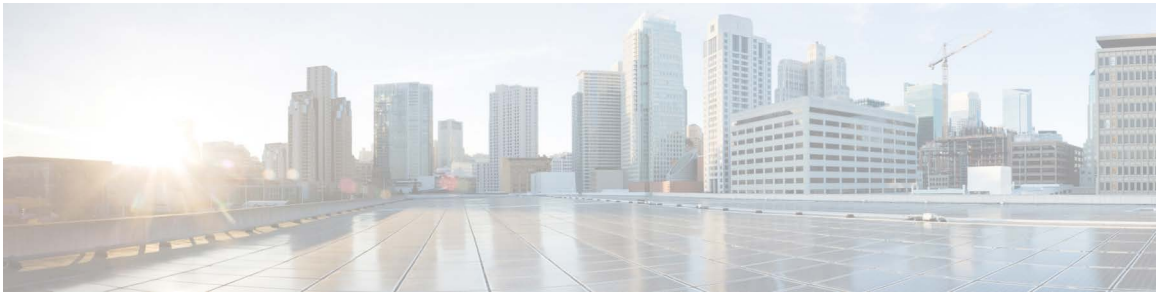

Release Notes for AsyncOS 16.0.2 for Cisco Secure Email and Web Manager (Cloud) - MD (Maintenance Deployment)

Published: May 05, 2025

Contents

- What's New in this Release, page 2
- Changes in Behavior, page 4
- Accessing the New Web Interface, page 5
- Upgrade Paths, page 6
- Installation and Upgrade Notes, page 7
- Supported VMs for this Release, page 10
- Known and Fixed Issues, page 10
- Software Lifecycle Support Statement, page 12
- Related Documentation, page 12
- Service and Support, page 12

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

What's New in AsyncOS 16.0.2-088, page 2
What's New in AsyncOS 16.0.1-010, page 2
What's New in AsyncOS 16.0-195, page 3

What's New in AsyncOS 16.0.2-088

Feature	Description
Resetting Forgotten Passphrase	From AsyncOS 16.0.2 release onwards, cloud administrators can reset their passphrase themselves by clicking the Forgot Passphrase link on the login page. Existing cloud administrators will see a pop-up prompting them to add their email address on the Users page for self-service passphrase reset. Any new cloud administrators created via CLI after the upgrade to AsynOS 16.0.2 will see a pop-up to update their email address when they log into the Legacy Web Interface. For more information, see Resetting Forgotten Passphrase section of the *User Guide for AsyncOS 16.0.2 for Cisco Secure Email and Web Manager*.

What's New in AsyncOS 16.0.1-010

There are no new features in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 10

What's New in AsyncOS 16.0-195

Feature	Description
Regenerating SSH Keys for SCP Push Log Retrieval	Your Secure Email and Web Manager maintains separate host keys for the SCP Push log retrieval. It also allows you to regenerate SSH keys for the SCP Push log retrieval. You can regenerate SSH keys using the `LOGCONFIG` > `HOSTKEYCONFIG` > `REGENERATESCPKEYS` subcommand in the CLI. You can regenerate these new keys only through the CLI and not via the web interface. You must have Administrator or Cloud Administrator privileges to regenerate these new keys. **Note** When you regenerate SSH keys, you need to update these new keys into the SCP log push server. You can verify these new keys using the `LOGCONFIG` > `HOSTKEYCONFIG` > `USER` subcommand in the CLI. For more information, see "Configuring Host Keys" section of the user guide.
Transitioning from SecureX to XDR	SecureX is transitioning to an enhanced and more robust platform, XDR (Extended Detection and Response). As part of this transition, it is essential to integrate your Secure Email and Web Manager with the new XDR platform. For more information on how to integrate Secure Email and Web Manager with XDR, see "Integrating with Cisco XDR" chapter of the user guide.
Enhanced Alert Emails	The Alert emails that you receive from Secure Email and Web Manager when 75% of the disk quota for miscellaneous services is used are enhanced. These emails now include a direct link to a comprehensive Tech Zone article. This Tech Zone article provides detailed solutions to address your technical inquiries related to disk quota management.
Certificate Expiry Alert	Your Secure Email and Web Manager now provides you with timely alerts for the expiry of system certificates (Inbound, Outbound, HTTP, and LDAP) and custom Certificate Authority (CA) certificates. For more information on certificate expiry alert, see "Importing a Custom Certificate Authority List" and "Appliance Certificate Validation" sections of the user guide.

