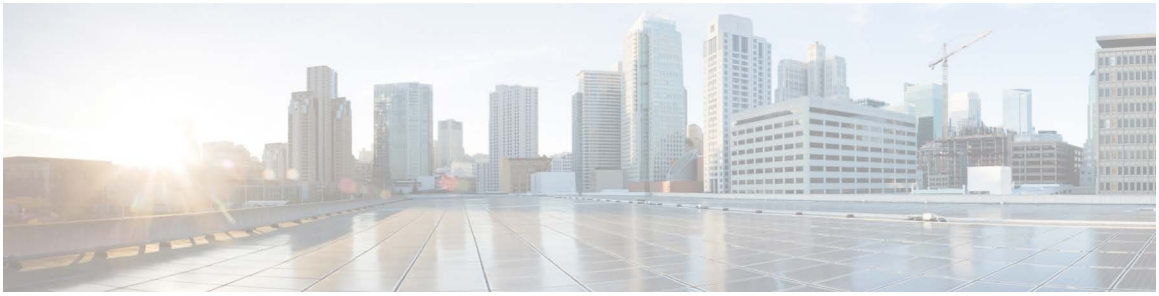

Release Notes for AsyncOS 15.5.4 for Cisco Secure Email and Web Manager - MD (Maintenance Deployment)

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 8
- Upgrade Paths, page 9
- Installation and Upgrade Notes, page 10
- Supported Hardware for this Release, page 15
- Known and Fixed Issues, page 15
- End-of-Sale and End-of-Life Announcement for Cisco SecureX, page 17
- Software Lifecycle Support Statement, page 17
- Related Documentation, page 18
- Service and Support, page 18

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

Note If you already have a Cisco SecureX account that is managed by different administrator login, Cisco recommends that you register your devices with SSE first before you perform smart licensing registration. You must not perform smart licensing registration without registering your device with SSE first. This is a known issue- Defect ID- CSCvy10226.

What's New in this Release

What's New in AsyncOS 15.5.4, page 2
What's New in AsyncOS 15.5.3, page 2
What's New in AsyncOS 15.5.2, page 2
What's New in AsyncOS 15.5.1, page 3

What's New in AsyncOS 15.5.4

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 15

What's New in AsyncOS 15.5.3

There are no new features in this release.

What's New in AsyncOS 15.5.2

Feature	Description
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.

What's New in AsyncOS 15.5.1

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 11. For information on how to execute the Vault Recovery process, see Executing Vault Recovery Process to Resolve Vault Issues, page 12.
Mandatory Usage of Cisco Smart Software Licensing for On-Premises Users	The Cisco Smart Software Licensing usage is mandatory from AsynOS 15.5.1 release (all releases post AsyncOS 15.0 release) for Cisco Secure Email and Web Manager. **Note** From this release onwards, there will be no support for classic licensing for On-Premises users. You will no longer be able to order new feature licenses or renew existing feature licenses in the Classic Licensing mode. **Prerequisite**: Make sure you create a smart account in the Cisco Smart Software Manager portal and enable Cisco Smart Software Licensing on your Secure Email and Web Manager. For more information, see the "Smart Software Licensing" section in the "Common Administrative Tasks" chapter of the user guide. After you enable Cisco Smart Software Licensing, you can upgrade your Secure Email and Web Manager to this release and continue to use the existing feature licenses in the Smart Licensing mode.
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 interface. For more information, see "Searching and the Interactive Email Report Pages" section in the "Using Centralized Email Security Reporting" chapter of the userguide.
C5 Nitro-Instance Support for AWS	From the AsyncOS 15.5.1 release onwards, Secure Email and Web Manager supports **c5.2xlarge** EC2 instance type for the **M600V** model deployed through AWS. For more information, see Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual on AWS EC2 Installation Guide.

Changes in Behavior

Changes in Behavior in AsyncOS 15.5.4, page 5
Changes in Behavior in AsyncOS 15.5.3, page 5
Changes in Behavior in AsyncOS 15.5.2, page 5
Changes in Behavior in AsyncOS 15.5.1, page 6

Changes in Behavior in AsyncOS 15.5.4

There are no changes in behavior for this release.

Changes in Behavior in AsyncOS 15.5.3

There are no changes in behavior for this release.

