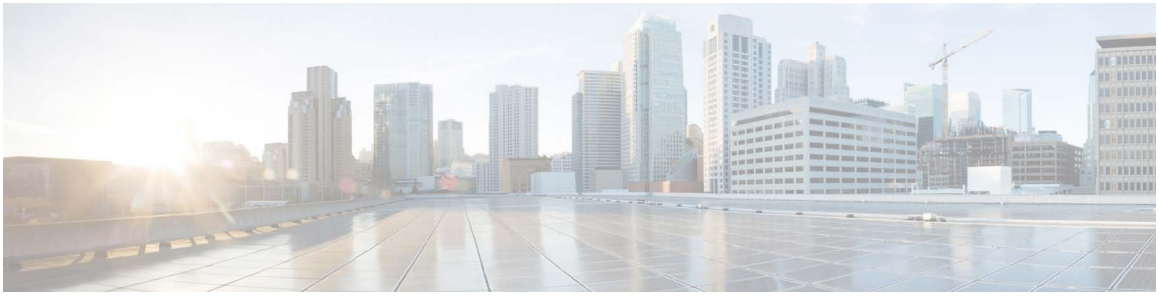

Release Notes for AsyncOS 14.3 Refresh for Cisco Secure Email and Web Manager (Cloud Release Only)

Published: September 29, 2022

Revised: February 16, 2023

Note The AsyncOS 14.3 Refresh for Cisco Secure Email and Web Manager release is a cloud release only.

Contents

Note You must ensure that you provide your email identifier with the domain name while you login the spam quarantine portal.

Cisco Systems, Inc.
www.cisco.com

What's New in this Release

Feature	Description
Custom User Role for AMP	The administrator can define a custom user role that provides access to view the AMP-related reports for all email gateways or the selected Reporting Group. The administrator can then assign this custom user role to a user. The administrator can navigate to **System Administrator > User Role > Add Email User Role and select AMP Reports in Access to data in Reporting Group** or **Access to data in all Email Appliances dropdown list for the Email Reporting field to** create the AMP custom user role. For more information, see "Access to Email Reporting" section in the "Distributing Administrative Tasks" chapter of the user guide.

Changes in Behavior

`Print` and `Clear` subcommands are available for the `Certconfig` command	Before this release, you could not print or clear the different certificates or keys installed for inbound, outbound, HTTPS management access, and LDAPS services. After you upgrade to this release, you can print or clear the different certificates or keys installed for inbound, outbound, HTTPS management access, and LDAPS services. You can use `Certconfig` > `Print` or `Clear` subcommand in the CLI to print or clear the different certificates or keys installed.
JWT token - error message changes	Before this release, when you used JSON Web Token (JWT) token to make any API request, and if the JWT token was expired, the expired token error message was displayed. From this release onwards, when you use the JWT token to make any API request, if the JWT token used is older than 12 hours, an invalid token or expired token error message is displayed. The expired token error message is displayed only up to 12 hours from token generation.
Modifications to the SPoG feature	When you enable or disable SPoG, the session of all the users concurrently logged into the new web interface becomes invalid, and a new request to the server logs them out. The users must log in again. Also, if a Secure Email and Web Manager is added to SPoG, and you are currently logged into the new web interface of the same Secure Email and Web Manager, then you will be logged out due to a change in the flow of JWT validation. **Note** The SPoG feature works only if all the Secure Email and Web Manager under the SPoG cluster have the same version.

Message Tracking - Remediation Action Changes	Before this release, you could enter a-z, A-Z, 0-9, and any special characters for the Remediation Batch Name and Description fields in the Confirm Remediation dialog box. From this release onwards, you can only enter a-z, A-Z, 0-9, _, -, and spaces for the Remediation Batch Name and Description fields in the Confirm Remediation dialog box. Any other special characters are not allowed.
Syslog disk buffer size configuration changes	Before this release, the maximum syslog disk buffer size allowed for syslog push log subscription was 10GB. From this release onwards, the maximum syslog disk buffer size allowed for syslog push log subscription is 1GB. [Applicable for AsyncOS upgrade only]: During the upgrade, the system automatically reduces the maximum disk buffer size value to 1GB if the existing configured value is more than 1 GB before the upgrade. **Note** During the upgrade, if the allocated miscellaneous disk quota exceeds the configured limit, then you need to reduce the maximum disk buffer size value (if the existing configured value is more than 1 GB) to free up the allocated miscellaneous disk quota space to continue the upgrade process.

Accessing the New Web Interface

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

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

- You can use the URL - `https://example.com:4431/ng-login`

  where `example.com` is the appliance host name
- Log into the appliance and click **Security Management 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 12.0 and later):

- Google Chrome (Latest Stable Version)
- Mozilla Firefox (Latest Stable Version)
- Safari (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 12.0 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. To log in to spam quarantine, use the following URL -

`https://example.com:4431/euq-login`

where example.com is the appliance host name.

Note Make sure that the HTTP/HTTPS and the AsyncOS API ports are opened on the firewall.

Upgrading to AsyncOS 14.3.0

Upgrading to AsyncOS 14.3.0-124 Refresh

You can upgrade to release 14.3.0-124 from the 14.3.0-120 version.

Upgrading to AsyncOS 14.3.0-120 Refresh

You can upgrade to release 14.3.0-120 from the 14.3.0-115 version.

Upgrading to AsyncOS 14.3.0-115

You can upgrade to release 14.3.0-115 from the following versions:

- 14.0.0-404
- 14.0.0-418
- 14.1.0-199
- 14.1.0-239
- 14.1.0-250
- 14.2.0-206
- 14.3.0-068

Installation and Upgrade Notes

Important Additional Reading

You should also review the release notes for your associated Email and Web security releases.

For links to this information, see Related Documentation, page 6.

Post-Upgrade Requirements

Spam Notification URL Changes

After you upgrade to Secure Email and Web Manager 14.3, if you cannot log in using the saved spam notification URL, use the new URL mentioned in the spam notification mail.

Supported VMs for this Release

The following VMs are supported for this release:

- M100V
- M300V
- M600V

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 Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&rls=14.3.0&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20IronPort%20Security%20Management%20Appliance%20Software
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&rls=14.3.0&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20IronPort%20Security%20Management%20Appliance%20Software

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://bst.cloudapps.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, 14.2.0

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

In addition to the main documentation in the following table, information about other resources, including the knowledge base and Cisco support community, is in the More Information chapter in the online help and User Guide PDF.

Documentation For Cisco Secure Products:	Is Located At:
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 Email Gateway	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Command Line Reference guide for content security products	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email 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, call Cisco TAC and have your Virtual License Number (VLN) number ready.

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

Support site for legacy IronPort: Visit 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.