

# Release Notes for AsyncOS 13.0 for Cisco Content Security Management Appliances

---

Published: December 10, 2019

Revised: January 25, 2024

## Contents

- [What's New In This Release, page 2](#)
- [Changes in Behaviour, page 4](#)
- [Comparison of Web Interfaces, New vs. Legacy Web Interface, page 5](#)
- [Upgrade Paths, page 9](#)
- [Compatibility with Email and Web Security Releases, page 9](#)
- [Installation and Upgrade Notes, page 9](#)
- [Supported Hardware for this Release, page 13](#)
- [Known and Fixed Issues, page 13](#)
- [Related Documentation, page 14](#)
- [Service and Support, page 15](#)



**Note**


---

**Important!** After you perform an upgrade to Cisco Content Security Management Appliance 13.0.0-277, you cannot revert to the older version.

---



# What's New In This Release

Feature	Description
Support for new hardware models	<p>The AsyncOS 13.0 release for Cisco Content Security Management appliance supports the following hardware models:</p> <ul style="list-style-type: none"> <li>• M195</li> <li>• M395</li> <li>• M695</li> </ul> <p>For details, see <a href="https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html">https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html</a>.</p>
Managing Multiple Subset of Configuration Masters	<p>You can now configure subsets of a particular version of a Configuration Master to centrally manage the different policy configurations of your Web Security appliance.</p> <p>For more information, see the "Managing Web Security Appliances" chapter of the user guide or online help.</p>
Performing Threat Analysis using Casebooks	<p>The Cisco Content Security Management appliance now includes the casebook and pivot menu widgets.</p> <p> <b>Note</b> If you are using the Microsoft Internet Explorer browser to access your appliance, you will not be able to use the casebook widget.</p> <p>You can perform the following actions in your appliance using the casebook and pivot menu widgets:</p> <ul style="list-style-type: none"> <li>• Add an observable to a casebook to investigate for any threat analysis.</li> <li>• Pivot an observable to a new case, an existing case, or other devices registered in the Cisco Threat Response portal (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis.</li> </ul> <p>For more information, see the "Integrating with Cisco Threat Response Server" chapter of the user guide or online help.</p>
Ability to choose Cisco Threat Response server when registering appliance with Cisco Threat Response portal	<p>When registering your appliance with the Cisco Threat Response portal, you can now choose a Cisco Threat Response server to connect your appliance to the Cisco Threat Response portal.</p> <p>The following are the Cisco Threat Response servers that are supported for this release:</p> <ul style="list-style-type: none"> <li>• AMERICAS (<a href="https://api-sse.cisco.com">api-sse.cisco.com</a>)</li> <li>• EUROPE (<a href="https://api.eu.sse.itd.cisco.com">api.eu.sse.itd.cisco.com</a>)</li> </ul> <p>For more information, see "Integrating with Cisco Threat Response Server" chapter of the user guide or online help.</p>

Managing favorite reports on the New Web Interface	<p>You can create a custom report page by assembling charts (graphs) and tables from all your existing email security reports on the new web interface of your appliance.</p> <p>For more information, see the "Working with Reports on the New Web Interface" chapter of the user guide or online help.</p>
Creating a New CA Certificate for Policy, Virus, and Quarantines	<p>You can create a CA certificate of 2048 bits for Policy, Virus, and Quarantines using the <code>updatepvocert</code> CLI command.</p> <p>For more information, see "The <code>updatepvocert</code> CLI Command" section of the user guide or online help.</p>
Support for new features in AsyncOS 13.0 for Cisco Email Security Appliances	<ul style="list-style-type: none"> <li>• <b>Scheduling and Archiving Reports</b> - You can now schedule email reports and view the archived reports on the new web interface of your appliance. For more information, see the "Using Centralized Email Security Reporting" chapter of the user guide or online help.</li> <li>• <b>Safe Print Action report page</b> - You can use this report page to view: <ul style="list-style-type: none"> <li>– Number of safe-printed attachments based on the file type in graphical format.</li> <li>– Summary of safe-printed attachments based on the file type in tabular format.</li> </ul> <p>For more information, see the "Using Centralized Email Security Reporting" chapter of the user guide or online help.</p> </li> <li>• <b>Reporting Data Availability report page</b> - You can now view the reporting data availability report page on the new web interface of your appliance. For more information, see the "Using Centralized Email Security Reporting" chapter of the user guide or online help.</li> <li>• <b>Policy, Virus and Outbreak Quarantine</b> - You can now configure Policy, Virus and Outbreak Quarantine on the new interface of your appliance. For more information, see "Centralized Policy, Virus and Outbreak Quarantines" chapter of the user guide or online help.</li> <li>• <b>Swagger UI support</b> - Swagger UI helps you to design and manage AsyncOS API resources on a web interface. For more information, see the "Setup, Installation and Basic Configuration" chapter of the user guide or online help.</li> <li>• <b>Export Reports</b> - You can now export email reporting pages in a .PDF (Portable Document File) format on the new web interface of your appliance. For more information, see the "Working With Reports on the New Web Interface" chapter of the user guide or online help.</li> </ul>

