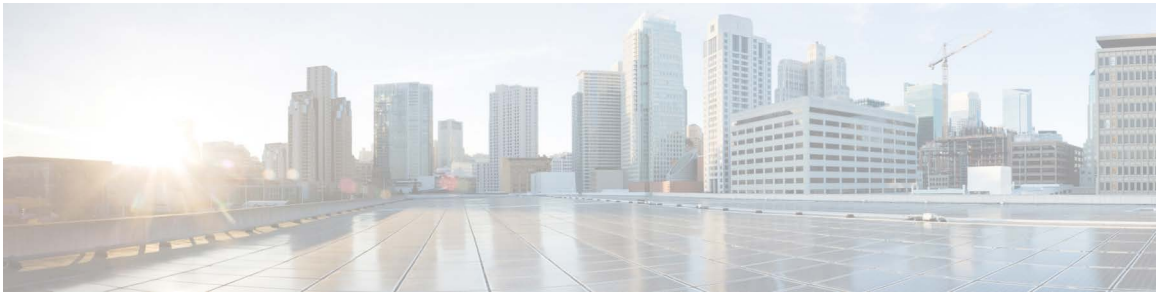

Release Notes for AsyncOS 15.0.2 for Cisco Secure Email and Web Manager (Cloud) - MD (Maintenance Deployment)

Published: January 15, 2026

Revised: March 26, 2026

Contents

- What's New in this Release, page 2
- Changes in Behavior, page 5
- Accessing the New Web Interface, page 11
- Upgrade Paths, page 12
- Installation and Upgrade Notes, page 12
- Supported VMs for this Release, page 14
- Known and Fixed Issues, page 14
- End-of-Sale and End-of-Life Announcement for Cisco SecureX, page 16
- Related Documentation, page 16
- Service and Support, page 17

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 AsynOS 15.0.2-007, page 2
- What's New in AsynOS 15.0.1-035, page 2
- What's New in AsynOS 15.0.0-413, page 2
- What's New in AsynOS 15.0.0-334, page 2

What's New in AsynOS 15.0.2-007

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 14

What's New in AsynOS 15.0.1-035

There are no new features in this release.

What's New in AsynOS 15.0.0-413

This release focuses specifically on IOPS optimization. For more information, see Changes in Behavior in AsyncOS 15.0.0-413, page 5.

What's New in AsynOS 15.0.0-334

Feature	Description
Single Log Line (SLL)	The SLL feature creates, indexes, and stores the email tracking data as a single log line or a flattened model. Therefore, you can execute a query and get a response quickly. This feature boosts the tracking query or search performance through fast response, low memory, and CPU usage. This feature is only applicable to post-upgrade email tracking data.

Configuring CRL Sources	The Secure Email and Web Manager checks a list of revoked certificates called a Certificate Revocation List (CRL) as part of its certificate verification to ensure that the user's certificate has not been revoked. You need to keep an up-to-date version of this list on a server, and the Secure Email and Web Manager downloads it on a schedule you create. You can manually update the list too. You can configure CRL sources using the following ways: • Navigate to **Network > CRL Sources > Add CRL Source > Add CRL (Certificate Revocation Lists) Source** window in the legacy web interface. • Use the `Certconfig > CRL` subcommand in the CLI. For more information on Configuring CRL Sources, see "Configuring CRL Sources" section in the "Common Administrative Tasks" chapter of the user guide.
Removal of Old Splunk Data	When you upgrade to Secure Email and Web Manager 15.0 and later, and if email tracking data is contained in the Splunk database, the system will delete the Splunk database and binaries if you proceed with the upgrade. **Note** From the Secure Email and Web Manager 13.6.2 release onwards, the Splunk database is no longer used for storing email tracking data. All new email tracking data is stored in the Lucene database. After you upgrade to Secure Email and Web Manager 15.0, all tracking data before the upgrade to Secure Email and Web Manager 13.6.2 will be removed and cannot be recovered. **Note** The `debug` submenu used to collect debug information for the Splunk database will be removed from the `Diagnostic > Tracking` subcommand in the CLI.

