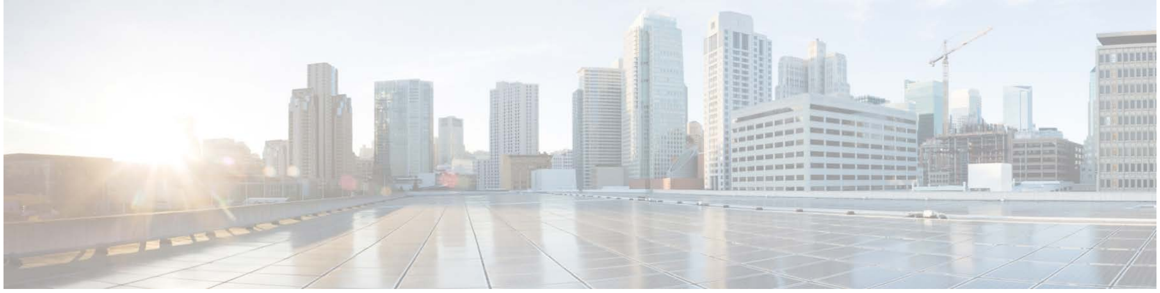

Release Notes for AsyncOS 13.5.3 for Cisco Email Security Appliances

Published: February 1, 2021

Revised: February 5, 2024

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

What's New in AsyncOS 13.5.3

Feature	Description
Support for Cloud Connector Logging	The Cisco Email Security appliance now supports a new type of log subscription - **Cloud Connector Logs**. Use this log subscription to view information about Web Interaction Tracking data from Cisco Aggregator Server. Most of the information is present at the Info or Warning Level.

What's New in AsyncOS 13.5.2

Feature	Description
Cisco SecureX Integration	Cisco Email Security appliance now supports integration with Cisco SecureX. Cisco SecureX is a security platform embedded with every Cisco security product. The integration of the Email Security appliance with Cisco SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration. Cisco SecureX unifies visibility of security infrastructure, enables automation, accelerates incident response workflows, and improves threat detection. The distributed capabilities of Cisco SecureX are available in the form of applications (apps) and tools in the Cisco SecureX Ribbon. For more information, see "Integrating with Cisco SecureX or Cisco Threat Response" chapter in the user guide or online help. You can also access the "Integrate Cisco Email Security Gateway with Cisco SecureX or Cisco Threat Response" walkthrough by clicking the How-Tos widget on the web interface of your appliance. To view the complete list of walkthroughs supported in each release, see Walkthroughs Supported in AysncOS for Cisco Email Security Appliances.

Enhancement to Messages with File Analysis Pending functionality	A new option - **Drop Message Attachments while File Analysis Verdict Pending** is added under **Messages with File Analysis Pending** section (Mail Policies > Incoming Mail Policies and click the link in the Advanced Malware Protection column of the mail policy to modify.) Now, you can choose whether to drop attachments in case of any file analysis verdict pending while delivering the final message from the appliance. The default option is 'No.' If you set the option as 'Yes', the Processing Details section of the Message Tracking (Monitor > Message Tracking) displays the details related to the message attachments dropped when the file analysis verdict is pending. The Mail logs also display the log details of the message attachments dropped when the file analysis verdict is pending based on the configured AMP policy. You can also enable this option using the `policyconfig` command in the CLI. For more information, see "File Reputation Filtering and File Analysis" chapter in the user guide or online help.
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.

Configuring Custom SMTP Helo for SMTP Conversation	A new option is added in the `interfaceconfig` > `edit` subcommand in the CLI to configure custom SMTP Helo for SMTP conversation. You can use the new CLI option to modify the default interface hostname used for the SMTP Helo.
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# For more information, see the "Managing Spam and Graymail" chapter in the user guide or online help.

What's New in AsyncOS 13.5.1

Feature	Description
Search and Remediate Messages in the Mailboxes	You can now configure your appliance to remediate the messages manually using the Search and Remediate feature. This feature provides the capability to search for the messages using the Message Tracking filter and apply remedial action on the messages. For more information, see "Remediating Messages in Mailboxes" chapter in the user guide or online help.
Improving User Experience of Cisco Email Security Gateway using Cisco Success Network	You can use the Cisco Success Network (CSN) feature to send your appliance and feature usage details to Cisco. These details are used by Cisco to identify the appliance version and the features activated but not enabled on your appliance. The ability to send your appliance and feature usage details to Cisco helps an organization to: • Improve the effectiveness of the product in user networks by performing analytics on collected telemetry data and suggesting users with recommendations using a digital campaign. • Improve user experience with Cisco Email Security gateway. For more information, see "Integrating with Cisco Threat Response" chapter in the user guide or online help.

