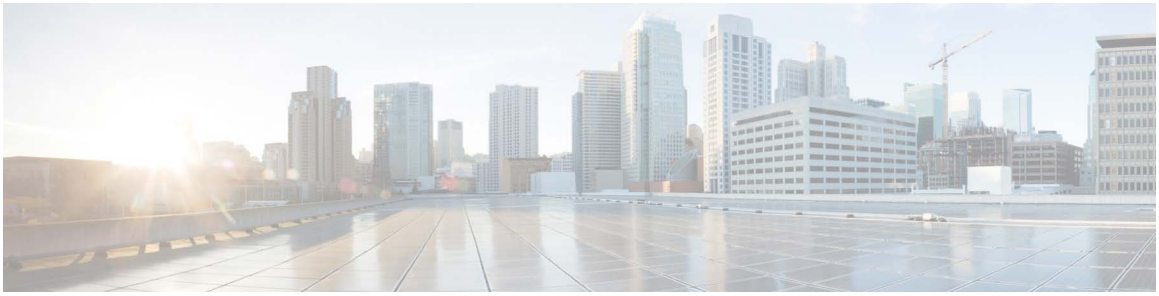

Release Notes for AsyncOS 15.5.1 for Cisco Secure Email and Web Manager (Cloud) - MD (Maintenance Deployment)

Published: April 30, 2024

Revised: March 26, 2026

Contents

- What's New in this Release, page 2
- Changes in Behavior, page 4
- Upgrade Paths, page 7
- Installation and Upgrade Notes, page 7
- Supported VMs for this Release, page 9
- Known and Fixed Issues, page 9
- End-of-Sale and End-of-Life Announcement for Cisco SecureX, page 10
- Software Lifecycle Support Statement, page 10
- Service and Support, page 11

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
Monitoring Vault Service and Sending Alerts	Your Secure Email and Web Manager now monitors the Vault service and keeps track of its status, whether it is initialized or not. It also sends appropriate alert messages and logs status information into mail_logs. You can access the alert logs using one of the following ways: • Navigate to **System Administration** > **Alerts** page on the web interface, and click the **View Top Alerts** button. • Use the `displayalerts` command in the CLI. If the Vault service fails to initialize due to any issues, you receive alert messages (in the mail, on the web interface, and in the CLI) to indicate that the Vault service is down, and you have to execute the Vault Recovery process to restore the Vault service. **Note** If the upgrade fails while upgrading to AsyncOS 15.5.1, then you should check for the Vault service error in upgrade_logs. If a Vault service error is identified, then you must restore the Vault service or proceed with the upgrade process without saving the configuration. You will receive alert messages in the following scenarios: • If the Vault service fails to initialize after you upgrade to AsyncOS 15.5.1, you receive alert messages through the mail, on the web interface, and in the CLI. • If any of the services of your Secure Email and Web Manager use the Vault service that fails to initialize, you receive alert messages through the mail, on the web interface, and in the CLI. If encryption is enabled, you always receive an alert mail. If encryption is disabled, you receive an alert mail only if the services using the Vault service are configured. You can check the encryption status using the `adminaccessconfig` > `encryptconfig` subcommand. The Vault monitoring mechanism checks the Vault service every 75 minutes. If it is down, then it sends alert messages until the Vault service is restored. For information on an example of a successful vault health check and initialization log entry, see "Successful Vault Health Check and Initialization" section in "Logging" chapter of the user guide.

	To restore the Vault service, you have to execute the Vault Recovery process. **Caution** If the encryption (CLI > `adminaccessconfig` > `encryptconfig`) is enabled, ensure that you always save and keep a copy of Secure Email and Web Manager's configuration to avoid data loss. For more information on how to save the Secure Email and Web Manager's configuration, see Saving Secure Email and Web Manager's Configuration, page 7. For information on how to execute the Vault Recovery process, see Executing Vault Recovery Process to Resolve Vault Issues, page 8.
TLS 1.3 Support for Web Interface and API Server	You can use TLS 1.3 for TLS communication across the legacy or new web interfaces of your Secure Email and Web Manager and the API services. For more information, see "Secure Communication Protocol" section in the "Common Administrative Tasks" chapter of the user guide.
Search Filter Enhancement	To enhance your search, two new filters, Contains and Does Not Contain, are added to the drop-down list on the Search ribbon at the bottom of the reporting pages on the new web inteface. For more information, see "Searching and the Interactive Email Report Pages" section in the "Using Centralized Email Security Reporting" chapter of the userguide.