Resetting the Network Configuration to the Initial Manufacturer Value	A new subcommand `Reload Status` that displays the status of the execution of the last Reload subcommand (that resets the network configuration) is added to the `Diagnostic` command. For more information on this command, See the "Diagnostic - Reload command" and "Diagnostic - Reload Status command" sections in the "Common Administrative Tasks" chapter of the user guide.
Performing X.509 Validation for Peer Certificate during TLS Communication	You can configure your Secure Email and Web Manager to perform X.509 validation for peer certificates. The X.509 validation is applicable for the following services: • Outbound SMTP • LDAP • Updater • Alert over TLS • Syslog Server • Smart Licensing Server • SSE Connector • SSE Server You can configure X.509 validation for Peer Certificate using the following ways: • Navigate to **System Administration > SSL Configuration > SSL Configuration** page on the web interface. • Execute the `sslconfig` command in the CLI. For more information, see the "X.509" section of the "Common Administrative Tasks" chapter in the user guide.
New RAM Value for Secure Email and Web Manager Virtual Appliance Model	From AsyncOS 15.0 release onwards, there is a new RAM value for the M600V Secure Email and Web Manager virtual appliance model deployed through KVM or VMWare ESXi. For more information on the new RAM value applicable for the virtual appliance model, see Cisco Content Security Virtual Appliance Installation Guide.

Changes in Behavior

- Changes in Behavior in AsyncOS 15.0.2-007, page 5
- Changes in Behavior in AsyncOS 15.0.1-035, page 5
- Changes in Behavior in AsyncOS 15.0.0-413, page 5
- Changes in Behavior in AsyncOS 15.0.0-334, page 6

Changes in Behavior in AsyncOS 15.0.2-007

There are no changes in behavior for this release.

Changes in Behavior in AsyncOS 15.0.1-035

There are no changes in behavior for this release.

Changes in Behavior in AsyncOS 15.0.0-413

IOPS Optimization	As part of ongoing performance improvements, the Secure Email and Web Manager is optimized to perform the I/O (read and write) operations efficiently. There are no functional changes made in this release.

Changes in Behavior in AsyncOS 15.0.0-334

SSH Server and Client Configuration Changes	[**Upgrade Scenario**] The following SSH Server and Client Configuration changes are applicable when you upgrade your Secure Email and Web Manager from a lower AsyncOS version to AsyncOS 15.0 version and later. **[SSH Server Configuration Changes]** • The following cipher algorithms, MAC methods, KEX algorithms, and host key algorithm are removed from your Secure Email and Web Manager by default: – **Cipher algorithms** - `rijndael-cbc@lysator.liu.se`, `3des-cbc`, `blowfish-cbc`, `cast128-cbc`, `arcfour`, `arcfour128`, and `arcfour256` – **MAC methods** - `hmac-md5`, `umac-64@openssh.com`, `hmac-ripemd160`, `hmac-ripemd160@openssh.com`, `hmac-sha1-96`, `hmac-md5-96` – **KEX algorithms** - `diffie-hellman-group-exchange-sha256`, `diffie-hellman-group-exchange-sha1`, `diffie-hellman-group1-sha1` – **Host key algorithm** - `rsa1` • The "Minimum Server Key Size" option is removed from the CLI of your Secure Email and Web Manager by default. • The host key algorithm - `rsa-sha2-256` is added to your Secure Email and Web Manager by default. [**SSH Client Configuration Changes**] • The following cipher algorithms - `aes128-gcm@openssh.com`, and `aes256-gcm@openssh.com` are added to your Secure Email and Web Manager by default. • The host key algorithm - `rsa-sha2-256` is added to your Secure Email and Web Manager by default.

