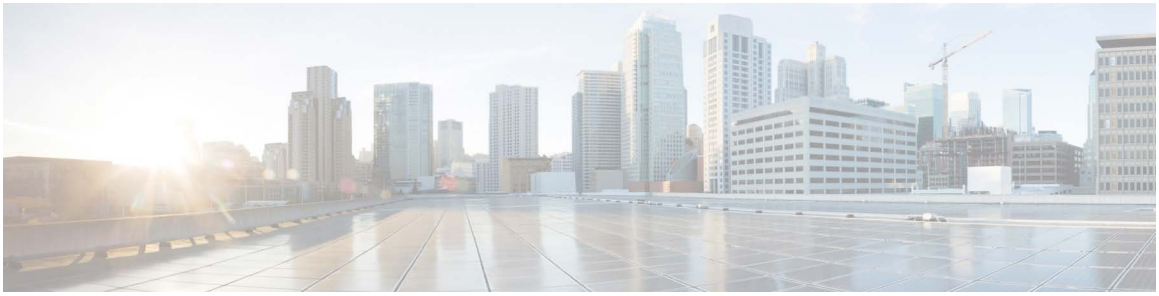

Release Notes for AsyncOS 13.5 for Cisco Content Security Management Appliances

Published: January 13, 2020
Revised: January 25, 2024

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Support for new hardware models	The AsyncOS 13.5 release for Cisco Content Security Management appliance supports the following hardware models: • M195 • M395 • M695 For details, see https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html.
Ability to configure web reporting modules on Cisco Threat Response	You can now configure web reporting modules on the Cisco Threat Response. On the Cisco Threat Response, navigate to **Settings > Integration Modules > Configure Modules > SMA Web - Cisco Content Security Management Appliance - Web** to configure web reporting modules. For more information, see https://visibility.amp.cisco.com/
Performing Threat Analysis using Casebooks	The Cisco Content Security Management appliance now includes the casebook and pivot menu widgets. **Note** If you are using the Microsoft Internet Explorer browser to access your appliance, you will not be able to use the casebook widget. You can perform the following actions in your appliance using the casebook and pivot menu widgets: • Add an observable to a casebook to investigate for any threat analysis. • 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. For more information, see the "Integrating with Cisco Threat Response" chapter of the user guide or online help.
Ability to choose Cisco Threat Response server when registering appliance with Cisco Threat Response portal	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. The following are the Cisco Threat Response servers that are supported for this release: • `AMERICAS (api-sse.cisco.com)` • `EUROPE (api.eu.sse.itd.cisco.com)` For more information, see "Integrating with Cisco Threat Response" chapter of the user guide or online help.

Managing favorite reports	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. For more information, see the "Working with Reports on the New Web Interface" chapter of the user guide or online help.
Scheduling and Archiving Web Reports	You can now schedule web reports and view the archived reports on the new web interface of your appliance. For more information, see "Using Centralized Web Reporting" chapter of the user guide or online help.

Single Sign-On using SAML 2.0	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. For more information, see "Common Administrative Tasks" chapter of the user guide or online help.
Support for new features in AsyncOS 13.0 for Cisco Email Security Appliances	• **Scheduling and Archiving Email Reports** - You can now schedule email reports and view the archived reports on the new web interface of your appliance. For more information, see "Using Centralized Email Security Reporting" chapter of the user guide or online help. • **Safe Print Action report page** - You can use this report page to view: – Number of safe-printed attachments based on the file type in graphical format. – Summary of safe-printed attachments based on the file type in tabular format. For more information, see "Using Centralized Email Security Reporting" chapter of the user guide or online help. • **Reporting Data Availability report page** - You can now view the reporting data availability report page on the new web interface of your appliance. For more information, see "Using Centralized Email Security Reporting" chapter of the user guide or online help. • **Policy, Virus and Outbreak Quarantine** - 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. • **Swagger UI support** - Swagger UI helps you to design and manage AsyncOS API resources on a web interface. For more information, see "Setup, Installation, and Basic Configuration" chapter of the user guide or online help. • **Web Usage Analytics** - You can now enable and disable your website usage or activity from being sent for statistical analysis. For more information, see "Common Administrative Tasks" chapter of the user guide or online help. • **Export Reports** - 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 "Working With Reports on the New Web Interface" chapter of the user guide or online help.

