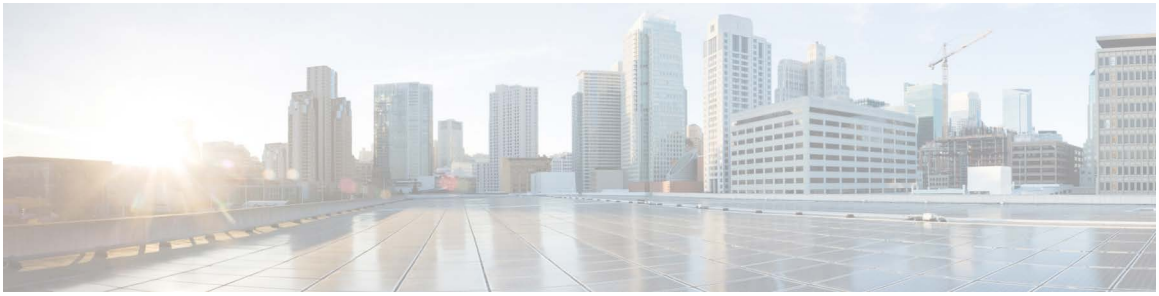

Release Notes for AsyncOS 15.0 for Cisco Secure Email Gateway - GD (General Deployment)

Published: August 10, 2023

Revised: November 14, 2023

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Improved Efficacy to Detect Threats	Your email gateway is now more secure with: • Improved HTML parsing and malicious script detection • Improved URL parsing and redirection detection Perform the following configuration steps to use this feature: 1. Enable the **Graymail** service engine globally on your email gateway in any one of the following ways: **Web Interface**: Navigate to *Security Services* > *IMS and Graymail* page and select the **Graymail Detection** checkbox under *Graymail Global Settings* **CLI:** Use the `graymail` > `setup` sub command and type **yes** for the "`Would you like to use Graymail Detection? [Y]>`" statement 2. Enable the **Anti-spam service** engine for the required incoming mail policy as follows: a. Navigate to **Mail Policies** > **Incoming Mail Policie**s page on the web interface. b. Click the **Disabled** link under 'Anti-Spam' in the 'Policies' field. c. Select the **Use IronPort Anti-Spam service** or **Use IronPort Intelligent Multi-Scan** option buttons, whichever is applicable, to enable Anti-Spam scanning for the mail policy. d. Select the required action - 'deliver,' 'drop,' 'spam quarantine,' or 'bounce,' whichever is applicable, to apply to positively identified spam messages. e. [Optional]: Perform any other required Anti-Spam configuration settings. f. Click **Submit** and commit your changes. A new verdict - **ThreatScanner Spam Positive** is added in Message Tracking and Mail Logs to indicate that the message is categorized as "spam" due to improved threat detection. The recommended Anti-Spam policy action for **ThreatScanner Spam Positive** verdict is **Quarantine**. The **Graymail** logs with Spamcause data are available at **Information** log levels.

Enforcing TLS for Outgoing Messages at Sender or Recipient Level	The existing Destination Controls configuration allows you to override the TLS modes (such as TLS Mandatory, TLS Preferred, and so on) on a per-domain basis. If you need to enforce TLS for outgoing messages based on additional conditions such as – senders, recipients, and so on, you can now use the `X-ESA-CF-TLS-Mandatory` header. You can configure the "Content Filter – Add/Edit Header" action to add the `X-ESA-CF-TLS-Mandatory` header in the "Header Name:" field based on any content filter conditions and attach the content filter to an outgoing mail policy.
URL Retrospective Verdict and URL Remediation	The URLs with unknown reputation can turn malicious anytime, even after it has reached the user's mailbox. You can configure URL filtering on your email gateway to send alerts based on the URL retrospective verdicts received from Talos. You can also configure your email gateway to perform auto-remedial actions on the messages in user mailbox when the URL verdict changes from unknown to malicious. For more information, see the "Protecting Against Malicious or Undesirable URLs" chapter in the user guide associated with this release.
Integrating Secure Email Gateway with Threat Defense	The Threat Defense Connector client connects the Secure Email Gateway with the Secure Email Threat Defense to scan messages for Advanced Phishing and Spoofing. When you configure the Threat Defense Connector, the Secure Email Gateway sends a copy of the actual message as an attachment to the Threat Defense portal's message intake address. The message gets delivered to the user inbox, and advanced scanning completes in the Threat Defense portal. You can enable the Threat Defense Connector in any of the following ways: • From the **Security Services** > **Threat Defense Connector** page of the web interface. • Using the `threatdefenseconfig` command in the CLI. For more information, see the "Integrating Secure Email Gateway with Threat Defense" chapter in the user guide or the CLI Reference Guide associated with this release.