Changes in Behavior in AsyncOS 15.5.2

There are no changes in behavior for this release.

Changes in Behavior in AsyncOS 15.5.1

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`
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

Note Next generation user interface is best experienced with trailblazer being enabled. Therefore, we recommend that you access the new interface with trailblazer enabled.

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

Note The new web interface of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the `trailblazerconfig` command in the CLI to configure the trailblazer HTTPS ports. Make sure that the trailblazer HTTPS port is opened on the firewall.

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

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/ng-login`

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

  By default, `trailblazerconfig` is enabled on the appliance.

  - Make sure that the configured HTTPS port is opened on the firewall. The default HTTPS port is 4431.
  - Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.
- When `trailblazerconfig` CLI command is disabled, use the following URL - `https://example.com:<https-port>/ng-login`

  where `example.com` is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.

Note If the trailblazerconfig CLI command is disabled, you may need to add multiple certificates for API ports for certain browsers.

- 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 in any one of the following ways:

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/euq-login`.

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.
- When `trailblazerconfig` CLI command is disabled, use the following URL - `https://example.com:<https-port>/euq-login`.

  where `example.com` is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.

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 15.5.4-007 - MD (Maintenance Deployment)

You can upgrade to release 15.5.4-007 from the following versions:

- 15.0.1-035
- 15.0.2-007
- 15.5.1-029
- 15.5.2-005
- 15.5.3-017

Installation and Upgrade Notes

- Important Additional Reading, page 10
- Virtual Appliance, page 10
- Pre-Upgrade Requirements, page 11
- IPMI Messages During Upgrade, page 14
- Upgrading to This Release, page 14
- Post-Upgrade Requirements, page 15

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 18.

Virtual Appliance

To set up a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html.

Note Fiber Network Interface Cards on virtual appliances are not compatible with AsyncOS versions 12.5 and later. This is a known issue. Defect ID: CSCvr26218

Note The RAM size of M600V virtual appliance is increased from 8 GB to 16 GB. You will receive an alert if your virtual appliance does not meet this requirement.

Upgrading a Virtual Appliance

If your current Virtual Appliance release does not support more than 2TB of disk space, and you want to use more than 2 TB of disk space with this release, you cannot simply upgrade your virtual appliance.

Instead, you must deploy a new virtual machine instance for this release.

When you upgrade a virtual appliance, the existing licenses remain unchanged.

Migrating From a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance using the documentation described in Virtual Appliance, page 10.

Step 2 Upgrade your physical appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded physical appliance

Step 4 Load the configuration file from the hardware appliance onto the virtual appliance.

Be sure to select appropriate options related to disk space and network settings.

What To Do Next

If you will use your hardware appliance as a backup appliance, see information about backups in the user guide or online help. For example, you should ensure that the backup appliance does not pull data directly from managed email and web security appliances, or publish configurations to web security appliances.

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.

Perform the following important pre-upgrade tasks:

- Saving Secure Email and Web Manager's Configuration, page 11
- Executing Vault Recovery Process to Resolve Vault Issues, page 12
- FIPS Compliance, page 13
- Verify Associated Email and Web Security Appliance Versions, page 13
- Back Up Your Existing Configuration, page 13
- Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode, page 13
- Back Up Your Existing Databases, page 13

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.

FIPS Compliance

AsyncOS 15.5.1 release is FIPS compliant and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #4036).

Verify Associated Email and Web Security Appliance Versions

Before upgrading, verify that the Email Security appliances and Web Security appliances that you want to manage will run releases that are compatible. See the Installation and Upgrade Notes, page 10.

Back Up Your Existing Configuration

Before upgrading your Cisco Secure Email and Web Manager, save the XML configuration file from your existing Security Management appliance. Save this file to a location off the appliance. For important caveats and instructions, see the "Saving and Exporting the Current Configuration File" section in the user guide or online help.

Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode

After upgrading your managed Email Security appliance in FIPS mode to AsyncOS 15.5.1 or later, the Centralized Policy, Virus, and Outbreak Quarantine is disabled. From AsyncOS 13.0 onwards, Email Security appliances in FIPS mode uses a certificate of 2048 bits to enable Centralized Policy, Virus, and Outbreak Quarantines. The earlier AsyncOS versions have certificates of size 1024 bits.