New Cisco Talos Email Status Portal	The new 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. **Note** Users of the legacy portal can still access their previous submissions in the new portal. **Note** 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 gateway 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# For more information, see "Managing Spam and Graymail" chapter in the user guide or online help.
Ability to connect Appliance to Cisco Threat Response using proxy server	You can now connect your appliance to Cisco Threat Response using a proxy server. You can configure a proxy server in any one of the following ways: • Security Services > Service Updates page in the web interface. • `updateconfig` > `setup` sub command in the CLI. For more information, see "System Administration" chapter in the user guide
Accessing new web interface of appliance in Dusk Mode	Dusk Mode is a reversed color scheme that utilizes light-colored typography, UI elements, and iconography on dark backgrounds. You can now access the new web interface of your appliance using the dusk mode. To switch to the dusk mode, click on the user icon on the top-right corner of the new web interface and select **Dusk Theme**. For more information, see "Setup and Installation" chapter in the user guide

Support for APJC data center on Cisco Threat Response Server	You can now choose the APJC data center as the Cisco Threat Response server to connect your appliance to Cisco Threat Response. For more information, see "Integrating with Cisco Threat Response" chapter in the user guide or online help and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances.*
New Walkthroughs available on the 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 added in this release: • Prevent Accidental Leak of Financial Data • Allow Phishing Awareness Campaign Messages to Bypass Scanning Engines **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*. To view the complete list of walkthroughs supported in each release, see Walkthroughs Supported in AysncOS for Cisco Email Security Appliances.

What's New in AsyncOS 13.5.0

Feature	Description
Integrating the Cisco Email Security Gateway with Cisco Advanced Phishing Protection cloud service	The Cisco Advanced Phishing Protection engine on the Cisco Email Security Gateway checks the unique behavior of all legitimate senders, based on the historic email traffic sent to your organization. The cloud service interface of Cisco Advanced Phishing Protection provides risk analysis to distinguish good messages from potentially malicious messages. The Cisco Advanced Phishing Protection cloud service relies on the email gateway as a sensor engine to receive a copy of the message metadata sent inbound into your organization. This sensor engine collects metadata such as message headers from the email gateway and relays them to the Cisco Advanced Phishing Protection cloud service for analysis. After the analysis, potentially malicious messages are remediated from the recipient mailbox automatically based on the pre-configured policies on the Cisco Advanced Phishing Protection cloud service. The ability to use the Cisco Email Security Gateway as a sensor engine helps an organization to: • Identify, investigate, and remediate threats, observed on the message headers from the recipient mailbox. • View the reporting data of the metadata of the message from multiple email gateways in your organization. • Send real-time alerts to the end-users about malicious messages. For more information, see "Integrating the Cisco Email Security Gateway with Cisco Advanced Phishing Protection" chapter in the user guide.
Improve Phishing Detection Efficacy using Service Logs	The Service Logs feature are used to collect personal data based on the Cisco Email Security Appliance Data Sheet guidelines. The Service Logs are sent to the Cisco Talos Cloud service to improve Phishing detection. For more information, see Enabling Service Logs on Appliance, page 6.

Improved Phishing Efficacy	The Cisco Email Security appliance now provides improved IP Reputation and URL Reputation services for faster and better Phishing catch rates. For more information, see the *User Guide for AsyncOS 13.5 for Cisco Email Security Appliances*.

Note If you have configured an HTTP proxy server, the IP Reputation and URL Reputation services, and Service Logs will directly connect to the Internet to get the IP and URL reputations. If you want to use proxy for these services, then configure the HTTPS proxy server on your email gateway.

Note If you have configured an HTTPS proxy server, make sure that you do not configure the proxy server to decrypt the HTTPS traffic originating from your email gateway.

Note Make sure you do not use application-layer firewall rules [for example, Server Name Indication (SNI) matching] in your network to allow email traffic between your email gateway and the Cisco IP Reputation and URL Reputation services and Service Logs that use TLS 1.3 secure protocol.

Changes in Behavior

- Changes in Behavior in AsyncOS 13.5.3, page 9
- Changes in Behavior in AsyncOS 13.5.2, page 9
- Changes in Behavior in AsyncOS 13.5.1, page 10
- Changes in Behavior in AsyncOS 13.5.0, page 11

Changes in Behavior in AsyncOS 13.5.3

File Reputation Service Configuration Changes	There is no option to enable or disable SSL communication when you onfigure the File Reputation service in your appliance. The appliance uses the SSL protocol by default to communicate with the File Reputation service using firewall port 443 only. The following options to configure SSL communication settings for the File Reputation service in your appliance are removed: • The **Use SSL (Port 443)** checkbox in Security Services > File Reputation and Analysis page in the web interface of your appliance. • The `Do you want to enable SSL communication (port 443) for file reputation? [Y]>` statement in `ampconfig` > `advanced` sub command in the CLI.
External 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.