Customizing Graymail Unsubscribe Banner	You can customize the following settings of the Graymail Unsubscribe banner based on your organization's requirements: • Position of the banner • Color of the banner • Text color of the banner message • Contents of the banner message The banner message supports the following languages: English (United States), Italian, Chinese, Portuguese, Spanish, German, French, Russian, Japanese, Korean, and Chinese (Taiwan). **Note** There is no CLI support for the feature in this release. For more information, see the "Customizing Graymail Unsubscribe Banner based on Organizational Requirements" section in the "Managing Spam and Graymail" chapter of the user guide associated with this release.
File Reputation Service Enhancement	From AsyncOS 15.x release onwards, the email gateway uses a new version of the AMP engine. This new AMP engine uses HTTPS (port 443) instead of TCP to ensure secure communication between your email gateway and Secure Endpoint Cloud. **Note** [For Secure Endpoint Private Cloud users only]: Before you upgrade to this release, make sure you have met all the prerequisites for the new File Reputation service activation. For more information, see the Deleting Encryption Notification Templates sub-section under the "Pre-Upgrade Note" section of this document. **Note** [For Secure Endpoint Private Cloud users only] If you skipped the instructions on File Reputation service activation during the upgrade, see the Mandatory Usage of Cisco Smart Software Licensing in Next AsyncOS Release sub-section under the "Post-Upgrade Notes' section of this document on how to activate the File Reputation Service after the upgrade. For more information, see the "File Reputation Filtering and File Analysis" chapter of the user guide associated with this release.

Obtaining Configuration Information using AsyncOS APIs	You can use the Configuration APIs to perform various operations (such as create, retrieve, update, and delete) in your email gateway. The various API categories for configuration are: • Authentication APIs • URL Lists APIs • Dictionary APIs • Host Access Table (HAT) APIs **Note** For Configuration APIs, the administrator and cloud administrator user roles are only supported. **Note** For Configuration APIs: - If you modify any of the APIs in the cluster mode, the changes apply to all the other machines in the cluster. - If you modify any of the APIs in the group mode, the changes apply to all the other machines in the group. - If you modify any of the APIs in the machine mode, the changes only apply to the specified machine. For more information, see the "Configuration APIs" section in the *AsyncOS 15.0 API for Cisco Secure Email Gateway - Getting Started Guide*.

Removal of Old Splunk Database for Email Tracking Data	When you upgrade to Secure Email Gateway 15.0 and later, and if the email tracking data is contained in the Splunk database, the system deletes the Splunk database if you proceed with the upgrade. During the upgrade, a warning message indicating that the system will delete the Splunk database is displayed in the CLI or the web interface of your email gateway. Following is a sample warning message displayed at the time of the upgrade: `"From Secure Email Gateway 12.1.x version onwards, we have moved to a newer storage system for email tracking data. Generally, the old data is replaced with new data in the new storage system automatically. However, in some scenarios (for example, 'late upgrades', 'low mail flow' and 'tracking data', and so on), there could be traces of old data still present in the old storage system that is no longer supported.` `In your case it is, 7.1 MB, which was last updated in 01 Jul 2022.` `If you proceed with this upgrade process, the data in the old storage will be removed.` `You can choose to proceed with the upgrade or abort the upgrade.` `Do you want to proceed with the upgrade?[Y]"` **Note** The `debug` sub menu used to collect debug information for the Splunk database is removed from the `Diagnostic` > `Tracking` sub command in the CLI.
Deleting Log Files from Email Gateway	You can now delete log files stored in the /data/pub/directories path of your email gateway. You can use the `logconfig` > `deletelogfile` sub command in the CLI to delete the log files. **Note** If your email gateway is in a cluster, the `deletelogfile` sub command is a machine level option. For more information, see the "Example- Deleting Log Files" section of the CLI Reference Guide associated with this release.
FIPS Certification	Cisco Secure Email Gateway is FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #4036). For more information, see the "FIPS Management" chapter of the user guide associated with this release.

