# Release Notes for AsyncOS 15.5.1 for Cisco Secure Email Gateway - GD (General Deployment)

**Published: April 30, 2024**

# Contents

# What's New In This Release

| Feature | Description |
|---------|-------------|
| Monitoring Vault Service and Sending Alerts | Your email gateway now monitors the Vault service and keeps track of its status, whether it is initialized or not. It also sends appropriate alert messages and logs status information into error_logs.<br><br>You can access the alert logs using one of the following ways:<br><br>• Navigate to **System Administration** > **Alerts** page on the web interface, and click the **View Top Alerts** button.<br><br>• Use the `displayalerts` command in the CLI.<br><br>If the Vault service fails to initialize due to any issues, you receive alert messages (in the mail, on the web interface, and in the CLI) to indicate that the Vault service is down, and you have to execute the Vault Recovery process to restore the Vault service.<br><br>**Note** If the upgrade fails while upgrading to AsyncOS 15.5.1, then you should check for the Vault service error in upgrade_logs. If a Vault service error is identified, then you must restore the Vault service or proceed with the upgrade process without saving the configuration.<br><br>You will receive alert messages in the following scenarios:<br><br>• If the Vault service fails to initialize after you upgrade to AsyncOS 15.5.1, you receive alert messages through the mail, on the web interface, and in the CLI.<br><br>• If any of the services of your email gateway use the Vault service Vault service that fails to initialize, you receive alert messages through the mail, on the web interface, and in the CLI. The alert messages sent depend on the encryption status. You can check the encryption status using the `fipsconfig` > `encryptconfig` subcommand.<br><br>The Vault monitoring mechanism checks the Vault service every 75 minutes. If it is down, then it sends alert messages until the Vault service is restored.<br><br>For information on an example of a successful vault health check and initialization log entry, see "Successful Vault Health Check and Initialization" section in "Logging" chapter of *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |

| | |
|---|---|
| | To restore the Vault service, you have to execute the Vault Recovery process. |
| | ⚠️ **Caution** If the encryption (CLI > `fipsconfig` > `encryptconfig`) is enabled, ensure that you always save and keep a copy of email gateway's configuration to avoid data loss. |
| | For more information on how to save the email gateway's configuration, see Saving Email Gateway's Configuration, page 11. |
| | For information on how to execute the Vault Recovery process, see Executing Vault Recovery Process to Resolve Vault Issues, page 11. |
| Identifying Messages that Violate End-Of-Message RFC Standard | Your email gateway now identifies and filters the messages that violate the end-of-message RFC standard (that is, <CRLF.CRLF>) to detect threats. |
| | When email gateway receives a message with an invalid end-of-message sequence, it adds an **X-Ironport-Invalid-End-Of-Message** Extension Header (X-Header) to all message IDs (MIDs) within that connection until a message that complies with the end-of-message RFC standard is received. |
| | You can configure policies in content filters to perform necessary actions on these messages. |
| | For more information on configuring the CR and LF Handling field, see the "Listening for Connection Requests by Creating a Listener Using Web Interface" section of *User Guide for AsyncOS 15.5.1 for Secure Email Gateway.* |
| Restarting API Server through CLI | You can now restart the API server using a new CLI subcommand - `API_SERVER`. You can use the `API_SERVER` subcommand to restart and view the status of the API server. The `API_SERVER` subcommand is added under the `diagnostic` > `SERVICES` subcommand. |
| | For more information on the diagnostic command and the subcommands, see the "diagnostic" section in the "The Commands: Reference Examples" chapter of *CLI Reference Guide for AsyncOS 15.5.1 for Cisco Secure Email Gateway.* |

