection) feature will no longer be supported from Secure Email Cloud Gateway 14.3 onwards. For more details, click here. Contact Cisco Technical Assistance for further assistance. **Note** The above statement does not apply to existing users who have a valid license and are actively using the Cisco Secure Email Phishing Defense feature.
Custom User Role for AMP Configurations	The administrator can define a custom user role that provides access to AMP Configuration, AMP Reports, File Analysis Quarantine, and Message Tracking. The administrator can then assign this custom user role to the delegated administrator. The administrator can define the custom user role for AMP configurations in the following ways: • Navigate to **System Administrator** > **User Role** > **Add User Role** and select **No access** or **Full access** for the AMP Configurations field in the web interface. • Use the `userconfig` > `ROLE` sub command in the CLI and provide appropriate input for the AMP Configurations statement. For more information, see "Distributing Administrative Tasks" chapter in the user guide or the CLI Reference Guide associated with this release.

Consolidated Event Logs Enhancement	In the Consolidated Event Logs, two new fields are added, which can be used to include additional data when integrating your email gateway with the Security Information and Event Management (SIEM) application: • Custom Log Entries • Custom Log Headers You can use the two fields to add a custom header, custom log entry, or both in Consolidated Event Logs. **Note** You can add only 25 custom log headers in Consolidated Event Logs. You can configure the two fields in your email gateway in the following ways: • Custom Log Entry field – Use the **Add CEF Log Entry** Content Filter Action (for incoming or outgoing content filters, whichever is applicable) in the web interface or enter the `Add CEF Log Entry` content filter action under `policyconfig` > `incoming mail policies` or `outgoing mail policies` > `filters` > `new` > `add` > `Action` sub command in the CLI. **Note** The corresponding Message Filter action used is `cef-log-entry`. • Custom Log Header field – Use the **CEF Headers** option in the Log Subscriptions > Global Settings page in the web interface or the `logconfig` > `ceflogheaders` sub command in the CLI. The CEF log entry appears in Consolidated Event Logs when you configure the 'Consolidated Event Logs' log subscription with "Custom Log Entries" or "Custom Log Headers" (whichever is applicable) present in "Selected Log Fields." For more information, see the "Content Filters" and "Logging" chapters in the user guide or the CLI Reference Guide associated with this release.

Using only User-defined Passphrases to open Password-protected Attachments	From this release onwards, you can choose to use only the user-defined passphrases created in your email gateway to open password-protected attachments in incoming and outgoing messages. You can configure this feature in any one of the following ways: • Use the **Apply User-defined Passwords Only** checkbox in the Security Services > Scan Behavior > Edit Global Settings page of the web interface. • Use the `“Do you want to apply user-defined  passwords only? y/n”` statement under `scanconfig` > `protectedattachmentconfig` sub command in the CLI. For more information, see the: • “Configuring Scan Behavior” section in the “Using Message Filters to Enforce Email Policies” chapter of the user guide associated with this release. • "Example - Using Only User-defined Passphrases to Open Password-protected Attachments” section in the “The Commands: Reference Examples” chapter of the CLI Reference Guide associated with this release.

Changes in Behavior

Message Tracking - Remediation Action Changes	[Before this Release]: In the Message Tracking > Remediate > Confirm Remediation Action dialog box, you could enter any special characters in addition to 'a-z,' 'A-Z, ' and '0-9' characters for the 'Remediation Batch Name' and 'Description' fields. [From this Release onwards]: In the Message Tracking > Remediate > Confirm Remediation Action dialog box, you can only enter 'a-z,' 'A-Z, ' '0-9,' '_,' '-' characters, and spaces for the 'Remediation Batch Name' and 'Description' fields.
Changes to Default Log Level Selected for Audit Logs	[Before this Release]: When you would create an 'Audit log' log subscription using the web interface or the CLI, the 'Information' option would be selected as the default log level. [From this Release onwards]: When you create an 'Audit log' log subscription using the web interface or the CLI, the 'Debug' option is selected as the default log level. You can change the log level option if required.