Generation 2 Deployment Support for Hyper-V Models	From AsyncOS 15.0 release onwards, Secure Email Gateway supports Generation 2 deployment for Hyper-V models. **Note** The supported model for Hyper-V Generation 2 deployment is **C600V** only. **Note** Currently, there is no support for "Secure Boot" and "Trusted Platform Module (TPM)" technologies in Generation 2 deployment. For more information, see the *Cisco Content Security Virtual Appliance Installation Guide* from https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html
Microsoft Hyper-V Server 2019 Support	Secure Email Gateway 15.0 supports Microsoft Hyper-V Server 2019. For more information, see the *Cisco Content Security Virtual Appliance Installation Guide* from https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html
Supported Model for AWS Deployment	From AsyncOS 15.0 release onwards, the supported model for AWS deployment is C600V only. For more information, see the *Cisco Content Security Virtual Appliances on AWS EC2 Installation Guide* from https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html
Generation 2 Deployment Support for Azure	From AsyncOS 15.0 release onwards, Secure Email Gateway supports Generation 2 deployment for Azure. **Note** The supported model for Azure Generation 2 deployment is **C600V** only. **Note** The Generation 2 Image does not boot after you deploy it on the Azure platform. You must reboot the virtual machine after you deploy the Generation 2 image. For more information, see the *Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual on Azure Deployment Guide* from https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html

New RAM Values for Secure Email Gateway Virtual Appliance Models	From AsyncOS 15.0 release onwards, there are new RAM values for the following Secure Email Gateway virtual appliance models deployed through KVM or VMWare ESXi: • C100V • C300V • C600V For details on the new RAM values applicable for each virtual appliance model, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html
New Note for Removal of Weak Algorithms during System Upgrade	[Applicable to FIPS and non-FIPS modes]: During the system upgrade to AsyncOS 15.0 and later, a new Note statement is added to inform you that the system removes all weak algorithms in Ciphers, Keys, KEX, and MAC (if configured) after the upgrade process.

New DLP Policy Pre-defined Classifiers	The following new DLP policy pre-defined classifiers are added in the Mail Policies > DLP Policy Manager > Add DLP Policy > Custom Policy > Add > Policy Matching Details page of your web interface: • Bank Account Numbers (Austria IBAN) • Bank Account Numbers (Belgium IBAN) • Bank Account Numbers (Bulgaria IBAN) • Bank Account Numbers (Croatia IBAN) • Bank Account Numbers (Cyprus IBAN) • Bank Account Numbers (Czech Republic IBAN) • Bank Account Numbers (Denmark IBAN) • Bank Account Numbers (Estonia IBAN) • Bank Account Numbers (Finland IBAN) • Bank Account Numbers (Greece IBAN) • Bank Account Numbers (Hungary IBAN) • Bank Account Numbers (Ireland IBAN) • Bank Account Numbers (Latvia IBAN) • Bank Account Numbers (Lithuania IBAN) • Bank Account Numbers (Luxembourg IBAN) • Bank Account Numbers (Malta IBAN) • Bank Account Numbers (Poland IBAN) • Bank Account Numbers (Portugal IBAN) • Bank Account Numbers (Romania IBAN) • Bank Account Numbers (Slovakia IBAN) • Bank Account Numbers (Slovenia IBAN) • Bank Account Numbers (Spain IBAN) • Cambodia National ID • Cyprus National ID • Finland National ID • Malta National ID • Myanmar National ID • Portugal National ID • Vietnam National ID
ECDSA Certificates Support for SSL Communication	You can now use the Elliptic Curve Digital Signature Algorithm (ECDSA) certificates that allow the combination of Elliptic Curve Diffie Hellman Ephemeral (ECDHE) algorithm for Key Exchange and ECDSA authentication to configure the following SSL services: • GUI HTTPS • Inbound SMTP

