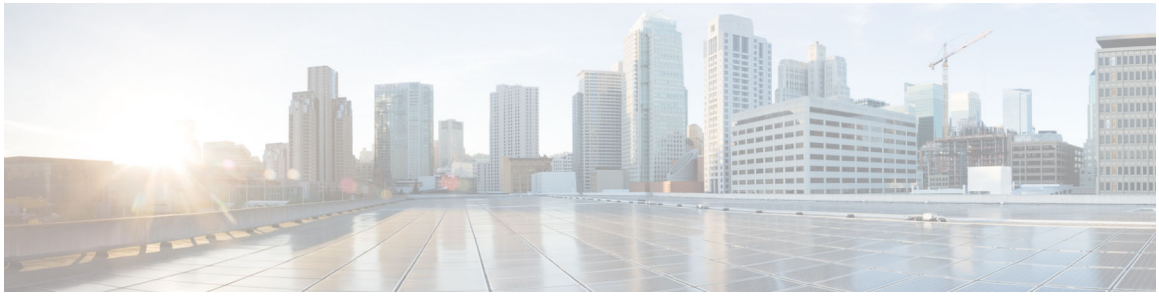

Release Notes for AsyncOS 12.1 for Cisco Email Security Appliances

Published: April 12, 2019
Revised: June 20, 2019

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Intelligent Multi-Scan Enhancement	Intelligent Multi-Scan (IMS) is a high performant multi-layer anti-spam solution. Cisco Email Security appliance provides an updated IMS engine with this release. This engine has a different combination of anti-spam engines that can increase the spam catch rates. To use the updated IMS engine, you must add the IMS feature key and accept the license in your appliance. For the existing IMS users, all the mail policies for IMS are migrated to work seamlessly with the updated IMS engine.
Minimum Scores for Entity-based Rules of Custom Classifiers for Custom DLP Policies	You can now use the recommended minimum scores or choose to override the minimum score for entity-based rules, when you create custom classifiers for custom DLP policies. You can use the minimum score for an entity-based rule instead of the configured weight of the rule. The minimum score differentiates the partial and the full matches, and calculates the score accordingly. This helps in reducing the number of false positives and false negatives. To configure the minimum score: 1. Go to **Mail Policies > DLP Policy Customizations > Custom Classifiers Settings** section and select the Use recommended minimum scores for entity-based rules check box. 2. Go to **Mail Policies > DLP Policy Customizations > Add Custom Classifier** (or review an existing custom classifier) and enter the minimum score. For more information, see the "Data Loss Prevention" chapter in the user guide.

Changes in Behavior

SSL Configuration Changes	After you upgrade to this release, you cannot enable TLS v1.0 and v1.2 methods simultaneously. However, you can enable these methods in conjunction with the TLS v.1.1 method, when you configure SSL settings.
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.

Changes in Character Encoding supported for Data Loss Prevention (DLP)	Data Loss Prevention now supports the following character encodings for multi-byte plain text files in Chinese, Japanese and Korean languages: • Traditional Chinese (Big5) • Simplified Chinese (GB2312) • Korean (KS-C-5601/EUC-KR) • Japanese (Shift-JIS(X0123)) • Japanese (EUC). However, Data Loss Prevention (DLP) does not support the following character encodings: • Japanese (ISO-2022-JP) • Korean (ISO2022-KR) • Simplified Chinese (HZGB2312)
Changes in Mail Policy Settings	After you upgrade to this release, you can set the priority in which the appliance checks for message headers in the incoming and outgoing messages. The appliance first checks for the message header with the highest priority for all the mail policies. If there is no header match in any of the mail policies, the appliance looks for the next message header in the priority list for all the mail policies. If none of the message headers match in any of the mail policies, the default mail policy settings are used.

Upgrade Paths

Upgrading to Release 12.1.0-089 - GD (General Deployment) Refresh

You can upgrade to release 12.1.0-089 from the following versions:

- 9.7.2-145
- 11.0.0-274
- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.0.3-238
- 11.0.3-242
- 11.1.0-128
- 11.1.0-131
- 11.1.0-135
- 11.1.0-603

- 11.1.1-042
- 11.1.2-023
- 11.1.2-509
- 11.1.2-701
- 11.1.2-802
- 12.0.0-281
- 12.0.0-419
- 12.1.0-071
- 12.1.0-085
- 12.1.0-087

Upgrading to Release 12.1.0-087 - GD (General Deployment) Refresh

You can upgrade to release 12.1.0-087 from the following versions:

- 9.7.2-145
- 11.0.0-274
- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.0.3-238
- 11.0.3-242
- 11.1.0-128
- 11.1.0-131
- 11.1.0-135
- 11.1.0-603
- 11.1.1-042
- 11.1.2-023
- 11.1.2-509
- 11.1.2-701
- 11.1.2-802
- 11.1.3-006
- 12.0.0-281
- 12.0.0-419
- 12.1.0-071
- 12.1.0-085

Upgrading to Release 12.1.0-071 - GD (General Deployment)

You can upgrade to release 12.1.0-071 from the following versions:

- 11.0.0-274
- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.0.3-238
- 11.1.0-128
- 11.1.0-131
- 11.1.0-135
- 11.1.0-603
- 11.1.1-042
- 11.1.2-023
- 11.1.2-509
- 11.1.2-701
- 11.1.2-802
- 12.0.0-281
- 12.0.0-419
- 12.1.0-043
- 12.1.0-070

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 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 11, 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 12.1 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 12.1.

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 10 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 9.

Post-Upgrade Notes

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 12.1:

- 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.

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 10
- Lists of Known and Fixed Issues, page 10
- Finding Information about Known and Resolved Issues, page 10

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=12.1&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.1.0-089&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, 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.

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 "Related Documentation" section.