Follow these steps to enable the Centralized Policy, Virus, and Outbreak Quarantines:

Step 1 Upgrade the Cisco Secure Email and Web Manager to AsyncOS 15.5.1.

Step 2 Upgrade your Cisco Email Security appliance to the latest supported version.

After the upgrade, the Centralized Policy, Virus and Outbreak Quarantines setting will be disabled.

Step 3 On the upgraded Cisco Secure Email and Web Manager, run the `updatepvocert` command on the CLI.

The CA certificate for Centralized Policy, Virus, and Outbreak Quarantines is updated to 2048 bits.

Step 4 On the upgraded Cisco Email Security appliance, verify if the Centralized Policy, Virus, and Outbreak Quarantines is enabled. For more information, see the *Cisco Secure Email and Web Manager User Guide*.

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.

IPMI Messages During Upgrade

If you are upgrading your appliance using the CLI, you may observe messages that are related to IPMI. You can ignore these messages. This behavior is a known issue.

Defect ID: CSCuz33125

Upgrading to This Release

Step 1 Address all topics described in Pre-Upgrade Requirements, page 11.

Step 2 Follow all instructions in the "Before You Upgrade: Important Steps" section in the user guide PDF for THIS release.

Step 3 Perform the upgrade:

Follow instructions in the "Upgrading AsyncOS" section of the "Common Administrative Tasks" chapter of the user guide PDF for your EXISTING release.

Note Do not interrupt power to the appliance for any reason (even to troubleshoot an upgrade issue) until at least 20 minutes have passed since you rebooted. If you have a virtual appliance, do not use the hypervisor or host OS tools to reset, cycle, or power off the virtual machine.

Step 4 After about 10 minutes, access the appliance again and log in.

Step 5 Follow instructions in the "After Upgrading" section of the user guide PDF for THIS release.

Step 6 If applicable, see Migrating From a Hardware Appliance to a Virtual Appliance, page 10.

Important! After you upgrade to this release, you can try any one of the following steps to make the navigation in your browser seamless:

- Accept the certificate used by the web interface and use the following URL syntax: `https://hostname.com:<https_api_port>` (for example, `https://some.example.com:6443`) in a new browser window and accept the certificate. Here `<https_api_port>` is the AsyncOS API HTTPS port configured in **Network > IP Interfaces**. Also, ensure that the API ports (HTTP/HTTPS) are opened on the firewall.
- By default, `trailblazerconfig` CLI command is enabled on your appliance. Make sure that the HTTPS port is opened on the firewall. Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

  If the `trailblazerconfig` CLI command is disabled, you can run the `trailblazerconfig > enable` command using the CLI to avoid the following issues:

  - Requiring to add multiple certificates for API ports in certain browsers.
  - Redirecting to the legacy web interface when you refresh the spam quarantine, Safelist or Blocklist page.

- Metrics bar on the Advanced Malware Protection report page does not contain any data.

For more information, see section "The trailblazerconfig Command" of the user guide.

Note Reboot your appliance or clear your browser cache if you are unable to access the web interface. If the problem persists, contact Cisco Customer Support.

Post-Upgrade Requirements

Spam Notification URL Changes

After you upgrade to Secure Email and Web Manager 15.5.3, if you cannot log in using the saved spam notification URL, use the new URL mentioned in the spam notification mail.

Supported Hardware for this Release

Supported Hardware:

- M195
- M395
- M695

Supported VMs:

- 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 16
- Finding Information about Known and Resolved Issues, page 17

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 15.5.4, page 16
- Known and Fixed Issues for AsyncOS 15.5.3, page 16
- Known and Fixed Issues for AsyncOS 15.5.2, page 16
- Known and Fixed Issues for AsyncOS 15.5.1, page 16

Known and Fixed Issues for AsyncOS 15.5.4

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=15.5.4,15.5.3,15.5.1,15.5.0,15.5.2
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.5.4&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Known and Fixed Issues for AsyncOS 15.5.3

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=15.5.3,15.5.1,15.5.0,15.5.2
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.5.3&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Known and Fixed Issues for AsyncOS 15.5.2

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=15.5.2,15.5.0,15.5.1
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.5.2&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Known and Fixed Issues for AsyncOS 15.5.1

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, 15.5.3.

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.

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.

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 Appliances	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 Security appliances	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.

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.