Changes in Behavior

Sender Domain Reputation Filtering - Domain Exception List Changes	[Before this Release]: When you disabled the "Match Domain Exception List based on Domain in Envelope From:" option, the message is matched against the Domain Exception list, only if the domains in the "Envelope From:," "From:," and "Reply-To:" headers of the message are the same and in the Domain Exception List. [From this Release onwards]: When you disable the "Match Domain Exception List based on Domain in Envelope From:" option, the message is matched against the Domain Exception list, even if the domains in the "Envelope From:," "From:," and "Reply-To:" headers of the message are different and any of the domains in the "HELO:," "RDNS:," "Envelope From:," "From:," and "Reply-To:" are in the Domain Exception List
New condition to categorize messages as Unscannable due to RFC violation	[Before this Release]: When a MIME part of the message contained more than one "Content-Transfer-Encoding" header, the content scanner would not categorize the message as "Unscannable" due to an RFC violation. [From this Release onwards]: When a MIME part contains more than one "Content-Transfer-Encoding" header, the content scanner categorizes the message as "Unscannable" due to an RFC violation. The action configured under “Security Services > Scan Behavior > Action when a message is unscannable due to RFC violations" is applied to the message.
Syslog Message Changes	[Before this Release]: A Syslog message would display the configured IP address of the email gateway. [From this Release onwards]: The Syslog message does not display the IP address but now shows the configured FQDN or host name of the email gateway.

[Upgrade Scenario]: SSH Server and Client Configuration Changes	The following SSH Server and Client Configuration changes are applicable when you upgrade your email gateway from a lower AsyncOS version to AsyncOS 15.0 version and later. [**For Non-FIPS mode only**]: Following are the SSH Server and Client Configuration changes applicable when your email gateway is not in the FIPS mode: [**SSH Server Configuration Changes**]: • The following cipher algorithms, MAC methods, KEX algorithms, and host key algorithm are removed from your email gateway by default: – **Cipher algorithms** - `3des-cbc` and `rijndael-cbc@lysator.liu.se` – **MAC methods** - `hmac-md5`, `umac-64@openssh.com`,`hmac-ripemd160`, `hmac-ripemd160@openssh.com`, `hmac-sha1-96`, and `hmac-md5-96` – **KEX algorithms** - `diffie-hellman-group-exchange-sha256` and `diffie-hellman-group-exchange-sha1` – **Host key algorithm** - `rsa1` • The "Minimum **Server Key**" option is removed from the CLI of your email gateway by default. • The host key algorithm - `rsa-sha2-256` is added to your email gateway by default. [**SSH Client Configuration Changes**]: • The following cipher algorithms - `arcfour256` and `arcfour128` are removed from your email gateway by default. • The host key algorithm - `rsa-sha2-256` is added to your email gateway by default.

[Upgrade Scenario]: SSH Server and Client Configuration Changes (contd.)	[**For FIPS Mode only**]: Following are the SSH Server and Client Configuration changes applicable when your email gateway is in the FIPS mode: [**SSH Server Configuration Changes**]: • The following cipher algorithm, KEX algorithms, and host key algorithm are non-FIPS compliant and removed from your email gateway. – **Cipher algorithms** - `3des-cbc` – **KEX algorithms** - `diffie-hellman-group-exchange-sha256` and `diffie-hellman-group-exchange-sha1` – **Host key algorithm** - `ssh-rsa` • The "Minimum Server Key Size" option is removed from the CLI of your email gateway because it is non-FIPS compliant. • The host key algorithm - `rsa-sha2-256` is added to your email gateway by default. • The host key algorithm - `ssh-dss` is removed from your email gateway by default (if configured using the `logconfig` > `hostkeyconfig` sub command in the CLI). [**SSH Client Configuration Changes**]: • The Cipher algorithm - `3des-cbc` is non-FIPS compliant and removed from your email gateway. • The host key algorithm - `rsa-sha2-256` is added to your email gateway by default.

