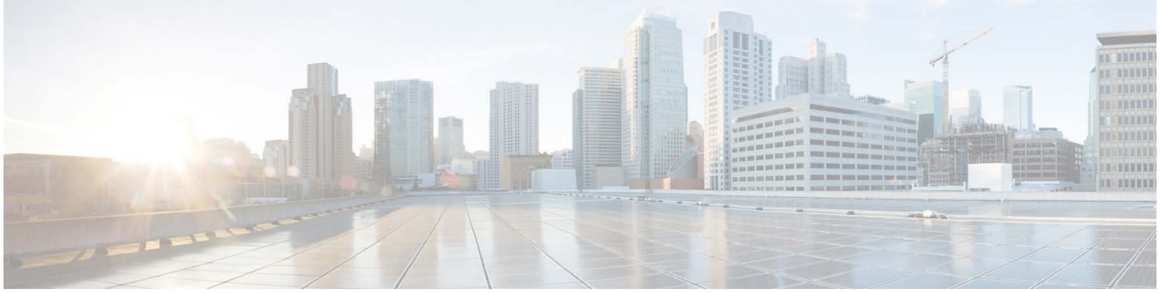

Release Notes for AsyncOS 12.5.3 for Cisco Email Security Appliances

Published: March 3, 2021
Revised: May 19, 2023

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

What's New In AysncOS 12.5.3

Feature	Description
Enhancement for Request Retry Method of File Reputation Service	You can now set the reputation query timeout value within the range of 20–30 seconds while configuring the file reputation and analysis services (Security Services > File Reputation and Analysis). The default value is 20, which is the minimum value. During the configured query timeout, the appliance sends the file reputation queries to the AMP server. If the appliance fails to receive response from the AMP server, it retries by sending the query again to the AMP server. The query timeout includes the time taken for the first query request and the retry request. The retry method enables the appliance to receive responses when there are network latencies, issues related to the AMP server, and so on.
New Cisco Talos Email Status Portal	The Cisco Talos Email Status Portal replaces the legacy Cisco Email Submission and Tracking Portal. The Cisco Talos Email Status Portal is a web-based tool for monitoring the status of email submissions from end-users. **Important:** • Users of the legacy portal can still access their previous submissions in the new portal. • You will not be able to submit samples of spam, phish, ham, marketing or non-marketing emails that may have been misidentified by your email appliance in the new portal. For more information on how to submit email samples, see the How to Submit Email Messages to Cisco document at https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html#

What's New In AysncOS 12.5.2

This release contains a number of bug fixes; see the Known and Fixed Issues, page 20 for additional information.

What's New In AysncOS 12.5.1

This release contains a number of bug fixes; see the Known and Fixed Issues, page 20 for additional information.

What's New In AysncOS 12.5.0

Feature	Description
New Hardware Support	The AsyncOS 12.5 release for Cisco Email Security appliances supports the following hardware models: • C195 • C395 • C695 • C695F For more information, see https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet_c22-739910.html.
Improved Advanced Malware Protection (AMP) Quarantine Management	During the AMP engine scanning process, an attachment that receives an unknown verdict from the File Reputation service is sent for a pre-classification check and file analysis. During the pre-classification check phase, the message is now stored locally in your Email Security appliance and then sent to the Centralized Quarantine only when the attachment is sent for a complete file analysis. This improves the performance and reduces the overall load on the centralized quarantine.
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*.

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*.
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: **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. **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*.

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. **Note** The 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.
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.

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 feature on your appliance, you will not be able to roll back from Smart Licensing to 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*.

Configuring content and message filters to handle messages that skipped DMARC verification	You can configure your appliance to take actions on the messages that skipped the DMARC verification.
	Use the following settings in the Other Header content filter to categorize the messages that skipped the DMARC verification:
	• Add the Header Name as `X-Ironport-Dmarc-Check-Result`
	• Select **Header Value**, choose **Equals**, and add any one of the following values - `validskip`, `invalidskip`, `temperror`, and `permerror`
	The following is an example of a message filter rule syntax that is used to categorize a message that skipped the DMARC verification:
	`Quarantine_messages_DMARC_skip: if`
	`(header("X-Ironport-Dmarc-Check-Result") == "^validskip$") {`
	`quarantine("Policy"); }`
	For more information on the header values used in the content and message filters, contact Cisco TAC.

Ability to view or delete Cisco Content Security Management appliance connection parameters and host keys	You can now view or delete the Cisco Content Security Management appliance connection parameters and host keys in your appliance by using the `smaconfig` CLI command.