Changes in Behavior

Changes in `sshconfig` CLI command	After you upgrade to this release, you can use the sshconfig > sshd command in the CLI to edit the following SSH server configuration settings: • Public Key Authentication Algorithms • Cipher Algorithms • KEX Algorithms • MAC Methods • Minimum Server Key Size.
SSL Configuration Changes	After you upgrade to this release, you cannot configure SSL settings for the end-user spam quarantine service on your appliance.
Changes in Passphrase Settings	The option to automatically generate a login passphrase is removed. You must now manually enter a passphrase of your choice.
Performance improvement on reporting	After you upgrade to this release, the Security Management appliances can handle more number of Email security appliances and process the email reporting data faster.
Changes in message tracking performance	After you upgrade to this release, the new web interface of the appliance displays the message details of a message search query faster.
Viewing archived reports from legacy web interface	After you upgrade to this release, the new web interface of your appliance shows you the archived reports that are available on your legacy web interface. You can use the **View Legacy Archived Reports** tab of the **Schedule & Archive Reports** page on your new web interface to view the archived reports of the legacy web interface.

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.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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.
Custom Reports	To view your customized reports, select **Email** from the Product drop-down and choose **My Favorite Reports** from the Reports drop-down.	You can view the custom reports page from **Email > Reporting > My Reports**.
Scheduling & Archiving Reports	To view your scheduled and archived reports, select **Email** from the Product drop-down and choose **Monitoring > Schedule &Archive**.	You can schedule reports using the **Email > Reporting > Scheduled Reports** page, and archive your reports using the **Email > Reporting > Archived Report** 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.
Advanced Malware Protection Report Pages	The following sections are available on the **Advanced Malware Protection** report page of the Reports menu: • Summary • AMP File Reputation • File Analysis • File Retrospection • Mailbox Auto Remediation	The **Email > Reporting** drop-down menu of the Security Management appliance has the following Advanced Malware Protection report pages: • Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Mailbox Auto Remediation
Outbreak Filters Page	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.	The **Email > Reporting Outbreak Filters** page displays the Past Year Virus Outbreaks and Past Year Virus Outbreak Summary.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Spam Quarantine (Admin and End-User)	Click **Quarantine > Spam Quarantine > Search** on the new web interface to access the Spam Quarantine page. For more information on the end-users access to the Spam Quarantine portal on the new web interface, see Accessing the New Web Interface, page 8.	-
Policy, Virus and Outbreak Quarantines	Click **Quarantine > Other Quarantine** on the new web interface. You can only view Policy, Virus and Outbreak Quarantines on the Security Management appliance.	You can view, configure and modify the Policy, Virus and Outbreak Quarantines on the appliance.
Select All action for Messages in Quarantine	You can select multiple (or all) messages in a quarantine and perform a message action, such as, delete, delay, release, move, etc.	You cannot select multiple messages in a quarnatine and perform a message action.
Maximum Download Limit for Attachments	The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.	-
Rejected Connections	To search for rejected connections, click **Tracking > Search > Rejected Connection** tab on the Security Management appliance.	-
Query Settings	The **Query Settings** 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 the gear icon on the Security Management appliance and choose **Email > Message Tracking > Message Tracking Data Availability** 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.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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

You can upgrade to release 13.5.0-117 from the following version:

Note This release is compatible with AsyncOS 12.0.1 for Cisco Web Security Appliances.

- 11.4.0-800
- 12.0.0-478
- 12.0.1-011
- 12.0.2-001
- 12.5.0-636
- 12.5.0-658

- 13.0.0-239
- 13.5.0-078
- 13.5.0-114

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

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.

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 11
- 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 10.

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 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 cerificate 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.

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

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

Register for a Cisco account if you do not have one. Go to https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Lists of Known and Fixed Issues

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=13.5.0&sb=afr&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager&sts=open
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=13.5.0&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 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, 13.5

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	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web Security appliances	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
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.