Email Threat Defense Remediation Report	A new report - *Email Threat Defense Remediation* has been added to the Remediation Reports page. For more information on the Email Threat Defense Remediation report, see the "Remediation Reports Page" section of the user guide.
Restarting API Server through CLI	You can now restart the API server using a new CLI subcommand - `API_SERVER`. You can use the `API_SERVER` subcommand to restart and view the status of the API server. The `API_SERVER` subcommand is added under the `diagnostic` > `SERVICES` subcommand. For more information on the diagnostic command and the subcommands, see the " Restarting and Viewing Status of Services Enabled on Appliance" section in the " Common Administrative Tasks" chapter of the user guide.

Changes in Behavior

Changes in Behavior in AsyncOS 16.0.2-088, page 4

Changes in Behavior in AsyncOS 16.0.1-010, page 4

Changes in Behavior in AsyncOS 16.0.0-195, page 5

Changes in Behavior in AsyncOS 16.0.2-088

There are no changes in behavior for this release. For the list of known and fixed issues, see Known and Fixed Issues for AsyncOS 16.0.2-088, page 10

Changes in Behavior in AsyncOS 16.0.1-010

There are no changes in behavior for this release. For the list of known and fixed issues, see Known and Fixed Issues for AsyncOS 16.0.1-010, page 10

Changes in Behavior in AsyncOS 16.0.0-195

Alert Messages for CA Certificates Expiry	Before this release, you did not receive any alert message from Secure Email and Web Manager when Certificate Authority (CA) certificates (added using the `updateconfig -> TRUSTED_CERTIFICATES` CLI subcommand) were about to expire or had already expired. After you upgrade to this release, you receive alert messages from Secure Email and Web Manager whenever CA certificates (added using the `updateconfig -> TRUSTED_CERTIFICATES` CLI subcommand) are about to expire or have expired.
Error Message for SP Certificate Expiry	Before this release, the Secure Email and Web Manager did not display any error message when the Service Provider (SP) certificate expired. After you upgrade to this release, your Secure Email and Web Manager displays an error message to notify you when the SP certificate expires. The Security Assertion Markup Language (SAML) Single Sign-On (SSO) login is also not allowed if the SP certificate has expired.
Enhanced Security for Invalid User Error Messages	From this release onwards, the error message displayed to invalid users is made more generic. This change prevents the identification of valid and invalid account names, thereby enhancing the product's security posture and resiliency.
Changes to Default Settings for Usage Analytics	Before this release, Usage Analytics was enabled by default for fresh installations. From this release onwards, Usage Analytics is disabled by default for fresh installations.
Display Message Changes for Spam-Quarantined Emails Without Message Body	Before this release, if you tried to open a spam-quarantined email and the message body of the email was not found in our file system, your Secure Email and Web Manager displayed an application error message. From this release onwards, if you try to open a spam-quarantined email and the message body of the email is not found in our file system, your Secure Email and Web Manager displays the following message: *The message that you have opened does not contain a message body*.
Visibility of Sender Address to End User	From this release onwards, the sender address will remain visible to the end user until it is deleted from Safelists or Blocklists for all the end-user associated mail IDs and alias IDs.

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 in to 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.

Upgrade Paths

- Upgrading to Release 16.0.2-088 - MD (Maintenance Deployment), page 6
- Upgrading to Release 16.0.1-010 - MD (Maintenance Deployment), page 7
- Upgrading to Release 16.0.0-195 - GD (General Deployment), page 7

Upgrading to Release 16.0.2-088 - MD (Maintenance Deployment)

You can upgrade to release 16.0.2-088 from the following versions:

- 15.0.1-035
- 15.5.1-024
- 15.5.1-029
- 15.5.2-005
- 15.5.3-017
- 16.0.0-195
- 16.0.1-010

Upgrading to Release 16.0.1-010 - MD (Maintenance Deployment)

You can upgrade to release 16.0.1-010 from the following versions:

- 14.2.0-241
- 14.3.0-124
- 15.0.0-418
- 15.5.1-029
- 15.5.2-005
- 15.5.3-017
- 16.0.0-195

Upgrading to Release 16.0.0-195 - GD (General Deployment)

You can upgrade to release 16.0.0-195 from the following versions:

- 15.0.0-413
- 15.0.0-418
- 15.5.1-024
- 15.5.1-029
- 15.5.2-005
- 16.0.0-191

Installation and Upgrade Notes

- Important Additional Reading, page 7
- Pre-Upgrade Notes, page 7
- Post-Upgrade Notes, page 9

Important Additional Reading

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

For links to this information, see Software Lifecycle Support Statement, page 12.