Changes in Behavior in AsyncOS 13.5.2

Casebook Behavior	Prior to AsyncOS 13.5.2 release, **Casebook** was a standalone widget. After you upgrade to this release, **Casebook** is a part of the Cisco SecureX Ribbon.
System Health Check Changes	Prior to this release, the system health check was done automatically during the upgrade process. After you upgrade to this release, you can perform the system health check manually in any one of the following ways: • Go to System Administration > System Health > Run System Health Check option in the web interface. See the "System Administration" chapter in the user guide. • Use the `healthcheck` command in the CLI. See the *"CLI Reference Guide for AsyncOS for Cisco Email Security Appliances."*
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. For more information, see "Managing Spam and Graymail" chapter in the user guide or online help.
Disclaimer Changes during Decoding Errors	If the disclaimer added to the footer or header of the message generates a decoding error, the disclaimer or message body is split into separate message attachment.

Changes in Behavior in AsyncOS 13.5.1

Content Scanner Changes	The Content Scanner in your appliance can now extract file names at the first nested level of password-protected attachments (.zip format) for messages.
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	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.Appliance
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.
No Support for Domain Names containing Underscore (_)	The Cisco Email Security appliance will not process the messages that contain an Underscore (_) in the domain name part of an email address.
Changes in Message-ID Header for Incoming Messages	The appliance now adds a system-generated message-ID header for all incoming messages that do not contain a message-ID header. The system-generated message-ID header is added to the message at the time of mail delivery after the appliance processes the message.
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.
DANE Verification Changes	The DANE verification is now bypassed for domains that have DANE enabled and added in SMTP routes for outgoing message
No Support for RC4 Encryption Algorithm	There is now no support for the RC4 encryption algorithm type. You will not be able to choose the RC4 encryption algorithm option when you configure the envelope settings for an encryption profile.

New Alert to notify expiry of Appliance and Custom CA Certificates	When an appliance certificate or a custom CA certificate is going to expire or has expired, the appliance now sends a system alert with a critical or warning severity.
SSL Configuration Changes	The following are the new changes made to SSL configuration settings: • There is no support for SSLv2 and SSL v3 methods. • There is no support for the TLS v1.0 method if your appliance is in the FIPS mode. • The TLS v1.0 method is disabled by default if your appliance is in the non-FIPS mode. • You can enable the TLS v1.0 method for the TLS client services (LDAP and Updater) in any one of the following ways: – System Administration > SSL Configuration page of the web interface of your appliance. See the "System Administration" section in the user guide – `sslconfig` command in the CLI. See the "CLI Reference Guide for AsyncOS 13.5.1 for Cisco Email Security Appliances." **Note** If you plan to upgrade from a lower AsyncOS version (for example, 12.x or 13.0) in non-FIPS mode with TLS v1.0 enabled, to AsyncOS 13.5.1 and later, then TLS v1.0 is disabled by default. You need to enable the TLS v1.0 method on your appliance after upgrade.

Changes in Behavior in AsyncOS 13.5.0

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 analyze the database and take corrective measures.

Changes in Outbreak Filters for Spam Positive Messages	Prior to this release, if a spam positive message is identified as outbreak positive by Outbreak Filters, the message was sent to Outbreak Quarantine. After you upgrade to this release, if a spam positive message is identified as outbreak positive by Outbreak Filters, the message is not sent to Outbreak Quarantine.
Shortened URLs Expansion Changes	Prior to this release, you could disable the expansion of shortened URLs using the `websecurityadvancedconfig` CLI command in your appliance. After you upgrade to this release, all shortened URLs are expanded. There is no option to disable the expansion of shortened URLs.

Upgrade Paths

Upgrading to Release 13.5.3-010 - MD (Maintenance Deployment)

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

You can upgrade to release 13.5.3-010 from the following versions:

- 11.0.4-003
- 11.1.1-108
- 12.5.0-066
- 12.5.1-037
- 12.5.2-011
- 13.0.0-392
- 13.0.0-403
- 13.0.1-030
- 13.5.0-263
- 13.5.1-277
- 13.5.1-352
- 13.5.2-015
- 13.5.2-036

Upgrading to Release 13.5.2-036 - MD (Maintenance Deployment)

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

You can upgrade to release 13.5.2-036 from the following versions:

- 11.1.1-108
- 12.5.0-066
- 12.5.1-037
- 12.5.2-011
- 13.0.0-392
- 13.0.0-403
- 13.0.1-030
- 13.5.0-263
- 13.5.1-277
- 13.5.1-352
- 13.5.2-015

Upgrading to Release 13.5.1-277 - GD (General Deployment)

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

You can upgrade to release 13.5.1-277 from the following versions:

- 12.0.0-419
- 12.1.0-089
- 12.5.0-066
- 12.5.1-037
- 12.5.2-011
- 13.0.0-392
- 13.0.0-403
- 13.0.1-030
- 13.5.0-263
- 13.5.1-177
- 13.5.1-269
- 13.5.1-273