Changes in Behavior

SSH Server Configuration Changes	**New Install Scenario** The following SSH server configuration changes are applicable when you install AsyncOS 15.5.1 for Cisco Secure Email and Web Manager for the first time. [**Non-FIPS Mode**] The following cipher algorithms, MAC method, Host key algorithms, and Kex algorithms are supported in your Secure Email and Web Manager: • Cipher algorithms - `aes128-gcm@openssh.com` and `chacha20-poly1305@openssh.com` • MAC method- `hmac-sha2-256` • Host key algorithms - `ecdsa-sha2-nistp256`, and `ssh-ed25519` • Kex algorithms - `curve25519-sha256` , `diffie-hellman-group14-sha256`, and `curve25519-sha256@libssh.org` [**FIPS Mode**] The following cipher algorithm, MAC method, and Host key algorithm are supported in your Secure Email and Web Manager: • Cipher algorithm - `aes128-gcm@openssh.com` • MAC method - `hmac-sha2-256` • Host key algorithm - `ecdsa-sha2-nistp256` **Note** When you upgrade your Secure Email and Web Manager from a lower AsyncOS version to AsyncOS 15.5.1 version and later, all the must-supported algorithms are added to the SSH Server.
Log Message Changes for TLS Connection Status	The log message for TLS connection status is modified to include details about the validity check along with the date and time of certificate expiry or certificate validity commencement for the following services: • LDAP • Updater • Syslog • Alert Over TLS • SMTP Outbound (EUQ)

Application SSH Client Algorithm Support	The application SSH client algorithms are supported for the following connections: • When you connect Secure Email Gateway to Secure Email and Web Manager. • When you back up the configuration from Secure Email and Web Manager. • When you add a secondary Secure Email and Web Manager to a primary Secure Email and Web Manager. [**Non-FIPS Mode**] The following cipher algorithm, MAC method, and KEX algorithm are added to your Secure Email and Web Manager by default in addition to the existing algorithms: • Cipher algorithms - `aes128-ctr` • MAC methods - `hmac-sha2-256` • KEX algorithms - `diffie-hellman-group14-sha256` [**FIPS Mode**] The following cipher algorithm and MAC method are added to your Secure Email and Web Manager by default in addition to the existing algorithms: • Cipher algorithms - `aes128-ctr` • MAC methods - `hmac-sha2-256`
Removal of Splunk Database Files	Before this release, the Secure Email and Web Manager retained Splunk database files after the upgrade process. After you upgrade to this release, if the Splunk database files were present before the upgrade process, the Secure Email and Web Manager removes all the Splunk database files.
Accepting Substrings of Passwords	Before this release, when you added a user with a password that contains a substring (three or more characters) of the string "password," the system would not accept any substrings such as "pas," "wor," or "ord." After you upgrade to this release, when you add a user with a password that contains a substring (3 or more characters) of the string "password," the system accepts substrings such as "pas," "wor," or "ord," ensuring more comprehensive detection of substrings.
Deleting Files from `/data/db/syslogs` Directory	Before this release, you could not delete files in the `/data/db/syslogs` directory. From this release onwards, you can use the `wipedata` CLI command to delete files in the `/data/db/syslogs` directory. When you delete files from the `/data/db/syslogs` directory using the `wipedata` command, you will also receive a notification message informing you to modify the log subscription to **Manual** and configure it back to **Syslog** if you want to retrieve the log files using Syslog Push.

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

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 15.5.1-029 - MD (Maintenance Deployment)

You can upgrade to release 15.5.1-029 from the following versions:

- 14.2.0-241
- 14.3.0-124
- 15.0.0-413
- 15.5.1-024

Installation and Upgrade Notes

- Important Additional Reading, page 7
- Pre-Upgrade Requirements, page 7
- Post-Upgrade Requirements, 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 End-of-Sale and End-of-Life Announcement for Cisco SecureX, page 10.

Pre-Upgrade Requirements

Perform the following important pre-upgrade tasks:

- Saving Secure Email and Web Manager's Configuration, page 7
- 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 15.5.1.

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 15.5.1, 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 Requirements

Spam Notification URL Changes

After you upgrade to Secure Email and Web Manager 15.5.1, 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 9
- Lists of Known and Fixed Issues, page 10
- 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?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager&rls=15.5.1,15.5.0
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.5.1&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, 15.5.1.

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.

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.

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