Pre-Upgrade Notes

- Saving Secure Email and Web Manager's Configuration, page 8
- Executing Vault Recovery Process to Resolve Vault Issues, page 8
- Back Up Your Existing Databases, page 9

Saving Secure Email and Web Manager's Configuration

If encryption is enabled on your Secure Email and Web Manager, we recommend you save a copy of your Secure Email and Web Manager's configuration before or after you upgrade to AsyncOS 16.0.

You can load the saved Secure Email and Web Manager's configuration to restore the previous configuration of your device after you execute the Vault Recovery process to restore the Vault service.

You can save the device's configuration using the following ways:

- Navigate to **System Administration > Configuration File** and **select Encrypt passphrases in the configuration files**.
- Use the `saveconfig` command in the CLI and type **2** to select the **Encrypt passphrases** option.

Executing Vault Recovery Process to Resolve Vault Issues

If your Secure Email and Web Manager encounters Vault-related issues before or after you upgrade to AsyncOS 16.0, then you must execute Vault Recovery process to resolve these issues. Perform the following steps to execute the Vault Recovery process:

1. Log in to your Secure Email and Web Manager through a direct SSH connection using the following credentials:

   username: **enablediag**

   password: **admin user's password**
2. Execute the `recovervault` command.
3. Enter the following sequence of subcommands, when prompted:
   a. `yes`
   b. `1 (encryption enabled) or 2 (encryption disabled)`
4. Log in to your Secure Email and Web Manager with administrator user credentials and reboot the device after the Vault Recovery process is complete.
5. [**Only If Encryption is Enabled**] Load a copy of the device's configuration that you had saved earlier to restore previous configuration.
6. Monitor your Secure Email and Web Manager for a couple of hours for any Vault service alerts.

Your Secure Email and Web Manager recovers, and the vault is reinitialized. Now, you can connect to the device without any issues.

Note **Encryption Disabled**

In this scenario, all the system configuration settings are retained.

Encryption Enabled

In this scenario, the following encrypted variables are reset to their default factory values:

- Log Subscriptions
- SAML settings
- LDAP settings
- SNMP settings
- Update settings
- User Config settings

- SMA appliance config settings
- SMA user settings
- CERTCONFIG settings
- Remote Power Cycle settings
- NTP setting for system time settings

If you want to restore the previous configuration, you must load the previously saved configuration file.

Back Up Your Existing Databases

Before you upgrade your Secure Email and Web Manager, back up the existing databases of your Secure Email and Web Manager.

For information on disaster recovery of the Secure Email and Web Manager, see Backing Up Security Management Appliance section in Common Administrative Tasks chapter of the user guide. For detailed steps to schedule a backup process, see Scheduling Single or Recurring Backups section in Common Administrative Tasks chapter of the user guide.

Post-Upgrade Notes

- Alert Emails for Internal Monitoring Purposes, page 9
- TLS 1.0 and TLS 1.1 Deprecation from AsyncOS 16.5 Release, page 9
- Spam Notification URL Changes, page 9

Alert Emails for Internal Monitoring Purposes

After you upgrade to the AsynOS 16.0 release, you may receive alert emails with the subject line "*Filebeat is failing to push logs to Kibana with error*." These alert emails are generated by the Secure Email and Web Manager for internal monitoring purposes. These alerts are intended for our internal operations team as part of enhanced monitoring implementation.

If you receive any of these alert emails, you can safely ignore them. These emails are purely informational and do not indicate any issue with your account or services.

TLS 1.0 and TLS 1.1 Deprecation from AsyncOS 16.5 Release

From the AsyncOS 16.5 release onwards, the TLS versions 1.0 and 1.1 will be removed from CLI and GUI configuration options for HTTPS, LDAP, and Updater.

For more information on TLS versions, see the “Specifying a Secure Communication Protocol” section in the "Common Administrative Tasks" chapter of the User Guide.

Spam Notification URL Changes

After you upgrade to Secure Email and Web Manager 16.0, 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 issues in this release.

- Bug Search Tool Requirements, page 10
- Lists of Known and Fixed Issues, page 10
- Finding Information about Known and Resolved Issues, page 11

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 16.0.2-088

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager&rls=16.0.2,16.0.0,16.0.1
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=16.0.2&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Known and Fixed Issues for AsyncOS 16.0.1-010

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager&rls=16.0.1,16.0.0
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=16.0.1&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Known and Fixed Issues for AsyncOS 16.0.0-195

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager&rls=16.0.0
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=16.0.0&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find the most current information about known and resolved issues.

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, 16.0.

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.

Software Lifecycle Support Statement

For information about software time-based release model and software release support timelines, see Software Lifecycle Support Statement.

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.

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 "Software Lifecycle Support Statement" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2025 Cisco Systems, Inc. All rights reserved.