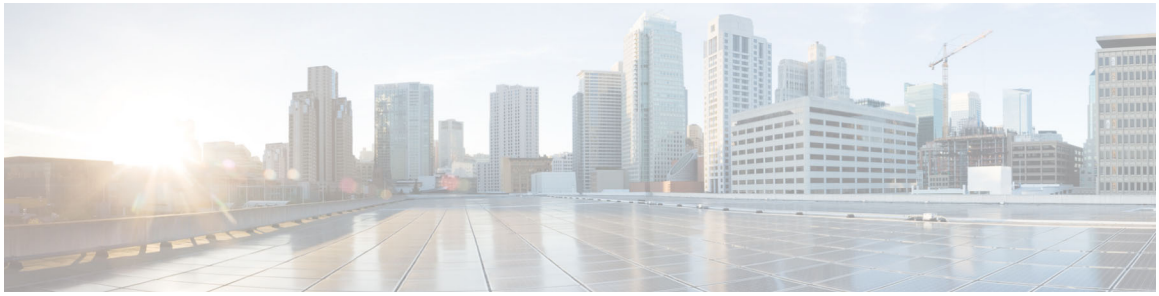

Release Notes for AsyncOS 12.0 for Cisco Email Security Appliances

Published: November 26, 2018

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Ability to consume External Threat Feeds	You can now configure your Cisco Email Security appliance to consume external threat information in STIX format communicated over TAXII protocol. The ability to consume external threat information in the appliance, helps an organization to: • Proactively respond to cyber threats such as, malware, ransomware, phishing attacks, and targeted attacks. • Subscribe to external threat feeds or other devices on your organization's network that is capable of fetching external threat feeds in STIX format communicated over a TAXII protocol, and consume the threat information in your appliance. • Import dynamic information (for example, a dynamic list of URLs) in your appliance and configure mail policies or define message actions based on the dynamic information. • Improve the efficacy of the appliance. If you are using the Classic licensing mode and you do not have an External Threat Feeds feature key, you must contact the Cisco Global Licensing Operations (GLO) team to obtain the feature key as follows: **Step 1** Send an email to the GLO team (licensing@cisco.com) with the message subject as "Request for External Threat Feeds Feature Key", and provide your Product Authorization Key (PAK) file and Purchase Order (PO) details in the email. **Step 2** The GLO team provisions the feature key manually, and sends you an email with the license key to install on your appliance. **Note** If you switch to the Smart Licensing mode on your appliance, you are automatically provided with an External Threat Feeds feature key. To configure this feature, see the "Configuring Cisco Email Security Gateway to Consume External Threat Feeds" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.

Filtering Messages using Sender's Domain Reputation	Cisco Sender Domain Reputation (SDR) is a cloud service that provides a reputation verdict for email messages based on a sender's domain and other attributes. This domain-based reputation analysis enables a higher spam catch rate by looking beyond the reputation of shared IP addresses, hosting or infrastructure providers, and derives verdicts based on features associated with fully qualified domain names (FQDNs) and other sender information in the SMTP conversation and message headers. For more information about SDR, contact Cisco Talos Security Intelligence and Research Group (Talos) at https://www.talosintelligence.com. To enable sender domain reputation filtering on your appliance, see the "Sender Domain Reputation Filtering" user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*. **Caution** AsyncOS 12.0 for Cisco Email Security Appliances has Sender Domain Reputation (SDR), that identifies, blocks a significant number of domain abuses. SDR sends Envelope From, From, Reply-To header information from the messages sent to you, to Cisco's threat intelligence data centers in the United States. See the updated Cisco Content Security Supplemental End User License Agreement: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html and Cisco Privacy Data Sheet for Cisco Email Security Appliances and Web Security Appliances: https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html. This feature is enabled by default. To disable it, choose Security Services > Domain Reputation settings.
Support for Cisco AMP Threat Grid Clustering for File Analysis	You can now add standalone or clustered Cisco AMP Threat Grid appliances for file analysis in any one of the following ways: • Security Services > File Reputation and Analysis page in the web interface. See the "File Reputation Filtering and File Analysis" chapter in the user guide. • `ampconfig` command in the CLI. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Configuring Threshold Settings for File Analysis	You can now set the upper threshold limit for the acceptable file analysis score. The files that are blocked based on the Threshold Settings are displayed as **Custom Threshold** in the Incoming Malware Threat Files section of the Advanced Malware Protection report. For more information, see the "File Reputation Filtering and File Analysis" chapter in the user guide.

