Release Notes for AsyncOS 13.7 for Cisco Email Security Appliances

Published: December 3, 2020
Revised: October 28, 2021

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Retrieving log information using AsyncOS APIs	You can now retrieve the following log details from your email gateway using AsyncOS APIs: • Log subscription details. • All log files for a specific log subscription. • Log files using a filename or a URL. For more information, see the "Logging APIs" section in the *AsyncOS 13.7 API for Cisco Email Security Appliances - Getting Started Guide*.
Recording AAA (Authentication, Authorization, and Accounting) events using Audit Logs	The Cisco Email Security gateway 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: • 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. For more information, see the "Logging" chapter in the user guide or online help.
Configuring OpenID Connect 1.0 on Email Gateway for AsyncOS APIs	The Cisco Email Security gateway 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 email gateway. Currently, your email gateway has been certified with OpenID Connect using Microsoft AD FS only. For more information, see the "System Administration" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances.*

New Access Privilege – Log Subscription for Delegated Administrators	A new access privilege option - **Log Subscription** is added in the System Administration > User Role page in the web interface of your appliance. Use the Log Subscription option to define whether delegated administrators assigned to the custom user role can access log subscriptions or Logging APIs to view or download log files. For more information, see the "Distributing Administrative Tasks" chapter in the user guide or online help.
Support for Cloud Connector Logging	The appliance now supports a new type of log subscription - **Cloud Connector Logs**. Use this log subscription to view information about Web Interaction Tracking data from Cisco Aggregator Server. Most of the information is present at the Info or Warning Level.
Configuring Email Gateway to consume SecureX Threat Response Feeds	You can configure your email gateway to consume threat feeds from the Cisco SecureX Threat Response portal. The Cisco SecureX Threat Response portal allows you to create custom feeds for the continuous gathering of observables and to consume them in your email gateway using the feed URL. A feed is a simple list of observables in JSON format. The feeds are created and managed in the **Intelligence > Feeds** page in the SecureX Threat Response portal. For more information, see: • "How to Configure Email Gateway to Consume External Threat Feeds" and "Configuring SecureX Threat Response Feeds Source" sections in the "Configuring Email Gateway to Consume External Threat Feeds" chapter of the user guide associated with this release. • "Configuring Email Gateway to Consume External Threat Feeds" section in "The Commands: Reference Examples" chapter of the CLI reference guide associated with this release.

Changes in Behavior

File Reputation Service Configuration Changes	There is no option to enable or disable SSL communication when you onfigure the File Reputation service in your appliance. The appliance uses the SSL protocol by default to communicate with the File Reputation service using firewall port 443 only. The following options to configure SSL communication settings for the File Reputation service in your appliance are removed: • The **Use SSL (Port 443)** checkbox in Security Services > File Reputation and Analysis page in the web interface of your appliance. • The `Do you want to enable SSL communication (port 443) for file reputation? [Y]>` statement in `ampconfig` > `advanced` sub command in the CLI.
External Threat Feeds - File Hash Configuration Changes	The appliance now detects file hashes categorized as malicious by the External Threat Feeds (ETF) engine, irrespective of the letter case (uppercase or lowercase) and applies appropriate configured actions on the message.

Upgrade Paths

Upgrading to Release 13.7.0-093 - GD (General Deployment)

Note The AsyncOS 13.7.0-093 for Cisco Email Security Appliances is a general deployment release for Cisco Cloud Email Security users.

Note While upgrading, do not connect any devices [keyboard, mouse, management devices (Raritan), and so on] to the USB ports of your appliance.

You can upgrade to release 13.7.0-093 from the following versions:

- 12.1.0-087
- 12.5.0-066
- 12.5.2-011
- 13.0.0-392
- 13.5.1-177
- 13.5.1-277

- 13.5.1-352
- 13.5.2-036
- 13.5.2-204
- 13.5.3-010
- 13.7.0-087

Upgrading to Release 13.7.0-087 - LD (Limited Deployment)

Note While upgrading, do not connect any devices [keyboard, mouse, management devices (Raritan), and so on] to the USB ports of your appliance.

You can upgrade to release 13.7.0-087 from the following versions:

- 13.5.1-277
- 13.5.1-352

Note The AsyncOS 13.7 for Cisco Email Security Appliances release will be provisioned on an on-demand basis. We recommend you upgrade to AsyncOS 14.0 for Cisco Email Security Appliances release (which will be available in a few months) to receive further software maintenance releases.

Installation and Upgrade Notes

Read through and consider the installation and upgrade impacts listed in this section.