Upgrading to Release 13.5.1-273 - LD (Limited Deployment)

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

You can upgrade to release 13.5.1-273 from the following versions:

- 12.0.0-419
- 12.1.0-089
- 12.5.0-066
- 12.5.1-037
- 12.5.2-011
- 13.0.0-392
- 13.0.0-403
- 13.0.1-030
- 13.5.0-263
- 13.5.1-177
- 13.5.1-269

Upgrading to Release 13.5.0-263 - LD (Limited Deployment)

You can upgrade to release 13.5.0-263 from the following versions:

- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-037
- 13.0.0-314
- 13.0.0-375
- 13.0.0-392
- 13.5.0-236

Installation and Upgrade Notes

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

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

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

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - C190
  - C195
  - C390
  - C395
  - C690
  - C695
  - C695F

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

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

The following hardware is NOT supported for this release:

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

Deploying or Upgrading a Virtual Appliance

If you are deploying or upgrading a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

Upgrading a Virtual Appliance

If your current Virtual Appliance release does not support more than 2TB of disk space, and you want to use more than 2 TB of disk space with this release, you cannot simply upgrade your virtual appliance.

Instead, you must deploy a new virtual machine instance for this release.

When you upgrade a virtual appliance, the existing licenses remain unchanged.

Migrating from a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance with this AsyncOS release using the documentation described in Deploying or Upgrading a Virtual Appliance, page 15.

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 23, below.

Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances

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

Pre-upgrade Notes

Before upgrading, review the following:

- Firewall Settings to Access Cisco Talos Services, page 16
- Firewall Settings to Access Cisco Advanced Phishing Protection Cloud Service, page 17
- Enabling Service Logs on Appliance, page 17
- Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels, page 18
- FIPS Compliance, page 18
- Reverting to Previous AsyncOS Versions, page 18
- 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 19

Firewall Settings to Access Cisco Talos Services

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

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

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

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

Firewall Settings to Access Cisco Advanced Phishing Protection Cloud Service

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

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

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

Enabling Service Logs on Appliance

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

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

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

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

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

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

Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels

Before you upgrade to AsyncOS 13.5.3, ensure that the Intelligent Multi-Scan and Graymail configurations are at the same cluster level. If not, you must review the Intelligent Multi-Scan and Graymail settings after the upgrade.

FIPS Compliance

AsyncOS 13.5.3 release is not a FIPS compliant release. If you have enabled FIPS mode on your appliance, you must disable it before upgrading to AsyncOS 13.5.3.

Reverting to Previous AsyncOS Versions

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

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

Upgrading Deployments with Centralized Management (Clustered Appliances)

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

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

Upgrading From a Release Other Than the Immediate Previous Release

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

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

Configuration Files

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

IPMI Messages During Upgrade

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

Defect ID: CSCuz28415

Upgrading to This Release

Before You Begin

- Clear all the messages in your workqueue. You cannot perform the upgrade without clearing your work queue.
- Review the Known Issues, page 8 and Installation and Upgrade Notes, page 14.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 15.

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.
- If you have changed the SSH key, re-authenticate the connectivity between the Cisco Email Security appliance and the Cisco Security Management appliance after the upgrade.

Post-Upgrade Notes

- Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 13.x, page 20
- Intelligent Multi-Scan and Graymail Global Configuration Changes, page 20

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

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

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

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

Intelligent Multi-Scan and Graymail Global Configuration Changes

The following are the changes to the global settings configuration for Intelligent Multi-Scan (IMS) and Graymail after you upgrade to AsyncOS 13.5.3:

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

Performance Advisory

Outbreak Filters

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

IronPort Spam Quarantine

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

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

Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

- Bug Search Tool Requirements, page 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 13.5.3, page 21
- Known and Fixed Issues for 13.5.2, page 21
- Known and Fixed Issues for 13.5.1, page 22
- Known and Fixed Issues for 13.5.0, page 22

Known and Fixed Issues for 13.5.3

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.5.3&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.5.3-010&prdNam=Cisco%20Secure%20Email%20Gateway

Known and Fixed Issues for 13.5.2

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.5.2&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.5.2-036&prdNam=Cisco%20Secure%20Email%20Gateway

Known and Fixed Issues for 13.5.1

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.5.1&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.5.1-277&prdNam=Cisco%20Secure%20Email%20Gateway

Known and Fixed Issues for 13.5.0

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.5.0&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.5.0-263&prdNam=Cisco%20Secure%20Email%20Gateway

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 Secure Email Gateway**, and click **OK**.

Step 4 In Releases field, enter the version of the release, for example, 13.5.3

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.

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 Secure Email and Web Manager	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email Gateway	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 Secure Email Encryption Service	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.

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.