[New Install Scenario]: SSH Server Configuration Changes	The following SSH server configuration changes are only applicable when you install AsyncOS 15.0 for Cisco Secure Email Gateway for the first time. [F**or non-FIPS mode only**]: The following cipher algorithms, MAC method, KEX algorithms, and host key algorithms are supported in your email gateway: • **Cipher algorithms** - `aes128-ctr`, `aes192-ctr`, `aes256-ctr`, `aes128-cbc`, `aes192-cbc`, and `aes256-cbc` • **MAC method** - `hmac-sha1` • **KEX algorithms** - `diffie-hellman-group14-sha1`, `ecdh-sha2-nistp256`, `ecdh- sha2-nistp384`, and `ecdh-sha2-nistp521` • **Host key algorithms** - `rsa-sha2-256`, `ssh-rsa`, and `ssh-dss` (disabled by default) **Note** You need to manually enable the "`ssh-dss`" cipher algorithm using the `shconfig` > `sshd` > `setup` sub command in the CLI. --- [**For FIPS mode only**]: To enable FIPS mode, make sure you first disable the following cipher algorithm and host key algorithm that are non-FIPS compliant using the `sshconfig` > `sshd` > `setup` sub command in the CLI. • **Cipher algorithm** - `aes192-ctr` • **Host key algorithm** - `ssh-rsa` **Note** The host key algorithm - `rsa-sha2-256` is newly added and is enabled by default on your email gateway.
SPF Email Verification Changes	[Before this Release]: The email gateway would perform the Sender Policy Framework (SPF) email verification process based on the SPF and TXT records per the RFC 4408 (Section 4.4) standard. [From this Release onwards]: The email gateway performs the SPF email verification process based on only the TXT records per the new RFC 7208 (Section 4.4) standard.
Changes to CEF Field Names for Consolidated Event Logs	From this release onwards, the following Common Event Format (CEF) field names are changed for the Consolidated Event logs: • '`endTime`' to '`end`' • '`startTime`' to '`start`' • '`sourceAddress`' to '`src`' • '`sourceHostName`' to '`shost`'

Changes in uploading HTML and Octet-stream Files for File Analysis	[Before this release]: The email gateway could only upload HTML and Octet-stream files (mime type - application/octet-stream and text/html) to the File Analysis server if the file extensions were selected for file analysis. [From this release onwards]: The email gateway can now upload the HTML and Octet-stream files to the File Analysis server for file analysis, even if the file extensions are not selected for file analysis. **Note** As the number of files uploaded to the File Analysis server may increase, the email gateway could potentially reach the file upload limit of the file analysis server quickly.
Changes in uploading Archived Files for File Analysis	[Before this release]: When the AMP engine failed to extract the archive files (including password-protected archived attachments) from a message, the attachments would not be uploaded to the File Analysis server. [From this release onwards]: When the AMP engine fails to extract the archive files (including password-protected archived attachments) from a message, the attachments are now uploaded to the File Analysis server for file analysis. **Note** As the number of files uploaded to the File Analysis server may increase, the email gateway could potentially reach the file upload limit of the file analysis server quickly.
Default Threshold Value Change for Message Scanning	[Before this release]: The default threshold value for the Intelligent-Multi Scan (IMS) and Graymail engines to never scan messages was set to 1 M. [From this release onwards]: The default threshold value for the Intelligent-Multi Scan (IMS) and Graymail engines to never scan messages is set to 2 M.
Support for importing ECDSA and EDDSA certificates	From this release onwards, support for the x509 certificates with ECDSA and EDDSA algorithms is introduced.
Cipher configuration changes	Non-compliant/weak TLS cipher suites are now disabled on Inbound SMTP, Outbound SMTP, GUI, LDAP and updater by default. Non-compliant CSDL Key SSH algorithms like `ssh-dss` is now disabled on SSH server by default but allowed to be configured.
Support to choose the signature algorithm while creating self-signed certificates	From this release onwards, you can choose the signature algorithm (sha256withRSAEncryption, sha384withRSAEncryption, or sha512withRSAEncryption) while generating self-signed/self-signed SMIME certificates in both CLI & GUI.