When you upgrade AsyncOS from the web interface or Command Line Interface (CLI), the configuration is saved to file in the /configuration/upgrade directory. You can access the upgrade directory using an FTP client. Each configuration file name is appended with the version number, and passwords in the configuration file are masked so they are not human readable.

You must be logged in as a user with administrator privileges to upgrade. Also, you must reboot the appliance after upgrading.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - C190
  - C195
  - C390
  - C395
  - C690
  - C695

- C695F

Note [For C695 and C695F models only]: Before you upgrade or restart the appliance, disable LLDP on the connected fiber switch port interface. This automatically disables the FCoE traffic.

To determine whether your appliance is supported, and to remedy the situation if it is not currently compatible, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html.

The following hardware is NOT supported for this release:

- C160, C360, C660, and X1060
- C170, C370, C370D, C670 and X1070
- C380 and C680 appliances

Deploying or Upgrading a Virtual Appliance

If you are deploying or upgrading a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/email-security-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 with this AsyncOS release using the documentation described in Deploying or Upgrading a Virtual Appliance, page 6.

Step 2 Upgrade your hardware appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded hardware appliance

Step 4 Load the configuration file from the hardware appliance onto the virtual appliance.

Be sure to select an appropriate option related to network settings.

Getting Technical Support for Virtual Appliances

Requirements for obtaining technical support for your virtual appliance are described in the *Cisco Content Security Virtual Appliance Installation Guide* available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

See also Service and Support, page 13, below.

Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances

Contact Cisco TAC for information required to provision your virtual appliance.

Pre-upgrade Notes

Before upgrading, review the following:

Firewall Settings to Access Cisco Talos Services

You need to open HTTPS (Out) 443 port on the firewall for the following hostnames or IP addresses (refer to the table below) to connect your email gateway to Cisco Talos services.

Note The HTTPS updater proxy configuration is used to connect to Cisco Talos services.

Hostname	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

For more information, see the “Firewall” chapter of the user guide.

Firewall Settings to Access Cisco Advanced Phishing Protection Cloud Service

You need to open HTTPS (Out) 443 port on the firewall for the following hostnames to connect your email gateway to Cisco Advanced Phishing Protection cloud service.

- kinesis.us-west-2.amazonaws.com
- sensor-provisioner.ep.prod.agari.com
- houston.sensor.prod.agari.com

For more information, see the "Firewall" chapter of the user guide.

Enabling Service Logs on Appliance

The Service Logs are used to collect personal data based on the Cisco Email Security Appliance Data Sheet guidelines.

The Service Logs are sent to the Cisco Talos Cloud service to improve Phishing detection.

The Cisco Email Security gateway collects limited personal data from customer emails and offers extensive useful threat detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed threat activity. Cisco uses the personal data to improve your email gateway capabilities to analyze the threat landscape, provide threat classification solutions on malicious emails, and to protect your email gateway from new threats such as spam, virus, and directory harvest attacks.

During the upgrade process, you can choose to enable Service Logs on your appliance in any one of the following ways:

- Select the **I Agree** option for Service Logs in the System Administration > System Upgrade page of the web interface.
- Type **Yes** for the *Do you agree to proceed with Service Logs being enabled by default? [y]>* statement in the upgrade CLI command.

For more information, see the “Improving Phishing Detection Efficacy using Service Logs” chapter of the user guide.

Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels

Before you upgrade to AsyncOS 13.7, ensure that the Intelligent Multi-Scan and Graymail configurations are at the same cluster level. If not, you must review the Intelligent Multi-Scan and Graymail settings after the upgrade.

FIPS Compliance

AsyncOS 13.7 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 13.7.

Reverting to Previous AsyncOS Versions

The following AsyncOS versions are affected by the Internal Testing Interface Vulnerability (http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa):

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047
- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

Upgrading Deployments with Centralized Management (Clustered Appliances)

If a cluster includes C160, C360, C660, X1060, C170, C370, C670, C380, C680, or X1070 hardware appliances, remove these appliances from the cluster before upgrading.

All machines in a cluster must be running the same version of AsyncOS, and x60, x70, and x80 hardware cannot be upgraded to this release. If necessary, create a separate cluster for your x60, x70, and x80 appliances.

Upgrading From a Release Other Than the Immediate Previous Release

If you are upgrading from a major (AsyncOS X.0) or minor (AsyncOS X.x) release other than the release immediately preceding this release, you should review the Release Notes for major and minor releases between your current release and this release.