Content Scanner - Maximum File Size Scan Limit Changes	[Before this Release]: The Content Scanner in your email gateway would scan the text contents of the message attachment, even if the size of the extracted text from the attachment exceeded the configured maximum file size scan limit. [From this Release onwards]: The Content Scanner only scans the extracted text contents of the message attachment based on the configured maximum file size scan limit. The remaining text contents that exceed the configured maximum file size scan limit are truncated. **For Example**: You configured the maximum file size limit as 5 MB, and the text contents extracted from the message attachment are more than 5 MB (for example, '8 MB'). The Content Scanner only scans the text contents of a 5 MB file size and truncates the remaining 3 MB file size.
Changes in uploading HTML and Octet-stream Files for File Analysis	[Before this release]: The email gateway could only upload HTML and Octet-stream files (mime type - application/octet-stream and text/html) to the File Analysis server if the file extensions were selected for file analysis. [From this release onwards]: The email gateway can now upload the HTML and Octet-stream files to the File Analysis server for file analysis, even if the file extensions are not selected for file analysis. **Note** As the number of files uploaded to the File Analysis server may increase, the email gateway could potentially reach the file upload limit of the file analysis server quickly.
Changes in uploading Archived Files for File Analysis	[Before this release]: When the AMP engine failed to extract the archive files (including password-protected archived attachments) from a message, the attachments would not be uploaded to the File Analysis server. [From this release onwards]: When the AMP engine fails to extract the archive files (including password-protected archived attachments) from a message, the attachments are now uploaded to the File Analysis server for file analysis. **Note** As the number of files uploaded to the File Analysis server may increase, the email gateway could potentially reach the file upload limit of the file analysis server quickly.

Upgrading to AsyncOS 14.3.0 Release

Upgrading to AsyncOS 14.3.0-032 Refresh Release

You can upgrade to release 14.3.0-032 from the following versions:

- 14.0.0-698
- 14.0.1-033
- 14.0.1-305
- 14.0.2-020
- 14.0.3-015
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.3.0-020
- 14.3.0-023

Upgrading to AsyncOS 14.3.0-023 Release

You can upgrade to release 14.3.0-023 from the following versions:

- 13.5.1-277
- 13.7.0-093
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.0.2-606
- 14.2.0-616
- 14.2.0-620
- 14.3.0-002
- 14.3.0-017

Supported VMs for this Release

The following VMs are supported for this release:

- C100V

- C300V
- C600V

Post-Upgrade Notes

Incorrect Display of External Threat Feeds Package Version

After you upgrade to this release and if your email gateway contains the latest External Threat Feeds (ETF) package, the system displays the default ETF package version as “1.0.0-0000001” and not the actual ETF package version of “2.0.0-005” on the web interface and the CLI. This is only a display issue and has no functional impact. The issue will be fixed in the upcoming release.

Defect ID: CSCwd49783.

Note You can use the `threatfeedstatus` command in the CLI to view the current version of the ETF engine. For more information, see the CLI Reference Guide associated with this release.

Monitoring Status of IP Reputation Service

After you upgrade, you may see the following IP address - 172.0.0.2 in the IP Reputation Debug logs.

The 172.0.0.2 IP address is mainly used to check the availability of the IP Reputation cloud service. This IP address is used internally to check the connectivity of the IP Reputation cloud service and your email gateway. The IP address has no relation to the incoming/outgoing messages or the user network.

DLP Service Status Check

After you upgrade to this release, you might experience an issue with the DLP service.

Solution: Check the status of the DLP service on your email gateway using the `diagnostic` > `services` > `DLP` > `status` sub command in the CLI. If the DLP service is not running, refer to the ’Workarounds’ section of the CSCvy08110 defect available in the Known Issues list. For more information on how to view the Known Issues, see Lists of Known and Fixed Issues, page 9.

Scanning Password-Protected Attachments in Email Gateway

When you configure the Content Scanner in your email gateway to scan the password-protected attachments, there may be a performance impact if your email traffic contains a high percentage of password-protected attachments.

[Smart Licensing users only] Unable to Connect Email Gateway to Cisco Talos Services

If your email gateway is in the Smart Licensing mode and the system time is behind GMT, your email gateway might experience connectivity issues to Cisco Talos Services.

Solution: Make sure that you configure your email gateway to use the NTP server in time settings.

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

After upgrading to AsyncOS 13.x, if your email gateways 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 14.0:

- If the global settings of IMS and Graymail are configured at different cluster levels, the email gateway 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 email gateway copies the IMS global settings to the machine level.
- If the maximum message size and timeout values for scanning messages are different, the email gateway 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

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 appliance causes a minimal reduction in system throughput for nominally loaded appliances. For email gateways 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 want 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 9
- Lists of Known and Fixed Issues, page 9
- Finding Information about Known and Resolved Issues, page 10

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 Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=14.3.0&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=14.3.0-032&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, 14.3

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.

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
Cisco Secure Email Cloud Gateway	https://www.cisco.com/c/en/us/support/security/cloud-email-security/products-user-guide-list.html
CLI Reference Guide for Cisco Secure Email Gateway	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 email gateway. For instructions, see the User Guide or online help.

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.