Enhanced User Experience using How-Tos Widget	The How-Tos is a contextual widget that provides in-app assistance to users in the form of walkthroughs to accomplish complex tasks on your appliance. The following are the walkthroughs that are supported for this release: • Verifying Incoming Messages using DMARC • Verifying Incoming Messages using SPF/SIDF • Verifying Incoming Messages using DKIM • Enabling and Configuring Graymail Engine on the Email Security Gateway • Enabling and Configuring Outbreak Filters on the Email Security Gateway • Detecting macro-enabled attachments in messages **Note** The list of walkthroughs is cloud updateable. Make sure that you clear your browser cache to view an updated version of the How-Tos widget and pop-up window. For more information, see the "Accessing the Appliance" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Viewing malicious messages based on the threat name	In Message Tracking, you can now search for incoming or outgoing messages detected as malicious by the AMP engine based on the threat name. For more information, see the "Tracking Messages" chapter in the user guide.
DNS-based Authentication of Named Entities (DANE) support for Outgoing TLS Connections	You can now securely send messages to a valid recipient domain by enabling DNS-based Authentication of Named Entities (DANE) for outgoing TLS connections on your appliance. The ability to securely send messages to a valid recipient domain helps an organization to ensure that business critical and confidential information is delivered to the intended recipient, provided the destination domain supports DANE. For more information, see the "Encrypting Communication with Other MTAs" chapter in the user guide.

Support for Smart Software Licensing	Smart Software Licensing enables you to manage and monitor Cisco Email Security appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM), which is the centralized database that maintains the licensing details of all the Cisco products that you purchase and use. The following are the advantages when you switch from the Classic Licensing mode to the Smart Licensing mode on your appliance: • You can handle the Product Authorization Key (PAK) licenses between the physical and virtual appliances easily, which was difficult in the Classic Licensing mode. • You can easily migrate the software licenses between devices or virtual accounts in your organization. • You do not need to manage or keep a copy of the PAK files on your appliance. • You can restrict the user access on the Smart Licensing account. **Caution** After you enable the Smart Licensing mode on your appliance, you may not be able to rollback to the Classic Licensing mode. To use this feature, see the *Smart Software Licensing* chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Forged Email Detection Enhancement	You can now create an exception list consisting of only full email addresses to bypass the Forged Email Detection content filter in **Mail Policies > Address Lists**. You can use this exception list in the Forged Email Detection rule if you want the appliance to skip email addresses from the configured content filter. For more information, see the "Content Filters" chapter in the user guide.
Log Subscription enhancement	You can use the Rate Limit option to configure the maximum number of logged events in the log file, within the specified time range (in seconds). The default time range value is 10 seconds. Use the **System Administration > Log Subscriptions** page in the web interface or the `logconfig` command in CLI to set the rate limit. For more information, see the "Logging" chapter in the user guide.

Changes in Behavior

Changes in bypassing DMARC verification of messages	Prior to this release, you could skip DMARC verification of messages from senders based on the full email addresses configured in the address list. After you upgrade to this release, you can now skip DMARC verification of messages from senders based on full email addresses or domains configured in the address lists.
Changes in using default passphrase for first login	If you install a new virtual or hardware appliance of AsyncOS 12.0 system, it is now mandatory to change the default passphrase when you log in to the appliance for the first time using the web interface or the CLI.
Changes in configuring Domain Keys/DKIM Verification	Prior to this release, if your appliance is in FIPS mode, you could only use 2048-bit DKIM keys to verify incoming messages. After you upgrade to this release, if your appliance is in FIPS mode, you can verify your incoming messages using 1024, 1536, or 2048-bit DKIM keys.

Upgrade Paths

You can upgrade to release 12.0.0-281 from the following versions:

- 11.0.0-274
- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.1.0-131
- 11.1.0-135
- 11.1.1-042
- 12.0.0-208
- 12.0.0-227
- 12.0.0-269

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 - C380, C680, C190, C390, or C690.

  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 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 7.

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

Please contact Cisco TAC for information required to provision your virtual appliance.

Pre-upgrade Notes

Before upgrading, review the following:

FIPS Compliance

AsyncOS 12.0 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 12.0.

Upgrading Deployments with Centralized Management (Clustered Appliances)

If a cluster includes C160, C360, C660, X1060, C170, C370, C670 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 and x70 hardware cannot be upgraded to this release. If necessary, create a separate cluster for your x60 and x70 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 work queue. You cannot perform the upgrade without clearing your work queue.
- Review the Known and Fixed Issues, page 11 and Installation and Upgrade Notes, page 6.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 7.

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 10.

Post-Upgrade Notes

Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 12.x

After upgrading to AsyncOS 12.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]>
```

Performance Advisory

DLP

- Enabling DLP for outbound messages on an appliance that is already having anti-spam and anti-virus scanning running on inbound messages can cause a performance degradation of less than 10%.
- Enabling DLP on an appliance that is only running outbound messages and is not running anti-spam and anti-virus can cause higher performance degradation as compared to the previous scenario.

SBNP

SenderBase Network Participation now uses the Context Adaptive Scanning Engine (CASE) to collect data to power IronPort Information Services. In some configurations customers may experience a moderate performance decline.

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 or X-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 11
- Finding Information about Known and Resolved Issues, page 11

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=282509130&rls=12.0.0&sb=afr&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.0.0&sb=fr&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, 11.1

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.

Documentation for FCS

Important! For the most current and complete FCS documentation, see the .html version of the user guide on Cisco.com.

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
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.

This document is to be used in conjunction with the documents listed in the "Documentation for FCS" section.