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

Changes in Behavior in AsyncOS 12.5.3

External Thread Feeds - File Hash Configuration Changes	The appliance now detects file hashes categorized as malicious by the External Thread Feeds (ETF) engine, irrespective of the letter case (uppercase or lowercase) and applies appropriate configured actions on the message.
Registering Appliance with Cisco Talos Email Status Portal Changes	You must now obtain a registration ID from the new Cisco Talos Email Status Portal before you register your appliance with the new portal.
SSL Cipher Configuration Changes	The @STRENGTH parameter is now added to the default SSL cipher strings for Inbound SMTP, Outbound SMTP, and GUI connections. Now, all connection requests sent from your appliance (acting as a client) to a remotely configured MTA (acting as a server) will get rejected if the MTA supports only weak ciphers and older TLS methods. The @STRENGTH parameter sorts the cipher list and displays the strongest ciphers at the top of the list. Based on the selected TLS method, the cipher list will not contain all the weak ciphers.
Changes in Sophos Anti-Virus Configuration Settings on Appliance	Prior to this release, the StrongPDF option was automatically enabled by default in the Sophos Anti-Virus engine in your appliance. The Sophos Anti-Virus engine used the StrongPDF option to categorize clean PDF files that were corrupted as "unscannable" because of EOF (End-of-File) missing, and so on. After you upgrade to this release, the StrongPDF option is disabled by default. The Sophos Anti-Virus engine now automatically categorizes clean PDF files that were corrupted as "clean" because of EOF (End-of-File) missing, and so on. You can use the *`antivirusconfig`* > `PDF` sub command in the CLI to enable the StrongPDF option on the Sophos Anti-Virus engine in your appliance.
File Reputation Service Configuration Changes	There is no option to enable or disable SSL communication when you configure 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.
Changes to Login Username	Prior to this release, you could not log in to your appliance with a username that consists of only numerical digits. After you upgrade to this release, you can now log in to your appliance with a username that consists of only numerical digits.
File Reputation Query Timeout Changes	The appliance now adds extra buffer time of 2 seconds to the total timeout period during the file reputation query process.

Changes in Behavior in AsyncOS 12.5.2

Content Scanner Changes	The Content Scanner in your appliance can now extract file names at the first nested level inside password-protected zipped attachments in incoming and outgoing messages.

Changes in Behavior in AsyncOS 12.5.1

Changes to Passphrase Settings	The option to automatically generate a login passphrase is removed. You must now manually enter a passphrase of your choice.
Changes in alerts when database size limit is reached	After you upgrade to this release, an alert is sent when the messages in the database that stores the message details and file retrospective details, reaches a size of 2GB. Contact Cisco Customer support to analyse the database and take corrective measures.

Changes in Behavior in AsyncOS 12.5.0

Changes in deleting text resources	Prior to this release, you could delete the text resources that are referenced in any incoming message or content filters. After you upgrade to this release, you cannot delete text resources that are referenced in any incoming message or content filters.
Changes when scanning attachments with long file names	If the file name of the attachment contains more than 255 characters, the attachment and files within the attachment are marked as unscannable and not processed further in the email pipeline. The Message Tracking page and the AMP log display the truncated file name in the following format: `<First 225 characters of original filename+'~too_long_name~'+the last ten characters of original filename>`
Changes while loading the configuration file for File Analysis	The following are the behavior changes when you load the configuration file for File analysis using Configuration File > Load Configuration option in the web interface: • The file types under the file groups are selected as per the configuration file and the other file types remain unselected. • You cannot add a new file type or change the group for the file type using the Load Configuration option.
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.
Changes to the SMTP route configuration with the USEDNS keyword	Prior to this release, you could use only the default port (25) as the destination port to configure the SMTP route with the `USEDNS` keyword. After you upgrade to this release, you can use any valid destination port to configure the SMTP route with the `USEDNS` keyword.
Handling Unscannable Messages due to decoding errors found during URL Filtering actions	The Cisco Email Security appliance can now handle messages that are not scanned due to decoding errors found during URL Filtering actions. You can configure any of the following actions on such messages through the **Security Services > Scan Behavior >Edit Global Settings** page in the web interface: • Modify the message subject. • Add a custom header to the message. • Modify the message recipient. • Send the message to alternate destination host. • Quarantine the message. For more information, see 'Configuring Scan Behavior' chapter in Email Security Appliance user guide.
Changes in Demo Certificates	Prior to this release, the appliance was pre-configured with a demonstration certificate to enable the TLS connections. After you upgrade to this release, the appliance generates a unique certificate to enable TLS connection. The existing demonstration certificate that is used in the following configurations are replaced with the new certificate: • Mail Delivery • LDAP • Networking • URL Filtering • SMTP Services
Changes in Threshold Value for Memory Page Swapping	Prior to this release, the default threshold level for memory page swapping was measured based on the number of pages. After you upgrade to this release, you can now configure your appliance to measure the threshold value for memory page swapping in percentage. The default threshold value for memory page swapping is set to 10%.