SSH Server and Client Configuration Changes	[**Banner Text Changes**] In the System Upgrade banner text, a note is added that informs you that the system will remove weak algorithms in Ciphers, Keys, Kex, and MAC after the upgrade process.
	[**New Install Scenario**] The following SSH server configuration changes are only applicable when you install AsyncOS 15.0 for Cisco Secure Email and Web Manager for the first time. The following cipher algorithms, MAC method, and host key algorithms are supported in your Secure Email and Web Manager: • **Cipher algorithms** - `aes128-ctr`, `aes192-ctr`, `aes256-ctr`, `aes128-cbc`, `aes192-cbc`, and `aes256-cbc` • **MAC method** - `hmac-sha1` • **Host key algorithms** - `rsa-sha2-256`, `ssh-rsa`, and `ssh-dss` (disabled by default) **Note** You need to manually enable the `ssh-dss` cipher algorithm using the `sshconfig` > `sshd` > `setup` subcommand in the CLI. • **KEX algorithms** - `diffie-hellman-group14-sha1`, `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384`, and `ecdh-sha2-nistp521`

X.509 Certificates Changes	[**Upgrade Scenario**] When you upgrade to Secure Email and Web Manger 15.0 and later versions, the system notifies you that the X.509 certificates with less secure signature algorithms are deleted after the upgrade. **Notification Message** *Note: The x509 certificates with less secure signature algorithms are deleted after upgrade if configured.*
	[**New Install Scenario**] The following signature algorithm changes for X.509 certificates are only applicable when you install AsyncOS 15.0 for Cisco Secure Email and Web Manager for the first time: • The following signature algorithms for x509 certificates are no longer supported - `sha1withrsaencryption`, `dsawithsha1`, `sha224withrsaencryption`, `ecdsa-with-sha1`, `ecdsa-with-sha224`, `md2withrsaencryption`, `md4withrsaencryption`, `md5withrsaencryption`, `ripemd128withrsaencryption`, `ripemd160withrsaencryption`, and `ripemd256withrsaencryption`. • The following curves for x509 certificates having ECDSA signature algorithms are not supported - `secp224r1`, `secp192r1`, `brainpoolP160r1`, `brainpoolP192r1`, `secp160r1`, `secp160r2`, `secp192k1`, `secp224k1`, `secp256k1`, `sect163k1`, `sect163r2`, `sect193r1`, `sect193r2`, `sect233k1`, `sect233r1`, `sect239k1`, `sect283k1`, `sect283r1`, `sect409k1`, `sect409r1`, `sect571k1`, and `sect571r1`.

X.509 Certificates Changes	[**Upload Certificate Scenario**] When you upload X.509 certificates with the less secure signature algorithm, you will receive an error message stating the X.509 certificates with the ABC algorithm are less secure. **Error Message** *Error: The x509 certificates with ripemd160WithRSA digest are less secure.*
	[**Loading configuration file Scenario]** **Loading configuration file using CLI** When you load a configuration file through CLI, the system warns you that the X.509 certificates with a less secure signature algorithm are deleted. **Warning Message** *WARNING: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].* **Loading configuration file using GUI** When you load a configuration file through GUI, the system warns you that the X.509 certificates with a less secure signature algorithm are deleted. **Warning Message** *Warnings: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].*
Resetting the Network Configuration to the Initial Manufacturer Value	Before this release, the `Diagnostic > Reload` subcommand was used to remove all user settings and reset the entire device. After you upgrade to this release, along with the previous functionality, this subcommand resets the network configuration to the initial manufacturer value.
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. After you upgrade to this release, 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.
No support for TLSv1.0 for communicatoin between Secure Email and Web Manager and syslog server	Before this release, the Secure Email and Web Manager used TLSv1.0 to communicate with the syslog server irrespective of the TLS version enabled on the syslog server. From this release onwards, the Secure Email and Web Manager uses the highest TLS version enabled on the syslog server. For example, if the highest TLS version on the syslog server is 1.2, then Secure Email and Web Manager uses TLSv1.2 to communicate with syslog server. **Note** TLSV1.0 is not supported now as it is an insecure TLS method.
Notification Message for Phase 2 Backup Process	Before this release, if any service task in the phase 2 backup process was in progress and exceeded 2 hours to complete, a notification message was not sent to the administrator. After you upgrade to this release, if any service task in the phase 2 backup process is in progress and exceeds 2 hours to complete, a notification message is sent to the administrator informing the status of the backup process along with the service name that is taking longer to complete.
Time Zone -> **Country** field changes	From this release onwards, the United States option available in the **Time Zone** ->**Country** field is modified to the United States of America.

