Release Notes for AsyncOS 11.1 for Cisco Email Security Appliances

Published: January 25, 2018
Revised: April 23, 2018

Contents

- What's New In This Release, page 2
- Changes in Behavior, page 5
- Upgrade Paths, page 5
- Installation and Upgrade Notes, page 7
- Known and Fixed Issues, page 12
- Related Documentation, page 13
- Service and Support, page 13

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
URL Filtering Support for Shortened URIs	You can now configure your appliance to perform URL filtering on shortened URIs, and retrieve the actual URL from the shortened URL. Based on the URL reputation score of the original URL, a configured action is taken on the shortened URL To enable URL filtering on shortened URLs, make sure that your appliance is able to connect to the following domains: • bit.ly • tinyurl.com • ow.ly • tumblr.com • ff.im • youtu.be • tl.gd • plurk.com • url4.eu • j.mp • goo.gl • fb.me • alturl.com • wp.me • chatter.com • tiny.cc • ur.ly **Note** The list of domains is cloud updatable. To enable URL filtering for shortened URLs in your appliance, see the "Protecting Against Malicious or Undesirable URLs" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliance*.
Support for URL Scanning in Attachments	You can now configure your appliance to scan for URLs in message attachments, and perform configured actions on such messages. You can use the URL Reputation and URL Category content and message filters to scan for URLs in message attachments. For more details, see the "Using Message Filters to Enforce Email Policies", "Content Filters" and "Protecting Against Malicious or Undesirable URLs" chapters in the user guide or online help.

AMP for Endpoints Console Integration	You can now integrate your appliance with AMP for Endpoints console, and add your own blacklisted or whitelisted file SHAs. After the integration, when a file SHA is sent to the File Reputation server, the verdict obtained for the file SHA from the File Reputation Server is overridden by the verdict already available for the same file SHA in the AMP for Endpoints console. To integrate your appliance with AMP for Endpoints console, see the "File Reputation Filtering and File Analysis" chapter in the user guide. The Advanced Malware Report page now includes a new section - **Incoming Malware Files by Category** to view the percentage of blacklisted file SHAs received from the AMP for Endpoints console. The threat name of a blacklisted file SHA is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report. See the "File Reputation Filtering and File Analysis" chapter in the user guide or online help.
Handling Unscannable Messages	You can now configure your appliance to handle messages that are not scanned by the following engines: • Content Scanner • File Reputation and File Analysis services • URL Filtering To configure appropriate actions on such messages, see the "Using Message Filters to Enforce Email Policies", "File Reputation Filtering and File Analysis", "Protecting Against Malicious or Undesirable URLs" chapters in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Improved Pre-classification Efficacy (Reducing File Uploads to Cisco AMP Threat Grid)	The File Analysis service in your appliance now supports all the file types supported by Cisco AMP Threat Grid. You can use this feature to: • Upload files that only contain dynamic content for file analysis. This helps administrators to track the daily file upload limit. • Reduce file uploads for file analysis. **Note** If you are using the private cloud file analysis server version 2.4 or an earlier version, it is recommended that you do not enable the new file types for file analysis. To configure this feature, see the "File Reputation Filtering and File Analysis" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*. A new verdict - **Low Risk** is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the Incoming Files Handed by AMP section of the Advanced Malware Protection report and in Message Tracking. For more details, see the "Tracking Messages" chapter in the user guide.

Improving File Retrospective Verdict Alerts	You can now configure your appliance to suppress the retrospective verdict alerts for messages that are not delivered to the message recipient, dropped or quarantined. To enable this feature, see "File Reputation Filtering and File Analysis" or the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
CASE Enhancement	To improve the anti-spam efficacy, the appliance now sends DMARC, SPF, DKIM information to the Context Adaptive Scanning Engine. **Note** The Cisco Email Security appliance does not send any of your organization's sensitive data to the Context Adaptive Scanning Engine.
Restarting and Viewing the Status of Service Engines enabled on the appliance.	You can use the `diagnostic > services` sub command in the CLI to: • Restart the service engines enabled on your appliance without having to reboot your appliance. • View the status of the service engines enabled on your appliance. To use this feature, see the "System Administration" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*
Setting the Priority for Message Headers	You can set the priority for a message header to match the incoming and outgoing messages in your appliance. To enable this feature, see the "Mail Policies" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
New datacenter added in APJC region for File Reputation service	Cisco has added the following new datacenter in the APJC region for the File Reputation service: *APJC (cloud-sa.apjc.amp.cisco.com)* You can configure your Email Security appliances to use the new File Reputation service. For more information, see the "File Reputation Filtering and File Analysis" chapter in the user guide or the online help.