Changes in Envelope Settings for Encrypted Messages	Prior to this release, the 'Use Decryption Applet' option in the **Security Services** > **Cisco Ironport Email Encryption** > **Add Encryption Envelope Profile** page was enabled by default to allow the message attachment to be opened in the browser environment. After you upgrade to this release, the 'Use Decryption Applet' option in the **Security Services** > **Cisco Ironport Email Encryption** > **Add Encryption Envelope Profile** page is disabled by default. This allows the message attachments to be decrypted at the key server and to open the attachments independent of the browser environment.
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 12.5.3-041 - MD (Maintenance Deployment) Refresh

You can upgrade to release 12.5.3-041 from the following versions:

- 11.0.4-003
- 11.0.4-004
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-071
- 11.5.0-076
- 12.0.0-419
- 12.1.0-071
- 12.1.0-087
- 12.1.0-089
- 12.5.0-066
- 12.5.1-031
- 12.5.1-037
- 12.5.2-011
- 12.5.3-035

Upgrading to Release 12.5.3-035 - MD (Maintenance Deployment)

You can upgrade to release 12.5.3-035 from the following versions:

- 11.0.4-003
- 11.1.1-042
- 11.1.2-023

- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-071
- 11.5.0-076
- 12.0.0-419
- 12.5.0-066
- 12.5.1-037
- 12.5.2-011
- 12.5.2-110

Upgrading to Release 12.5.2-011 - MD (Maintenance Deployment)

You can upgrade to release 12.5.2-011 from the following versions:

- 11.0.1-027
- 11.0.2-044
- 11.0.3-242
- 11.0.3-251
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-058
- 11.5.0-071
- 11.5.0-077
- 12.0.0-419
- 12.1.0-087
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-037
- 12.5.1-044

Upgrading to Release 12.5.1-037 - MD (Maintenance Deployment)

You can upgrade to release 12.5.1-037 from the following versions:

- 11.0.1-027
- 11.0.2-044
- 11.0.3-242
- 11.0.3-251
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-058
- 11.5.0-071
- 11.5.0-076
- 11.5.0-077
- 12.0.0-419
- 12.1.0-087
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-031

Upgrading to Release 12.5.1-031 - MD (Maintenance Deployment)

You can upgrade to release 12.5.1-031 from the following versions:

- 11.0.1-027
- 11.0.2-044
- 11.0.3-242
- 11.0.3-251
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-058
- 11.5.0-071

- 11.5.0-076
- 11.5.0-077
- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066

Upgrading to Release 12.5.0-066 - GD (General Deployment)

You can upgrade to release 12.5.0-066 from the following versions:

- 11.0.1-027
- 11.0.2-044
- 11.0.3-238
- 11.0.3-242
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-058
- 11.5.0-077
- 12.0.0-419
- 12.1.0-089
- 12.5.0-051
- 12.5.0-059

Upgrading to Release 12.5.0-059 - LD (Limited Deployment)

You can upgrade to release 12.5.0-059 from the following versions:

- 11.0.1-027
- 11.0.2-044
- 11.0.3-238
- 11.0.3-242
- 11.1.1-042
- 11.1.2-023
- 11.5.0-058
- 11.5.0-071

- 11.5.0-076
- 11.5.0-077
- 12.0.0-419
- 12.1.0-087
- 12.1.0-089
- 12.5.0-051

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, C380, C390, C395, C680, C690, C695, and C695F.

  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 16.

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.

Step 5 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 23, 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, page 17
- Upgrading Deployments with Centralized Management (Clustered Appliances), page 18
- Upgrading From a Release Other Than the Immediate Previous Release, page 18
- Configuration Files, page 18
- IPMI Messages During Upgrade, page 18
- TLS 1.0 Support for Cisco Email Encryption Service, page 18

FIPS Compliance

AsyncOS 12.5 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 12.5.

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

TLS 1.0 Support for Cisco Email Encryption Service

TLS 1.0 support for Cisco Email Encryption service will be disabled by June 2020. If you are using the Easy Open feature of the Cisco Email Encryption service, it is mandatory to upgrade your appliance to AsyncOS 12.5.1 or higher version.

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 20 and Installation and Upgrade Notes, page 16.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 16.

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 20.

Post-Upgrade Notes

- Intelligent Multi-Scan and Graymail Global Configuration Changes, page 19
- Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 12.x, page 19

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

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 21
- Lists of Known and Fixed Issues, page 21
- Finding Information about Known and Resolved Issues, page 22

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 and Fixed Issues for 12.5.3, page 21
- Known and Fixed Issues for 12.5.2, page 21
- Known and Fixed Issues for 12.5.1, page 21
- Known and Fixed Issues for 12.5.0, page 21

Known and Fixed Issues for 12.5.3

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&prdNam=Cisco%20IronPort%20Email%20Security%20Appliance%20Software&kw=*&bt=custV&sb=afr&svr=3nH&rls=12.5.3
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&prdNam=Cisco%20IronPort%20Email%20Security%20Appliance%20Software&kw=*&bt=custV&sb=fr&svr=3nH&rls=12.5.3-041

Known and Fixed Issues for 12.5.2

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.2&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.2-011&sb=fr&sts=fd&svr=3nH&bt=custV

Known and Fixed Issues for 12.5.1

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.1&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.1-037&sb=fr&sts=fd&svr=3nH&bt=custV

Known and Fixed Issues for 12.5.0

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.0-066&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, 12.5.3

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.

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.