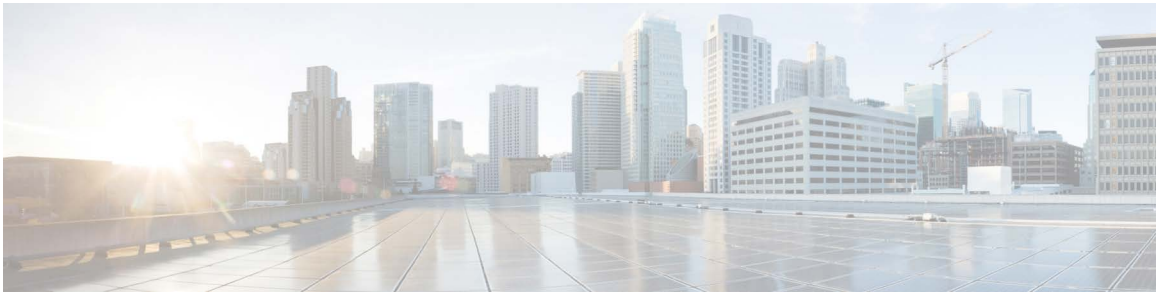

Release Notes for AsyncOS 13.8.0 for Cisco Content Security Management Appliances

First Published: October 5, 2020

Revised Date: January 25, 2024

Contents

Note AsyncOS 13.8.0 includes the following SSL configuration changes:

- The SSL v2.0 and SSL v3.0 methods are not supported.
- The TLS v1.0 method is disabled.

To ensure the smooth functioning of the services after upgrade, we recommend that you switch to TLS v1.1 or TLS v1.2 before you upgrade. For more information, see SSL Configuration Changes, page 9.

Note The Cisco Content Security Management appliance does not support the reporting, tracking, or quarantine functionalities for the new features introduced in Cisco Secure Email 14.0. You may receive the following alert about this limitation:

Cisco Systems, Inc.
www.cisco.com

```
Email Centralized Reporting is receiving data that cannot be processed by the Management
Appliance. This issue may occur if there is a version mismatch between the Email Appliance
and the Management Appliance. Please determine if there is an upgrade available for your
Management Appliance.
```

However, you can ignore them.

What's New in this Release

Feature	Description
Message Tracking Enhancements	The new web interface includes the following user experience enhancements: • The Message Tracking Search Results page is now enhanced to display more search results per page view. • The Message Tracking Search Details page layout is now enhanced to display the **Envelope Header and Summary** and **Sending Host Summary** panes alongside the **Processing Details** pane. This new layout allows you to view all the important information in the same page view without scrolling.
Reporting Enhancements	You can now schedule and archive My Favorite Reports. You can also export My Favorite Reports data in CSV or PDF format.
Spam Notification Enhancements	• You can now set an expiration period for the links in the Spam notification. These links will expire automatically after the specified period. • You can now show or hide the links to view all the quarantined messages in a Spam notification. Also, if you are showing the links in the spam notification, you can now force the end-user to authenticate before accessing the Spam quarantine. For more information, see the **Notifying End Users About Quarantined Messages** topic in the User Guide.
Security Enhancements	AsyncOS 13.8.0 includes the following security enhancements: • The appliance will no longer support SSL v2.0 and SSL v3.0 methods. When you upgrade from a lower AsyncOS version, the appliance will automatically use TLS v1.1 and TLS v1.2. For more information, see SSL Configuration Changes. • The appliance will now send the Cisco Technical Support requests over TLS. If your SMTP server is not using TLS, the requests are sent as plaintext. • You can now configure your appliance to send alerts over TLS. Use the following subcommand in the CLI to configure this functionality: **`alertconfig > SETUP > Do you want to enable TLS support to send alert messages?`**.
Cisco SecureX and Cisco Threat Response Enhancement	You can now configure your appliance to connect to Cisco SecureX and Cisco Threat Response via a proxy. Check the **Use Proxy** check box in the **Network > Cloud Service Settings** page to connect via a proxy.

YouTube Report (Web)	In the new web interface (**URL Categorie**s report page), you can now view the following information related to the YouTube categorization feature: • Top YouTube Categories: Total Transactions You can view the top YouTube Categories that are being visited on the site in a graphical format. • Top YouTube Categories: Blocked and Warned Transactions You can view the top YouTube URL that triggered a block or warning action to occur per transaction in a graphical format. For example, a user went to a certain YouTube URL and because of a specific policy that is in place, this triggered a block action or a warning. This YouTube URL then gets listed in this graph as a transaction blocked or warning. To view the **URL Categories** report page, select **Web** from the **Product** drop-down and choose **Monitoring > URL Categories** from the **Reports** drop-down. • YouTube Categories Matched The YouTube Categories Matched interactive table shows the disposition of transactions by YouTube category during the specified time range, plus bandwidth used and time spent in each category. To view the YouTube Categories Matched interactive table, choose **Web > Reporting > URL Categories.** • YouTube (YT) Category A new filter YT Category has been added under **Web > Tracking.** To filter by a specific YouTube category, expand the YouTube Category section, and select the YouTube categories that you want to view.