Improving User Experience by Collecting Feature Usage Statistics	<p>The Cisco Content Security Management appliance now collects feature/interface usage statistics on the new web interface of the appliance that helps Cisco improve overall user experience. All data collected is anonymized. If you want to opt-out of this feature, navigate to <b>Management Appliance &gt; System Administration &gt; General Settings &gt; Usage Analytics</b> page of the web interface to disable it.</p> <p>For more information, see section "Monitoring Web Usage Analytics" section in the user guide or online help.</p>
Improving user experience by collecting web interface usage statistics of the appliance	<p>The Cisco Content Security Management appliance can now collect the web interface usage statistics of the appliance using the Usage Analytics feature. This feature is used to collect and analyze the web interface usage data and provide insight to improve user experience of the appliance. For more information, see "Monitoring Web Usage Analytics" section in the user guide or online help.</p>
Single Sign-On using SAML 2.0	<p>The Cisco Content Security Management appliance now supports SAML 2.0 SSO so that the users can log in to the web interface of the appliance using the same credentials that are used to access other SAML 2.0 SSO enabled services within their organization.</p> <p>For more information, see section "Single Sign-On using SAML 2.0" of the user guide or online help.</p>

## Changes in Behaviour

Feature	Description
Changes in passphrase	After you upgrade to this release, you cannot use system-generated passphrases on your appliance when you change the passphrase for the first time.
Changes in Demo Certificates	<p>After you upgrade to this release, Cisco recommends using CA-trusted certificates for receiving, delivery, HTTPS management and LDAP.</p> <p>A message is displayed when you clear the trusted certificates or use a demonstration certificates on your appliance.</p>
Upgrade	<b>Important!</b> After you perform an upgrade to Cisco Content Security Management Appliance 13.0.0-277, you cannot revert to the older version

# Comparison of Web Interfaces, New vs. Legacy Web Interface

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Landing Page	After you log in to the Security Management appliance, the Mail Flow Summary page is displayed.	After you log in to the appliance, the System Status page is displayed.
Product Drop-down	You can switch between the Email Security Appliance and the Web Security Appliance from the Product drop-down.	You can use the Email or Web tab to switch between the Email Security Appliance and the Web Security Appliance.
Reports Drop-down	You can view reports for your Email and Web Security Appliances from the Reports drop-down.	You can view reports for your Email and Web Security Appliances from the Reporting drop-down menu.
Management Appliance Tab	Click on the Security Management appliance to access the Management Appliance tab.	You can enable and configure reporting, message tracking and quarantines, as well as configure network access, and monitor system status.
My Reports Page	Select <b>Email</b> from the Product drop-down and choose <b>My Favorite Reports</b> from the Reports drop-down.	You can view the My Reports page from <b>Email &gt; Reporting &gt; My Reports</b> .
Reporting Data Availability Page	Select <b>Email</b> from the Product drop-down and choose <b>Reporting Data Availability</b> from the Reports drop-down.	You can view the My Reports page from <b>Email &gt; Reporting &gt; Reporting Data Availability</b> .
Scheduling & Archiving Reports	Select <b>Email</b> from the Product drop-down and choose <b>Monitoring &gt; Schedule &amp; Archive</b> from the Reports drop-down.	You can schedule reports using the <b>Email &gt; Reporting &gt; Scheduled Reports</b> page, and archive your reports using the <b>Email &gt; Reporting &gt; Archived Report</b> page of the Security Management appliance.
Reporting Overview Page	The Email Reporting Overview page on the Security Management appliance has been redesigned as Mail Flow Summary page in the new web interface. The Mail Flow Summary page includes trend graphs and summary tables for incoming and outgoing messages.	The Email Reporting Overview page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Overview page includes graphs and summary tables for the incoming and outgoing messages.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Advanced Malware Protection Report Pages	<p>The following sections are available on the <b>Advanced Malware Protection</b> report page of the Reports menu:</p> <ul style="list-style-type: none"> <li>• Summary</li> <li>• AMP File Reputation</li> <li>• File Analysis</li> <li>• File Retrospection</li> <li>• Mailbox Auto Remediation</li> </ul>	<p>The <b>Email &gt; Reporting</b> drop-down menu of the Security Management appliance has the following Advanced Malware Protection report pages:</p> <ul style="list-style-type: none"> <li>• Advanced Malware Protection</li> <li>• AMP File Analysis</li> <li>• AMP Verdict Updates</li> <li>• Mailbox Auto Remediation</li> </ul>
Outbreak Filters Page	<p>The Past Year Virus Outbreaks and Past Year Virus Outbreak Summary are not available in the Outbreak Filtering report page of the new web interface.</p>	<p>The <b>Email &gt; Reporting Outbreak Filters</b> page displays the Past Year Virus Outbreaks and Past Year Virus Outbreak Summary.</p>
Spam Quarantine (Admin and End-User)	<p>Click <b>Quarantine &gt; Spam Quarantine &gt; Search</b> on the new web interface to access the Spam Quarantine page.</p> <p>For more information on the end-users access to the Spam Quarantine portal on the new web interface, see <a href="#">Accessing the New Web Interface, page 7</a>.</p>	-
Policy, Virus and Outbreak Quarantines	<p>Click <b>Quarantine &gt; Other Quarantine</b> on the new web interface.</p> <p>You can only view Policy, Virus and Outbreak Quarantines on the Security Management appliance.</p>	<p>You can view, configure and modify the Policy, Virus and Outbreak Quarantines on the appliance.</p>
Select All action for Messages in Quarantine	<p>You can select multiple (or all) messages in a quarantine and perform a message action, such as, delete, delay, release, move, etc.</p>	<p>You cannot select multiple messages in a quarantine and perform a message action.</p>
Maximum Download Limit for Attachments	<p>The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.</p>	-
Rejected Connections	<p>To search for rejected connections, click <b>Tracking &gt; Search &gt; Rejected Connection</b> tab on the Security Management appliance.</p>	-