Changes in Behavior

URL Reputation and Category Changes in Content and Message Filters	Prior to this release, if you configure a 'URL Category' or 'URL Reputation' content or message filter in your appliance, by default, the appliance scans for URLs in the message body and subject. After you upgrade to this release, you can configure your appliance to scan for URLs in the message body and subject, message attachments, or both. The 'URL Reputation' and 'URL Category' content and message filter conditions include the following new options: • **Include Attachments** - to scan for URLs within the message attachments. • **Include Message Body and Subject** - to scan for URLs in the message body and subject.
S/MIME Verification Changes	The Cisco Email Security appliance now also verifies the certificate authority of the sender domain during S/MIME certificate verification.
Configuration File Changes	You will now not be able to save the configuration file for your appliance using the “plain passphrase” option in the web interface or the CLI.
Changes in Attachment File Info content or message filter	When you configure an 'Attachment File Info' content or message filter in your appliance based on any one of the following conditions: • Select the 'Filename' option, choose either 'Does Not Equal,' 'Does Not Contain,' 'Does Not End With,' or 'Does Not Begin With' options, and enter a file name. • Select the 'File type' option, choose the 'Is not' option, and choose the file type from the drop-down list. • Select the 'MIME type' option, choose the 'Is Not' option, and enter the MIME type. The appliance now performs the configured action on messages with or without attachments based on any one of the above conditions.

Upgrade Paths

- Upgrading to Release 11.1.0-131 - GD (General Deployment) Refresh, page 5
- Upgrading to Release 11.1.0-086 - LD (Limited Deployment) Refresh, page 6
- Upgrading to Release 11.1.0-072 - LD (Limited Deployment) Refresh, page 6
- Upgrading to Release 11.1.0-069 - LD (Limited Deployment), page 6

Upgrading to Release 11.1.0-131 - GD (General Deployment) Refresh

You can upgrade to release 11.1.0-131 from the following versions:

- 10.0.2-020
- 10.0.3-004

- 11.0.0-264
- 11.0.0-274
- 11.0.1-027
- 11.1.0-069
- 11.1.0-072
- 11.1.0-086
- 11.1.0-128

Upgrading to Release 11.1.0-086 - LD (Limited Deployment) Refresh

You can upgrade to release 11.1.0-086 from the following versions:

- 11.1.0-069
- 11.1.0-072

Upgrading to Release 11.1.0-072 - LD (Limited Deployment) Refresh

You can upgrade to release 11.1.0-072 from the following versions:

- 9.8.1-015
- 10.0.0-203
- 10.0.1-103
- 10.0.2-020
- 10.0.2-107
- 10.0.3-004
- 11.0.0-264
- 11.0.0-274
- 11.0.1-027
- 11.0.1-030
- 11.0.1-030
- 11.1.0-054
- 11.1.0-069

Upgrading to Release 11.1.0-069 - LD (Limited Deployment)

You can upgrade to release 11.1.0-069 from the following versions:

- 10.0.3-004
- 11.0.0-274
- 11.0.1-030
- 11.0.1-027

- 11.1.0-054

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 the admin to upgrade. Also, you must reboot the appliance after upgrading.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - C380, C390, C680, or C690
  - C190

    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

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

Pre-upgrade Notes

Before upgrading, review the following:

- No Support for RSA DLP Suite and RSA Enterprise Manager, page 8
- Performance Degradation on C100V Models, page 9
- FIPS Compliance, page 9
- Reverting to Previous AsyncOS Versions, page 9
- Upgrading Deployments with Centralized Management (Clustered Appliances), page 9
- Upgrading From a Release Other Than the Immediate Previous Release, page 9
- Configuration Files, page 9
- IPMI Messages During Upgrade, page 10

No Support for RSA DLP Suite and RSA Enterprise Manager

RSA has announced End of Life (EOL) for RSA Data Loss Prevention Suite (DLP). Cisco now provides an alternative DLP solution that allows seamless migration of all the existing DLP policies created in RSA DLP to the new DLP engine. After the upgrade, you can view or modify the migrated DLP policies in Security Services > Data Loss Prevention page in the web interface. For more information, see the "Data Loss Prevention" chapter in the user guide.

There is no support for RSA Enterprise Manager Integration in Async0S 11.0 and later. If you have DLP policies created in RSA Enterprise Manager, you must recreate those policies in your appliance after the upgrade.

Performance Degradation on C100V Models

After you upgrade to AsyncOS 11.1 on C100V models, you might experience a performance degradation in certain configurations. For more details, see

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCve27500

FIPS Compliance

AsyncOS 11.1 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 11.1.

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 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

- Review the Known and Fixed Issues, page 12 and Installation and Upgrade Notes, page 7.
- 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 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.

Post-Upgrade Notes

Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 11.x

After upgrading to AsyncOS 11.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 12
- Lists of Known and Fixed Issues, page 12
- Related Documentation, 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/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.0&sb=afr&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.0&sb=fr&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, 11.1.1

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.

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.