Maintenance releases (AsyncOS X.x.x) include only bug fixes.

Configuration Files

Cisco does not generally support the backward compatibility of configuration files with previous major releases. Minor release support is provided. Configuration files from previous versions may work with later releases; however, they may require modification to load. Check with Cisco Customer Support if you have any questions about configuration file support.

IPMI Messages During Upgrade

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

Defect ID: CSCuz28415

Upgrading to This Release

Before You Begin

- Clear all the messages in your workqueue. You cannot perform the upgrade without clearing your work queue.
- Review the Known Issues, page 8 and Installation and Upgrade Notes, page 5.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 6.

Procedure

Use the following instructions to upgrade your Email Security appliance.

Step 1 Save the XML configuration file off the appliance.

Step 2 If you are using the Safelist/Blocklist feature, export the Safelist/Blocklist database off the appliance.

Step 3 Suspend all listeners.

Step 4 Wait for the work queue to empty.

Step 5 From the System Administration tab, select the System Upgrade page.

Step 6 Click the **Available Upgrades** button. The page refreshes with a list of available AsyncOS upgrade versions.

Step 7 Click the **Begin Upgrade** button and your upgrade will begin. Answer the questions as they appear.

Step 8 When the upgrade is complete, click the **Reboot Now** button to reboot your appliance.

Step 9 Resume all listeners.

What To Do Next

- After the upgrade, review your SSL configuration to ensure that you have selected the correct GUI HTTPS, Inbound SMTP, and Outbound SMTP methods to use. Use the **System Administration > SSL Configuration** page or the `sslconfig` command in CLI. For instructions, see the "System Administration" chapter in the User Guide or the online help.
- Review the Performance Advisory, page 11.
- If you have changed the SSH key, re-authenticate the connectivity between the Cisco Email Security appliance and the Cisco Security Management appliance after the upgrade.

Post-Upgrade Notes

Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 13.x

After upgrading to AsyncOS 13.x, if your appliances are in the cluster mode and DLP is configured, inconsistency in the DLP settings is seen when you run the `clustercheck` command using the CLI.

To resolve this inconsistency, force the entire cluster to use the DLP configuration of any of the other machines in the cluster. Use the following prompt - `How do you want to resolve this inconsistency?` in the `clustercheck` command as shown in the following example:

```
(Cluster)> clustercheck
Checking DLP settings...
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

Intelligent Multi-Scan and Graymail Global Configuration Changes

The following are the changes to the global settings configuration for Intelligent Multi-Scan (IMS) and Graymail after you upgrade to AsyncOS 13.7:

- If the global settings of IMS and Graymail are configured at different cluster levels, the appliance copies the global settings to the lowest configuration level. For example, if you configure IMS at the cluster level and Graymail at the machine level, the appliance copies the IMS global settings to the machine level.
- If the maximum message size and timeout values for scanning messages are different, the appliance uses the maximum timeout and maximum message size values to configure the IMS and Graymail global settings. For example, if the maximum message size values for IMS and Graymail are 1M and 2M respectively, the appliance uses 2M as the maximum message size value for both IMS and Graymail.

Performance Advisory

Outbreak Filters

Outbreak Filters uses the Context Adaptive Scanning Engine to determine the threat level of a message and scores messages based on a combination of Adaptive Rules and Outbreak Rules. In some configurations, you may experience a moderate performance decline.

IronPort Spam Quarantine

Enabling the IronPort Spam Quarantine on-box for a C-Series appliance causes a minimal reduction in system throughput for nominally loaded appliances. For appliances that are running near or at peak throughput, the additional load from an active quarantine may cause a throughput reduction of 10-20%. If your system is at or near capacity, and you desire to use the IronPort Spam Quarantine, consider migrating to a larger C-Series appliance or an M-Series appliance.

If you change your anti-spam policy from dropping spam to quarantining it (either on-box or off-box), then your system load will increase due to the need to scan additional spam messages for virus and content security. For assistance in properly sizing your installation please contact your authorized support provider.

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 11
- 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/search?kw=*&pf=prdNm&pfVal=282941569&rls=13.7.0&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941569&rls=13.7.0-093&sb=fr&sts=fd&svr=3nH&bt=custV

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://tools.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, 13.7

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.

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

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.
Cisco Content Security Management	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web Security	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Email Security	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html

Documentation For Cisco Content Security Products	Location
CLI reference guide for Cisco Content Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 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, have your Virtual License Number (VLN) number ready when you call Cisco TAC.

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site for legacy IronPort: 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.