Changes in signature algorithms for x509 certificates	The following signature algorithms for peer certificates in TLS services Inbound SMTP, Smart Licensing transport URL server, Enrollment Client , SSE server, Talos client, Syslog server, ECS client, and Cisco Security Awareness cloud server) are not supported: `'sha1withrsaencryption', 'sha224withrsaencryption', 'dsawithsha1', 'ecdsa-with-sha1', 'ecsda-with-sha224', 'md2withrsaencryption', 'md4withrsaencryption', 'md5withrsaencryption', 'ripemd128withrsaencryption', 'ripemd160withrsaencryption', 'ripemd256withrsaencryption', 'ripemd128withrsa', 'ripemd160withrsa', 'ripemd256withrsa'` The following curves for peer certificates with the ECDSA signature algorithm in TLS services ( Inbound SMTP, Smart Licensing transport URL server, Enrollment Client , SSE server, Talos client, Syslog server, ECS , and Cisco Security Awareness cloud server) are not supported: `'secp224r1', 'secp192r1', 'brainpoolP160r1', 'brainpoolP192r1', 'secp160r1', 'secp160r2', 'prime192v1', 'secp192k1', 'secp224k1', 'secp256k1', 'sect163k1', 'sect163r2', 'sect193r1', 'sect193r2', 'sect233k1', 'sect233r1', 'sect239k1', 'sect283k1', 'sect283r1', 'sect409k1', 'sect409r1', 'sect571k1', 'sect571r1'`
Expiry of Remote Access Account	From this release onwards, a remote access account created using the `techsupport > sshaccess` command remains active for 7 days. After that, you need to re-enable the remote access. The option to enter a random seed string for remote access is removed in the web interface and the CLI.

Upgrade Paths

Upgrading to Release 15.0.0-104 - GD (General Deployment)

You can upgrade to release 15.0.0-104 from the following versions:

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004

- 14.3.0-023
- 14.3.0-032
- 15.0.0-097

Upgrading to Release 15.0.0-097 - LD (Limited Deployment) Refresh

You can upgrade to release 15.0.0-097 from the following versions:

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004
- 14.3.0-023
- 14.3.0-032
- 15.0.0-012
- 15.0.0-048
- 15.0.0-068
- 15.0.0-085

Upgrading to Release 15.0.0-068 - LD (Limited Deployment)

You can upgrade to release 15.0.0-068 from the following versions:

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004
- 14.3.0-023

- 14.3.0-032
- 15.0.0-012
- 15.0.0-048

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 email gateway 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 email gateway.

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

When you upgrade a virtual email gateway, 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 18.

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 28, 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:

Upgrading Email Gateway from AsynOS 15.0.0-xxx to AsynOS 15.0.0-104 GD

When you upgrade your email gateway from AsynOS 15.0.0-xxx to AsynOS 15.0.0-104 GD release, and if you recieve an alert indicating "**Vault error**", contact Cisco TAC.

This is a known issue. Defect ID: CSCwh15269.

Deleting Encryption Notification Templates

When you upgrade your email gateway to AsyncOS 15.0.x, the system automatically removes any existing Encryption Notification Templates (HTML or text formats) that are detected to contain “unsupported formats” during the upgrade.

Prerequisites for File Reputation Service Activation - Secure Endpoint Private Cloud

Before you upgrade to this release, make sure you have met the following prerequisites for File Reputation service activation:

- Upgraded the Secure Endpoint Private Cloud to 3.8.1 or higher version
- Provided the Secure Endpoint - “Console Hostname” and “Activation Code” details when prompted during the upgrade process.