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Query Settings	The <b>Query Settings</b> field of the Message Tracking feature is not available on the Security Management appliance.	You can set the query timeout in the Query Settings field of the Message Tracking feature.
Message Tracking Data Availability	Click on the on the Security Management appliance and choose <b>Email &gt; Message Tracking &gt; Message Tracking Data Availability</b> to access Message Tracking Data Availability page.	You can view the missing-data intervals for your appliance.
Verdict Charts and Last State Verdicts	Verdict Chart displays information of the various possible verdicts triggered by each engine in your appliance.  Last State of the message determines the final verdict triggered after all the possible verdicts of the engine.	Verdict Charts and Last State Verdicts of the messages are not available.
Message Attachments and Host Names in Message Details	Message attachments and host names are not displayed in the Message Details section of the message on the Security Management appliance.	Message attachments and host names are displayed in the Message Details section of the message.
Sender Groups, Sender IP, SBRS Score and Policy Match in Message Details	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is displayed in the Message Details section of the message on the Security Management appliance.	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is not available in the Message Details section of the message.
Direction of the Message (Incoming or Outgoing)	Direction of the messages (incoming or outgoing) is displayed in the message tracking results page on the Security Management appliance.	Direction of the messages (incoming or outgoing) is not displayed in the message tracking results page.

## Accessing the New Web Interface

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

- [Upgrading to AsyncOS 13.0.0-277 - MD \(Maintenance Deployment\)](#), page 9

### Upgrading to AsyncOS 13.0.0-277 - MD (Maintenance Deployment)

You can upgrade to release 13.0.0.277 from the following versions:

- 12.0.1- 011
- 12.0.1- 017
- 12.0.2- 005
- 12.0.2- 007
- 12.5.0- 683
- 12.8.1- 002
- 13.0.0-249

## Compatibility with Email and Web Security Releases

Compatibility with AsyncOS for Email Security and AsyncOS for Web Security releases is detailed in the Compatibility Matrix available from

<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>.

## Installation and Upgrade Notes

- [Important Additional Reading](#), page 9
- [Virtual Appliance](#), page 10
- [Pre-Upgrade Requirements](#), page 10
- [IPMI Messages During Upgrade](#), page 11
- [Upgrading to This Release](#), page 11
- [Post Upgrade Notes](#), page 12

## 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 14.

## 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

## 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

Perform the following important preupgrade tasks:

- [Verify Associated Email and Web Security Appliance Versions, page 10](#)
- [Back Up Your Existing Configuration, page 11](#)

## 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 [Compatibility with Email and Web Security Releases, page 9](#).

## Back Up Your Existing Configuration


Before upgrading your Cisco Content Security Management appliance, 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.

