



Release Notes for AsyncOS 13.8.1 (LD) for Cisco Content Security Management Appliances

First Published: September 20, 2021
Revised: January 25, 2024

Contents

- [What's New in this Release, page 2](#)
- [Changes in Behavior, page 4](#)
- [Accessing the New Web Interface, page 5](#)
- [Upgrading to AsyncOS 13.8.1, page 6](#)
- [Installation and Upgrade Notes, page 8](#)
- [Supported Hardware for this Release, page 12](#)
- [Known and Fixed Issues, page 12](#)
- [Related Documentation, page 14](#)
- [Service and Support, page 14](#)



Note

AsyncOS 13.8.1 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 10](#).



Note

Important! After you perform an upgrade to Cisco Content Security Management 13.8.1-701, you cannot revert to any earlier version.



What's New in this Release

Feature	Description
Retrieving log information using AsyncOS APIs	<p>You can now retrieve the following log details from your appliance using AsyncOS APIs:</p> <ul style="list-style-type: none"> • Log subscription details. • All log files for a specific log subscription. • Log files using a filename or an URL. <p>For more information, see the Logging APIs section in the AsyncOS 13.8.1 API for Cisco Content Security Management Appliances - Getting Started Guide.</p>
Recording AAA (Authentication, Authorization, and Accounting) events using Audit Logs	<p>The Cisco Content Security Management Appliance supports a new type of log subscription—‘Audit Logs’ that records AAA (Authentication, Authorization, and Accounting) events. Some of the audit log details are as follows:</p> <ul style="list-style-type: none"> • User–Logon • User–Logon failed incorrect password • User–Logon failed unknown user name • User– Logon failed account expired • User–Logoff • User–Lockout • User–Activated • User–Password change • User–Password reset • User–Security settings/profile change • User–Created • User–Deleted or modified • User Configuration–Configuration changes made by the user • Group/Role–Deletion or modified • Group /Role–Permissions change • Quarantine–Actions performed on messages in the quarantine. <p>For more information, see Using Audit Logs, in the User Guide for AsyncOS 13.8.1 for Cisco Content Security Management Appliances.</p>

Configuring OpenID Connect 1.0 on Content Security Management Appliance for AsyncOS APIs	<p>The Cisco Content Security Management Appliance supports integration with applications or clients that use Identity Providers (IDPs) with OpenID Connect 1.0 authentication to connect seamlessly with AsyncOS APIs available in your appliance. Currently, your appliance has been certified with OpenID Connect using Microsoft AD FS only.</p> <p>For more information, see Common Administrative Tasks in the User Guide for AsyncOS 13.8.1 for Cisco Content Security Management Appliances.</p>
URL Search on Content Security Management appliance	<p>You can now perform a URL search on both incoming and outgoing URLs in the search bar available in the Web Interaction Tracking Page of the NG Reporting with the filter options Starts With and Exact Match within a selected time range. The search results can then be exported to a comma separated value (.CSV) file or sorted to view results in desired manner.</p>

Changes in Behavior

Casebook Behavior	<p>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.</p> <p>After you upgrade to this release, Casebook will be part of the Cisco SecureX Ribbon.</p>
Automatic Quarantine Queue Repair	<p>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.</p>
Passphrase Changes	<p>New user accounts cannot use passphrases containing three or more repetitive or sequential characters.</p>
Spam Quarantine Changes	<ul style="list-style-type: none"> • Prior to this release, the option to enable login without credentials for quarantine access was available under Edit Spam Quarantine > Spam Notifications > Message Body. <p>After upgrading to this release, this option is available under Edit Spam Quarantine > Spam Notifications > Quarantine Access.</p> <ul style="list-style-type: none"> • After upgrading to this release, you can configure the following options using the <code>spamdigestconfig</code> command in the CLI: <ul style="list-style-type: none"> - 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	<p>See SSL Configuration Changes, page 10</p>
Upgrade	<p>Important! After you perform an upgrade to Cisco Content Security Management 13.8.1-068, you cannot revert to any earlier version.</p>
Tunnel Services	<p>When you perform an upgrade, revert to earlier versions, reboot an appliance all the tunnel and service access will be disabled. You must enable the services again.</p>

Configuration Master	<p>Earlier Behavior</p> <p>In configuration masters page when user wants to change Configuration Master, commit is mandatory.</p> <p>Change in Behaviour</p> <p>In configuration masters page when user wants to change CM, upon clicking OK button in the popup window that CM is loaded, Yellow commit button does not appear.</p>
Sub Configuration Master	<p>Earlier Behavior</p> <p>Sub Configuration master gets overwritten and incorrectly pushed with Secondary configuration master.</p> <p>Change in Behaviour</p> <p>Note Do not perform any configuration changes simultaneously using:</p> <ul style="list-style-type: none"> • Multiple tabs on the same browser. • Multiple browsers on the same system or two different systems. <p>Also, do not use concurrent web interface and CLI sessions as it may lead to unexpected behavior.</p> <p>It is not recommended to concurrently switch or modify sub-Configuration masters. Additionally, User must not perform a configuration master push while changes are happening.</p> <p>However, if two users logged-in concurrently or same user logged-in from two different browsers and perform changes in Configuration Master concurrently, an error identifier message should be displayed to second user.</p>

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 13.8.1

- [Upgrading to AsyncOS 13.8.1-701 - LD \(Limited Deployment\)](#)

- [Upgrading to AsyncOS 13.8.1-090 - MD \(Maintenance Deployment\)](#)
- [Upgrading to AsyncOS 13.8.1-074 - MD \(Maintenance Deployment\)](#)
- [Upgrading to AsyncOS 13.8.1-068 - MD \(Maintenance Deployment\)](#)

Upgrading to AsyncOS 13.8.1-701 - LD (Limited Deployment)

You can upgrade to the release 13.8.1- 701 from the following versions:

- 13.8.1 - 052
- 13.8.1 - 090

Upgrading to AsyncOS 13.8.1-090 - MD (Maintenance Deployment)

You can upgrade to the release 13.8.1- 090 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 - 277
- 13.6.2 - 078
- 13.8.1 - 068
- 13.8.1 - 074

Upgrading to AsyncOS 13.8.1-074 - MD (Maintenance Deployment)

You can upgrade to the release 13.8.1- 074 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
- 13.6.2 - 052
- 13.6.2 - 058
- 13.8.1 - 068

Upgrading to AsyncOS 13.8.1-068 - MD (Maintenance Deployment)

You can upgrade to the release 13.8.1-068 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
- 13.6.2 - 052
- 13.8.0 - 344
- 13.8.1-052
- 13.8.1 - 063

Installation and Upgrade Notes

- [Important Additional Reading](#), page 8
- [Virtual Appliance](#), page 8
- [Pre-Upgrade Requirements](#), page 9
- [IPMI Messages During Upgrade](#), page 11
- [Upgrading to This Release](#), page 11

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 8 . |
| 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 9](#)
- [Back Up Your Existing Configuration, page 9](#)
- [Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode, page 10](#)
- [SSL Configuration Changes, page 10](#)

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 8](#).

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 9](#).
- 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 9](#).
-

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.

Supported Hardware for this Release

Supported Hardware:

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

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 13](#)
- [Lists of Known and Fixed Issues, page 13](#)

- [Finding Information about Known and Resolved Issues, page 13](#)

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=13.8.0,13.8.1&sb=af&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=Cisco%20Secure%20Email%20and%20Web%20manager&pf=prdNm&rls=13.8.0,13.8.1&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Finding Information about Known and Resolved Issues

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

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.

© 2024 Cisco Systems, Inc. All rights reserved.