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.

Upgrade Paths

Note Make sure you are upgrading to a stable version of Secure Email and Web Manager. Some of the upgrade paths listed in the release notes may be deprovisioned. For more details, refer to Compatibility Matrix > Deprovisioned AsyncOS Releases tab: https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/email-compatibility/index.html

Upgrading to Release 15.0.2-007 - MD (Maintenance Deployment)

You can upgrade to release 15.0.2-007 from the following versions:

- 15.0.0-334
- 15.0.0-413
- 15.0.0-418
- 15.0.1-035
- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224
- 14.2.0-241

Installation and Upgrade Notes

- Important Additional Reading, page 12
- Pre-Upgrade Requirements, page 12
- Post-Upgrade Requirements, page 13

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 16.

Pre-Upgrade Requirements

Security Enhancements in Upgrade Process

The upgrade process incorporates security enhancements. A pre-upgrade security cleanup scan is performed within system directories to identify and remove any malicious files, if present.

Files matching known threat signatures are automatically removed. Legitimate system files and configurations are not affected.

Additional enhancements have been introduced to prevent remote code injection and execution through the user interface, further improving overall system security.

CLI Upgrade Scenario

In a CLI-based upgrade, a security scan is automatically triggered as part of the upgrade process. A warning message indicates that the scan is being performed to detect suspicious files within system directories. Upon completion, scan results are displayed in the CLI output. If no malicious files are found, the system reports a clean status. If compromised files are detected, they are automatically removed. Scan details are also recorded in the upgrade logs.

GUI Upgrade Scenario

During a GUI-based upgrade, a security scan is introduced before the final continue step. A warning message indicates that a security scan will be performed. If no malicious files are found, the system reports a clean status. If compromised files are detected, they are automatically removed. The scan runs only after you click Continue, and the results are recorded in the upgrade logs. You can view the scan results from the upgrade logs after the upgrade process proceeds.

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 Requirements

- Executing Vault Recovery Script to Resolve Vault Issues, page 13
- Spam Notification URL Changes, page 14

Executing Vault Recovery Script to Resolve Vault Issues

If your Secure Email and Web Manager encounters vault-related issues and if encryption is **disabled**, then you must execute Vault Recovery Script to resolve these issues. Perform the following steps to execute the Vault Recovery Script:

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. `encryption disable [2]`
   c. `reboot`

Your Secure Email and Web Manager recovers, and the vault is reinitialized.

Now, you can connect to the system without any issues, and all the system configuration settings are retained.

If your Secure Email and Web Manager encounters vault-related issues and if encryption is **enabled**, contact Cisco TAC to resolve them.

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

- Certificate private keys
- RADIUS passwords
- LDAP bind passwords
- Local users' password hashes
- SNMP password
- FTP Push log subscriptions' passwords
- IPMI LAN password
- Updater server URLs
- SAML certificate passphrase

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

Spam Notification URL Changes

After you upgrade to Secure Email and Web Manager 15.0, 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 15
- Lists of Known and Fixed Issues, page 15
- Finding Information about Known and Resolved Issues, page 16

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 15.0.2, page 15
- Known and Fixed Issues for AsyncOS 15.0.1, page 15
- Known and Fixed Issues for AsyncOS 15.0.0, page 15

Known and Fixed Issues for AsyncOS 15.0.2

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&rls=15.0.2,15.0.1,15.0.0&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.0.2&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Known and Fixed Issues for AsyncOS 15.0.1

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&rls=15.0.1&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.0.1&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Known and Fixed Issues for AsyncOS 15.0.0

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.0.0&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.0.0&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, 15.0.

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.

End-of-Sale and End-of-Life Announcement for Cisco SecureX

SecureX is being terminated and will be replaced with Cisco XDR. For more information, see https://www.cisco.com/c/en/us/products/collateral/security/securex/securex-eol.html.

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

Documentation For Cisco Secure Products:	Is Located At:
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.

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.

© 2026 Cisco Systems, Inc. All rights reserved.