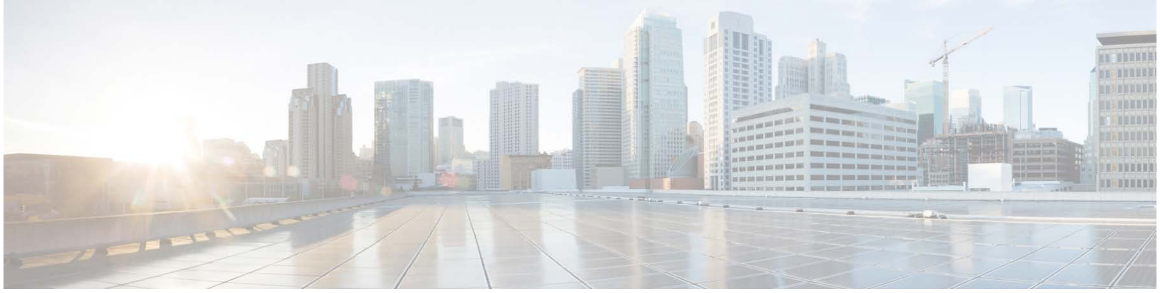

Release Notes for AsyncOS 15.0.1 for Cisco Secure Email Cloud Gateway - MD (Maintenance Deployment)

Published: November 30, 2023

Revised: February 13, 2024

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

What's New in AsyncOS 15.0.1

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 18.

What's New in AsyncOS 15.0

Feature	Description
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.
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.

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.

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 Prerequisites for File Reputation Service Activation - Secure Endpoint Private Cloud 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 Executing Vault Recovery Script to Resolve Vault Issues 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.
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.
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.

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. **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.
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 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

Change in Behavior

Changes in Behavior in AsyncOS 15.0.1

Deleting Bounce Profile - New Status Message	From this release onwards, when you delete the bounce profiles, you can view the "**processing**" status message at the top left corner of the **Bounce Profile** page until a delete confirmation message is displayed.
Uploading Archive Files for TG Analysis	Before this release, the archive files that your email gateway failed to extract were uploaded to Threat Grid (TG) for analysis. From this release onwards, the archive files that your email gateway failed to extract are not uploaded to TG for analysis.

Changes in Behavior inAsyncOS 15.0

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', 'ecdsa-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 15.0.1-030 - MD (Maintenance Deployment), page 12
- Upgrading to Release 15.0.0-104 - GD (General Deployment), page 13
- Upgrading to Release 15.0.0-097 - LD (Limited Deployment) Refresh, page 13
- Upgrading to Release 15.0.0-068 - LD (Limited Deployment), page 14

Upgrading to Release 15.0.1-030 - MD (Maintenance Deployment)

You can upgrade to release 15.0.1-030 from the following versions:

- 14.2.1-020
- 14.2.2-004
- 14.2.3-027
- 14.2.3-031
- 14.3.0-032
- 15.0.0-097
- 15.0.0-104

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

Supported VMs for this Release

The following VMs are supported for this release:

- C100V
- C300V
- C600V

Pre-Upgrade Notes

Before upgrading, review the following:

- Upgrading Email Gateway from AsynOS 15.0.0-xxx to AsynOS 15.0.0-104 GD, page 14
- Deleting Encryption Notification Templates, page 15
- Prerequisites for File Reputation Service Activation - Secure Endpoint Private Cloud, page 15

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.

Post-Upgrade Notes

- Executing Vault Recovery Script to Resolve Vault Issues, page 15
- Activating File Reputation Service for Secure Endpoint Private Cloud, page 17
- DLP Service Status Check, page 17
- Scanning Password-Protected Attachments in Email Gateway, page 17
- Intelligent Multi-Scan and Graymail Global Configuration Changes, page 17

Executing Vault Recovery Script to Resolve Vault Issues

If your email gateway (on Hardware, On Premises, CES, AWS, KVM, Azure, or Hyper-V) encounters vault-related issues and if encryption is **disabled**, then you must execute Vault Recovery Script to resolve these issues. Perform the following steps to execute the Vault Recovery Script:

1. Log in to your email gateway through a direct SSH connection using the following credentials:

   username: **enablediag**

   password: **admin user's password**

2. Execute the `recovervault` command.
3. Enter the following sequence of subcommands, when prompted:

   a. `yes`

   b. `encryption disable [2]`

   c. `reboot`

   Your email gateway recovers, and the vault is reinitialized.

   Now, you can connect to the system without any issues, and all the system configuration settings are retained.

If your email gateway (on Hardware,On Premises, CES, AWS, KVM, Azure, or Hyper-V) encounters vault-related issues and if encryption is **enabled**, contact Cisco TAC to resolve them.

Note In this scenario, the following encrypted variables are reset to their default factory values:

- Certificate private keys
- RADIUS passwords
- LDAP bind passwords
- Local users' password hashes
- SNMP password
- DK/DKIM signing keys
- Outgoing SMTP authentication passwords
- PostX encryption keys
- PostX encryption proxy password
- FTP Push log subscriptions' passwords
- IPMI LAN password
- Updater server URLs
- Authentication APIs client credentials
- AMP proxy password
- SAML certificate passphrase

If you want to restore the previous configuration, you must load the previously saved configuration file.

Note The client credentials for the Authentication APIs are not saved in the configuration file and therefore you must create new client credentials by calling the APIs.

Logs (for enablediag user):

```
Available Commands:

help -- View this text.

quit -- Log out.

service -- Enable or disable access to the service system.

network -- Perform emergency configuration of the diagnostic network interface.

clearnet -- Resets configuration of the diagnostic network interface.

ssh -- Configure emergency SSH daemon on the diagnostic network interface.

clearssh -- Stop emergency SSH daemon on the diagnostic network interface.

tunnel -- Start up tech support tunnel to IronPort.

print -- Print status of the diagnostic network interface.

recovervault -- Recover vault, it will only restore the encrypted variables to factory
values, will not touch anything related to configurations if encryption is disabled .

resetappliance -- Reset appliance reverts the appliance to chosen build with factory
default settings with default IP. No network configuration would be preserved.

reboot -- Reboot the appliance.


S/N 42189A47B0D50A645948-CEC55115B364
```

```
Service Access currently ENABLED (0 current service logins)
esa1.hc303-10.smtpi.com> recovervault

Are you sure you want to recover vault?  [N]> y
Encryption is enabled [1]>
Encryption is not enabled [2]>
```

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 18.

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 18
- Lists of Known and Fixed Issues, page 18
- Related Documentation, page 20

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 AsyncOS 15.0.1, page 19
- Known and Fixed Issues for AsyncOS 15.0, page 19

Known and Fixed Issues for AsyncOS 15.0.1

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=15.0.1&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.0.1-030&prdNam=Cisco%20Secure%20Email%20Gateway

Known and Fixed Issues for AsyncOS 15.0

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 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
Cisco Secure Email Cloud Gateway	https://www.cisco.com/c/en/us/support/security/cloud-email-security/products-user-guide-list.html
CLI Reference Guide for Cisco Secure Email Gateway	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 email gateway. For instructions, see the User Guide or online help.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2023-2024 Cisco Systems, Inc. All rights reserved.