## IPMI Messages During Upgrade

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

Defect ID: CSCuz33125

## Upgrading to This Release

- 
- Step 1** Address all topics described in [Pre-Upgrade Requirements, 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

- [Manage Email Security Appliance\(s\) in FIPS Mode on Security Management Appliance \(AsyncOS 13.0\), page 12](#)
- [Enable Centralized Policy, Virus and Outbreak Quarantine Communication between Security Management Appliance \(AsyncOS 13.0\) and Email Security Appliance\(s\), page 12](#)

### Manage Email Security Appliance(s) in FIPS Mode on Security Management Appliance (AsyncOS 13.0)

After you upgrade the Cisco Content Security Management appliance to AsyncOS 13.0 and if you upgrade the managed Email Security appliance(s) that is in FIPS mode to AsyncOS 13.0, the Centralized Policy, Virus, and Outbreak Quarantines setting on the Email Security appliance will be disabled, and the Centralized Policy, Virus, and Outbreak Quarantines communication between the Content Security Management appliance and Email Security appliance will stop.

The Centralized Policy, Virus, and Outbreak Quarantines setting is disabled because, from AsyncOS 13.x onwards, the managed Email Security appliance in the FIPS mode uses the CA certificate of 2048 bits to enable Centralized Policy, Virus, and Outbreak Quarantines setting. The earlier AsyncOS versions of the managed Email Security appliance have the CA certificates of 1024 bits.

### Enable Centralized Policy, Virus and Outbreak Quarantine Communication between Security Management Appliance (AsyncOS 13.0) and Email Security Appliance(s)

To enable the Centralized Policy, Virus, and Outbreak Quarantines setting, use the `updatepvocert` CLI command on the Cisco Content Security Management appliance. For more information, see the "The `updatepvocert` CLI Command" section of the user guide.

**Important!** If your Content Security Management appliance is managing multiple Email Security appliances (AsyncOS 13.0 and any version before AsyncOS 13.0), you must contact Cisco Customer Support to enable the Centralized Policy, Virus, and Outbreak Quarantines setting on the older version of the Email Security appliance.

For example, if the Content Security Management appliance on AsyncOS 13.0 is managing Email Security Appliances running AsyncOS 12.5 and other AsyncOS 13.0 Email Security appliances, perform the steps in the following order:

- 
- Step 1** Run the `updatepvocert` CLI command on the Content Security Management appliance to update the CA certificate to 2048 bits and enable its communication with the Email Security appliance.

**Caution**

When you run the `updatepvocert` CLI command, the Security Management appliance disconnects the older versions of the Email Security appliance such as AsyncOS 12.5 that have a CA certificate of 1024 bits. Contact Cisco Customer Support to update the CA certificate to 2048 bits. Cisco Customer Support will require a technical support tunnel to make changes to older versions of Email Security appliances.

**Step 2**

Verify the Centralized Policy, Virus, and Outbreak Quarantines communication of your Security Management appliance with its managed AsyncOS 13.0 Email Security appliance.

## Supported Hardware for this Release

All virtual appliance models.

- The following hardware models - M190, M195, M390, M395, M690, and M695.

To determine whether your appliance is supported, and to remedy the situation if it is not currently compatible, see <https://www.cisco.com/c/en/us/support/docs/field-notices/639/fn63931.html>.

- The following hardware is NOT supported for this release:
  - M160, M360, M660, and X1060
  - M170, M370, M370D, M670 and X1070
  - M380 and M680 appliances

## Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

- [Bug Search Tool Requirements, page 13](#)
- [Lists of Known and Fixed Issues, page 14](#)
- [Finding Information about Known and Resolved Issues, page 14](#)

## 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

<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch?kw=*&amp;pf=prdNm&amp;rls=13.0.0&amp;sb=afr&amp;sts=open&amp;svr=3nH&amp;bt=custV&amp;prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager">https://bst.cloudapps.cisco.com/bugsearch?kw=*&amp;pf=prdNm&amp;rls=13.0.0&amp;sb=afr&amp;sts=open&amp;svr=3nH&amp;bt=custV&amp;prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager</a>
<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch?kw=*&amp;pf=prdNm&amp;rls=13.0.0&amp;sb=fr&amp;sts=fd&amp;svr=3nH&amp;bt=custV&amp;prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager">https://bst.cloudapps.cisco.com/bugsearch?kw=*&amp;pf=prdNm&amp;rls=13.0.0&amp;sb=fr&amp;sts=fd&amp;svr=3nH&amp;bt=custV&amp;prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager</a>

## Finding Information about Known and Resolved Issues

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

### 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, 12.5
- 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.

---

## 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 PDF.

Documentation For Cisco Content Security Products:	Is Located At:
Security Management appliances	<a href="http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html</a>
Web Security appliances	<a href="http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html</a>
Email Security appliances	<a href="http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html</a>
Command Line Reference guide for content security products	<a href="http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html">http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html</a>
Cisco Email Encryption	<a href="http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html</a>

## 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](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](http://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.

© 2019 - 2024 Cisco Systems, Inc. All rights reserved.