IP Spoofing Profiles	You can now configure Web Proxy IP Spoofing by creating an IP spoofing profile and adding it to the routing policies. When IP spoofing profile is used in a routing policy, the web proxy changes the source IP address to custom IP address defined in the IP spoofing profile. To create a new IP spoofing profile or modify and existing IP spoofing profile, initialize the Configuration Master (version 12.5 or later), and choose **Web > Configuration Master > IP Spoofing Profiles**. To add IP spoofing profile in a routing policy, initialize the Configuration Master (version 12.5 or later), and choose **Web > Configuration Master > Routing Policies**. **Note** If you do not want to publish the Security Management Appliance IP Spoofing profiles to Web Security Appliance and overwrite the existing IP Spoofing profiles in the Web Security Appliance, follow the below steps: 1. Log into Security Management Appliance. 2. Go to **Configuration Master > IP Spoofing Profile**. 3. Click **Edit Settings**. 4. Set **Publish IP Spoofing Profiles to WSA** as **No**. The default option selected is **Yes**. For more information, see *User Guide for AsyncOS 12.5 for Cisco Web Security Appliances.*

Changes in Behavior

Casebook Behavior	In AsyncOS 13.6.2, Casebook was a standalone widget on the following pages: Service Status page under Email and Monitoring page under Web. Prior to AsyncOS 13.6.2, Casebook was a standalone widget on all the pages of the new web interface. After you upgrade to this release, Casebook will be part of the Cisco SecureX Ribbon.
Automatic Quarantine Queue Repair	After you upgrade to this release, the appliance will attempt to repair the corrupt quarantine queue automatically by discarding corrupt messages without your intervention. However, if you notice that the automatic repair has failed in the Cisco Text Mail Logs (mail_logs), contact Cisco TAC.
Passphrase Changes	New user accounts cannot use passphrases containing three or more repetitive or sequential characters.
Spam Quarantine Changes	• Prior to this release, the option to enable login without credentials for quarantine access was available under **Edit Spam Quarantine > Spam Notifications > Message Body**. After upgrading to this release, this option is available under **Edit Spam Quarantine > Spam Notifications > Quarantine Access**. • After upgrading to this release, you can configure the following options using the `spamdigestconfig` command in the CLI: – Set an expiration period for the links in the Spam notification. These links will expire automatically after the specified period. – Show or hide the links to view all the quarantined messages in a Spam notification. Also, if you are showing the links in the spam notification, you can now force the end-user to authenticate before accessing the Spam quarantine.
SSL Configuration Changes	See SSL Configuration Changes, page 9

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.

Upgrading to AsyncOS 13.8.0-344 - LD (Limited Deployment)

You can upgrade to the release 13.8.0-344 from the following versions:

- 12.0.0-478
- 12.5.0-678
- 13.0.0-249
- 13.6.2-023
- 13.6.2-034

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 13.

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 7.

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 pre-upgrade tasks:

- Verify Associated Email and Web Security Appliance Versions, page 8
- Back Up Your Existing Configuration, page 8
- Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode, page 8
- SSL Configuration Changes, page 9

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 7.

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.

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

After upgrading your managed Email Security appliance in FIPS mode to AsyncOS 13.0 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 Security Content Management appliance to AsyncOS 13.8.0.

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 Security Content Management appliance, 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 Security Content Management Appliance User Guide*.

SSL Configuration Changes

AsyncOS 13.8.0 includes the following SSL configuration changes for the web interface, LDAP, and Updater services:

- The SSL v2.0 and SSL v3.0 methods are not supported.
- The TLS v1.0 method is disabled after the upgrade.

The following table shows the pre-upgrade and post-upgrade scenarios:

Scenario	TLS Version	Before Upgrade	After Upgrade
1	TLS 1.0	Y	N
	TLS 1.1	N	Y
	TLS 1.2	N	Y
2	TLS 1.0	N	N
	TLS 1.1	Y	Y
	TLS 1.2	N	N
3	TLS 1.0	N	N
	TLS 1.1	N	N
	TLS 1.2	Y	Y
4	TLS 1.0	N	N
	TLS 1.1	Y	Y
	TLS 1.2	Y	Y
5	TLS 1.0	Y	N
	TLS 1.1	Y	Y
	TLS 1.2	Y	Y
6	TLS 1.0	Y	N
	TLS 1.1	Y	Y
	TLS 1.2	N	N

Keep in mind that:

- To ensure the smooth functioning of these services after the upgrade, we recommend that you switch to TLS v1.1 or TLS v1.2 before you upgrade.

- To use TLS v1.0 for these services, enable this protocol version after you upgrade. However, for enhanced security, we recommend that you switch to TLS v1.1 or TLS v1.2.

You can modify the SSL configuration using the **System Administration > SSL Configuration** page or the `sslconfig` command in the CLI. For more information, see the user guide or Online Help.

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 8.

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.

Note Depending on the size of the data present, the x95 appliances (M195, M395, M695, and M695F) may take up to three hours to come online after a reboot. This delay is because of a known issue (CSCvv48198).

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 8.

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

Supported Hardware:

- M190
- M195
- M390
- M395
- M690
- M695

Note Depending on the size of the data present, the x95 appliances (M195, M395, M695, and M695F) may take up to three hours to come online after a reboot. This delay is because of a known issue (CSCvv48198).

Supported VMs:

- M100V
- M300V
- M600V

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 12
- Lists of Known and Fixed Issues, page 12
- Finding Information about Known and Resolved Issues, page 12

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=13.6.0,13.6.1,13.6.2,13.8.0&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=13.6.0,13.6.1,13.6.2,13.8.0&sb=fr&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, 13.8.

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.