Features Configurable using IDN Domains in Email Gateway

Prerequisites:

Make sure you have met the following prerequisites before you use the Internationalized Domain Names (IDN) feature:

- All incoming messages must have IDNs encoded in UTF-8.
  For Example: An MTA that sends messages to the email gateway must support IDNs and make sure the domains in the messages are in the UTF-8 format.
- All outgoing messages must have IDNs encoded in UTF-8, and the destination server must accept and support IDNs accordingly.
  For Example: An MTA that accepts messages from the email gateway must support IDNs and domains encoded in the UTF-8 format.
- In all applicable DNS records, IDNs must be configured using the Punycode format.
  For Example: When you configure an MX record for an IDN, the domain in the DNS record must be in the Punycode format.

For this release, you can **only** configure the following features using IDN domains in your email gateway:

- **SMTP Routes Configuration Settings**:
  - Add or edit IDN domains.
  - Export or import SMTP routes using IDN domains.
- **DNS Configuration Settings**: Add or edit the DNS server using IDN domains.
- **Listener Configuration Settings:**
  - Add or edit IDN domains for the default domain in inbound or outbound listeners.
  - Add or edit IDN domains in the HAT or RAT tables.
  - Export or import HAT or RAT tables using IDN domains.
- **Mail Policies Configuration Settings**:
  - Add or edit domains using IDN domains for senders (’Following Senders’ or ’Following Senders are not’options) and recipients (’Following Recipients’ or ’Recipients are not’options) in Incoming Mail Policies.
  - Add or edit domains using IDN domains for senders (’Following Senders’ or ’Following Senders are not’options) and recipients (’Following Recipients’ or ’Recipients are not’options) in Outgoing Mail Policies.
  - Find senders or recipients using IDN domains in Incoming or Outgoing Mail Policies
  - Define Sender Verification Exception table using IDN domains.
  - Create an address list using IDN domains.
  - Add or edit the destination domain using IDN domains for destination controls.
- **Bounce Profiles Configuration Settings** - Add or edit the alternate email address using IDN domains.
- **Sender Domain Reputation Configuration Settings**: Define sender domain reputation scores for IDN domains.
- **IP Reputation Configuration Settings**: Define IP reputation scores for IDN domains.
- **LDAP Configuration Settings**: Create LDAP group queries, accept queries, routing queries, and masquerade queries for incoming and outgoing messages using IDN domains.
- **Reporting Configuration Settings:** View IDN data - usernames, email addresses, and domains) in the reports.
- **Message Tracking Configuration Settings**: View IDN data- usernames, email addresses, and domains) in message tracking.
- **Policy, Virus, and Outbreak Quarantine Configuration Settings:**

  - View messages with IDN domains that may be transmitting malware, as determined by the anti-virus engine.
  - View messages with IDN domains caught by Outbreak Filters as potentially being spam or malware.
  - View messages with IDN domains caught by message filters, content filters, and DLP message actions.
- **Spam Quarantine Configuration Settings**:
  - View messages with IDN domains detected as spam or suspected spam.
  - Add email addresses with IDN domains to the safelist and blocklist categories.

Note Currently, recipients with IDN domains can access the End-User Quarantine only if the end-user authentication method is set to 'None' under the 'End-User Quarantine Access' section in the 'Spam Quarantine' settings page.

- **SPF Configuration Settings**: Perform SPF verification of messages using IDN domains.
- **DKIM Configuration Settings**: Perform DKIM signing and verification of messages using IDN domains.
- **DMARC Configuration Settings**: Perform DMARC verification of messages using IDN domains.

New Categories and New Names for Existing URL Reputation Verdicts

The following table details the new categories and new names for the existing URL Reputation verdicts in your email gateway:

Current URL Reputation Verdict Name	New Cisco Talos URL Reputation Verdict Name	Score Range	Description
Clean	Trusted	+6.0 to +10.0	Displays a behavior that indicates exceptional safety.
Neutral	Favorable	+0.1 to +5.9	Displays a behavior that indicates a level of safety.
	Neutral	-3.0 to 0.0	Does not display a positive or negative behavior. However, this verdict has been evaluated.
	Questionable	-5.9 to -3.1	Displays a behavior that may indicate risk, or undesirable.
Malicious	Untrusted	-10.0 to -6.0	Displays a behavior that is exceptionally bad, malicious, or undesirable.
No Score	Unknown	No score	The verdict has not been previously evaluated or lacks the capability to assert a threat level verdict.

