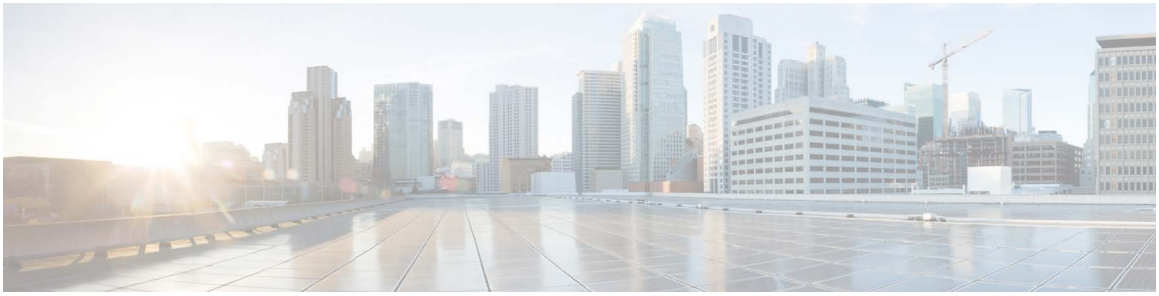

Release Notes for AsyncOS 16.0.3 for Cisco Secure Email and Web Manager - MD (Maintenance Deployment)

Published: September 11, 2025

Revised: March 26, 2026

Contents

- What's New in this Release, page 2
- Changes in Behavior, page 5
- Accessing the New Web Interface, page 7
- Upgrade Paths, page 9
- Installation and Upgrade Notes, page 9
- Supported Hardware for this Release, page 14
- Known and Fixed Issues, page 14
- Software Lifecycle Support Statement, 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.

Note If you already have a Cisco XDR 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.

Cisco Systems, Inc.
www.cisco.com

What's New in this Release

- What's New in AsyncOS 16.0.3-016, page 2
- 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 16.0.0-195, page 3

What's New in AsyncOS 16.0.3-016

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 AsyncOS 16.0.2-088

Feature	Description
Ensuring Seamless Connectivity between Secure Web Appliance (SWA) and Secure Email and Web Manager (SMA)	If you upgrade Secure Email and Web Manager from version 16.0.x to 16.0.2 (MR), all Secure Web Appliance 14.5.x will lose connection to the Secure Email and Web Manager. To ensure uninterrupted connectivity with Secure Email and Web Manager, upgrade your Secure Web Appliance from 14.5.x to 15.x or later version.
Support for Deployment on Google Cloud Platform (GCP)	From AsyncOS 16.0.2 release onwards, deployment of Secure Email Gateway and Secure Email and Web Manager Virtual Appliances is supported on Google Cloud Platform (GCP). For more information, see https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/ESA_SMA_Virtual_Appliance_Deployment_on_Azure_AWS_GCP_Guide.pdf

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 14

What's New in AsyncOS 16.0.0-195

Feature	Description
Nutanix Support	Your Secure Email and Web Manager 16.0 now supports Nutanix. **Nutanix Vesion Details**: – Nutanix AOS: 6.5.5.7 – Nutanix Prism Central: pc.2022.6.0.10 For more information, see *Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide*available at https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html.
ESXi 8.0 Support	Your Secure Email and Web Manager 16.0 now supports ESXi 8.0. For more information, see *Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide*available at https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html.
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.

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. The management of SSH keys varies depending on the scenarios: **New Install Scenario** When you net install the AsyncOS 16.0 version, a new SSH key is generated. **Upgrade Scenario** When you upgrade from AsyncOS 15.5.1 or earlier version to AsyncOS 16.0, you are prompted for consent to inquire if you want to regenerate SSH keys. If you choose to generate new keys, then a new key is generated, if not, the old key is retained. When you upgrade from AsyncOS 16.0 earlier version to AsyncOS 16.0 later version, you are not prompted for consent to inquire if you want to generate SSH keys. The available SSH key is retained. **Revert Scenario** When you revert from AsyncOS 16.0 to an earlier version, you will receive a warning message indicating if you need to replace SSH keys on the SCP push log server. If you have not generated new SSH keys, the warning message is not displayed, and you need not replace SSH keys on the SCP push log server. When you revert from the AsyncOS 16.0 later version to the AsyncOS 16.0 earlier version, the available SSH keys are retained. For more information, see "Configuring Host Keys" section 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 16.0.3-016, page 5
- Changes in Behavior in AsyncOS 16.0.2-088, page 6
- Changes in Behavior in AsyncOS 16.0.1-010, page 6
- Changes in Behavior in AsyncOS 16.0.0-195, page 6

Changes in Behavior in AsyncOS 16.0.3-016

Changes in Behavior	Description
Compatibility between Secure Email and Web Manager (SMA) and Secure Web Appliance (SWA)	Secure Email and Web Manager 16.0.3-016 (MD) is not compatible with the following Secure Web Appliance versions: • 15.2.3-007 (MD) • 15.2.2-009 (MD) • 15.2.1-011 (MD) • 15.2.0-164 (GD) For CM 15.2, Secure Email and Web Manager 16.0.3 (MD) is compatible only with Secure Web Appliance 15.2.4 (MD).

Changes in Behavior in AsyncOS 16.0.2-088

Changes in Behavior	Description
Ensuring Seamless Connectivity between Secure Web Appliance (SWA) and Secure Email and Web Manager (SMA)	If you upgrade Secure Email and Web Manager from version 16.0.x to 16.0.2 (MR), all Secure Web Appliance 14.5.x will lose connection to the Secure Email and Web Manager. To ensure uninterrupted connectivity with Secure Email and Web Manager, upgrade your Secure Web Appliance from 14.5.x to 15.x or later version.

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 15

Changes in Behavior in AsyncOS 16.0.0-195

Changes in Behavior	Description
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 will 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 has been 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

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 16.0.3-016 - MD (Maintenance Deployment)

You can upgrade to release 16.0.3-016 from the following versions:

- 15.0.1-035
- 15.5.1-029
- 15.5.3-017
- 16.0.0-195
- 16.0.1-010
- 16.0.2-088

Installation and Upgrade Notes

- Important Additional Reading, page 9
- Virtual Appliance, page 10
- Pre-Upgrade Notes, page 10
- IPMI Messages During Upgrade, page 12
- Upgrading to This Release, page 12
- Post-Upgrade Notes, 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.

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 Notes

- Saving Secure Email and Web Manager's Configuration, page 11
- Executing Vault Recovery Process to Resolve Vault Issues, page 11
- Verify Associated Email and Web Security Appliance Versions, page 12
- Back Up Your Existing Configuration, page 12
- Back Up Your Existing Databases, page 12

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.

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 9.

Back Up Your Existing Configuration

Before upgrading your Cisco Secure Email and Web Manager, save the XML configuration file from your existing Cisco Secure Email and Web Manager. 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.

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 Notes, page 10.

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 Notes

- TLS 1.0 and TLS 1.1 Deprecation from AsyncOS 16.5 Release, page 13
- Spam Notification URL Changes, page 14

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 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 14
- Lists of Known and Fixed Issues, page 14
- 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 16.0.3-016, page 15
- Known and Fixed Issues for AsyncOS 16.0.2-088, page 15
- Known and Fixed Issues for AsyncOS 16.0.1-010, page 15
- Known and Fixed Issues for AsyncOS 16.0.0-195, page 15

Known and Fixed Issues for AsyncOS 16.0.3-016

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=16.0.3,16.0.1,16.0.0,16.0.2
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=16.0.3&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

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 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

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.