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 Email Gateway

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.

Cisco Secure Email 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 email gateway 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 15.0, 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 15.0 Release is FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #4036).

Upgrading Deployments with Centralized Management (Clustered Appliances)

If a cluster includes C380 or C680 hardware appliances, remove these appliances from the cluster before upgrading.

All machines in a cluster must be running the same version of AsyncOS, and x80 hardware cannot be upgraded to this release. If necessary, create a separate cluster for your 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 email gateway 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 (Known and Fixed Issues, page 26) and Installation and Upgrade Notes, page 17.
- If you are upgrading a virtual email gateway, see Upgrading a Virtual Appliance, page 18.

Procedure

Use the following instructions to upgrade your email gateway:

Step 1 Save the XML configuration file off the email gateway.

Step 2 If you are using the Safelist/Blocklist feature, export the Safelist/Blocklist database off the email gateway.

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 email gateway.

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 26.
- If you have changed the SSH key, re-authenticate the connectivity between the email gateway and Cisco Secure Email and Web Manager after the upgrade.

Post-Upgrade Notes

Mandatory Usage of Cisco Smart Software Licensing in Next AsyncOS Release

The Cisco Smart Software Licensing usage is mandatory from the next AsyncOS release (all releases post AsyncOS 15.0 release) for Cisco Secure Email Gateway.

Note There will be **no support** for classic licensing from the next AsyncOS release. You will no longer be able to order new feature licenses or renew existing feature licenses in the Classic Licensing mode.

Prerequisite: Make sure you create a smart account in the Cisco Smart Software Manager portal and enable Cisco Smart Software Licensing on your email gateway. For more information, see the "Smart Software Licensing" section of the "System Administration" chapter of the user guide.

Result: After you enable Cisco Smart Software Licensing, you can upgrade your email gateway from AsyncOS 15.0 to the next AsyncOS release seamlessly and continue to use the existing feature licenses in the Smart Licensing mode.

Activating File Reputation Service for Secure Endpoint Private Cloud

Follow any one of the given steps based on your system setup to activate the File Reputation Service:

- [**For Cluster mode**]: Connect to the email gateway that is already configured with the new File Reputation service.
- [**For Standalone mode**]: Perform the following steps:

  1. Navigate to the **Security Services** > **File Reputation and Analysis** page on the web interface,
  2. Click the **Edit Global Settings** button.
  3. Click the **Advanced Settings for File Reputation** panel,
  4. Select the **Private reputation cloud** option from the "File Reputation Server" drop-down list.
  5. Enter the console hostname and activation code in the given fields.
  6. Click **Submit** and commit your changes.

DLP Service Status Check

After you upgrade to this release, you might experience an issue with the DLP service.

Solution: Check the status of the DLP service on your email gateway using the `diagnostic` > `services` > `DLP` > `status` sub command in the CLI. If the DLP service is not running, refer to the 'Workarounds' section of the CSCvy08110 defect available in the Known Issues list. For more information on how to view the Known Issues, see Lists of Known and Fixed Issues, page 27.

Scanning Password-Protected Attachments in Email Gateway

When you configure the Content Scanner in your email gateway to scan the password-protected attachments, there may be a performance impact if your email traffic contains a high percentage of password-protected attachments.

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 15.0:

- If the global settings of IMS and Graymail are configured at different cluster levels, the email gateway 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 email gateway copies the IMS global settings to the machine level.

- If the maximum message size and timeout values for scanning messages are different, the email gateway 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 email gateways 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 want 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 26
- Lists of Known and Fixed Issues, page 27
- Related Documentation, page 27

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?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=15.0.0&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.0.0-104&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, 15.0

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 Web Security	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

Documentation For Cisco Content Security Products	Location
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 email gateway. For instructions, see the User Guide or online help.