| Configuring Threat Scanner for Threat Detection | In the AsyncOS 15.0 release, the Threat Scanner feature was introduced to detect threats on incoming messages. In this release, you could not directly configure Threat Scanner to detect threats and it was configured in the back end. |
|---|---|
| | From this release onwards, you can configure Threat Scanner to detect incoming threats on your email gateway. You can enable or disable Threat Scanner for each incoming mail policy. When you enable Threat Scanner, it scans the incoming messages and influences the Anti-Spam verdict. |
| | **Prerequisite**: You must enable **Graymail Global Settings** to enable Threat Scanner. |
| | You can configure Threat Scanner per policy in the following ways: |
| | • **Web Interface**: Navigate to **Mail Policies** > **Incoming Mail Policies** and click the link under the **Anti-Spam** column of the mail policy to open the **Mail Policies: Anti-Spam** page. You can check or uncheck the **Enable Threat Scanner** check box. |
| | • **CLI**: Use the `policyconfig` command. |
| | **Install and Upgrade Scenarios** |
| | When you install or upgrade your email gateway from AsyncOS 15.0 or earlier versions to AsyncOS 15.5.1 release, Threat Scanner will be disabled by default. |
| | For more information, see the "Defining Anti-Spam Policies" section in the"Managing Spam and Graymail" chapter of *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |
| | For more information on configuring Threat Scanner using CLI, see the "Configuring Threat Scanner Per Policy "section in the "The Commands: Reference Examples" chapter of *CLI Reference Guide for AsyncOS 15.5.1 for Cisco Secure Email Gateway.* |

| | |
|---|---|
| Including Additional Attributes for Improved Efficacy of SDR Service | Your email gateway now includes the Additional Attributes (Display name and the complete email address - Username, and Domain) by default as part of telemetry data sent to Cisco TAC for reputation analysis to enhance the efficacy of the Sender Domain Reputation (SDR) service. |
| | When the administrator logs into the email gateway, you will receive a warning message informing that the **Include Additional Attributes** option in SDR is enabled by default so that telemetry data includes the processing of personal data. |
| | ✎ **Note**  The **Include Additional Attributes** option is enabled by default only when you enable Sender Domain Reputation Filtering. |
| | If you want to disable the Include Additional Attributes option: |
| | 1. Navigate to **Security Services** > **Domain** Reputation |
| | 2. Click **Edit Global Settings** and uncheck the **Include Additional Attributes** check box. |
| | For more information, see the "Enabling Sender Domain Reputation Filtering on Email Gateway" section in the "Sender Domain Reputation Filtering" chapter of *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |
| C5 Nitro-Instance Support for AWS | From the AsyncOS 15.5.1 release onwards, your email gateway supports **c5.4xlarge** EC2 instance type for the **C600V** model deployed through AWS. |
| | For more information, see Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual on AWS EC2 Installation Guide. |
| Mandatory Usage of Cisco Smart Software Licensing for On-Premises Users | The Cisco Smart Software Licensing usage is mandatory from this release (all releases post AsyncOS 15.0 release) for Cisco Secure Email Gateway. |
| | ✎ **Note**  From AsyncOS 15.5.1 onwards, there will be no support for classic licensing for On-Premises users. 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 in the "System Administration" chapter of the *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |
| | After you enable Cisco Smart Software Licensing, you can upgrade your email gateway to this release and continue to use the existing feature licenses in the Smart Licensing mode. |

| | |
|---|---|
| Configure Threat Defense Connector for individual incoming mail policies | You can now configure Threat Defense Connector for each incoming mail policy. To use this feature, you must have configured and enabled the Threat Defense Connector in your Secure Email Gateway. |
| | Go to **Mail Policies** > **Incoming Mail Policies** to enable or disable Threat Defense Connector for individual mail policies. |
| | For more information, see "Integrating Secure Email Gateway with Threat Defense" chapter of the *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |
| Support of Large Key Size Values for DKIM Verification | You can use the following large key size values for DKIM verification in your email gateway: |
| | • 3072 key bits size |
| | • 4096 key bits size |
| | You can select the new, large key size values for DKIM verification in the following ways: |
| | • **Web Interface**: Go to *Mail Policies > Verification Profiles > Add Profile* or *Default* and select **3072** or **4096** from the *'Smallest Key to be Accepted:'* or *'Largest Key to be Accepted:'* drop down list fields. |
| | • **CLI**: Use `domainkeysconfig` > `keys` > `new` or `edit` > `Enter the smallest key to be accepted` or `Enter the largest key to be accepted` options and enter the required value that corresponds to 3072 or 4096 for a specific DKIM Verification profile. |
| No Support for 512 and 768 Key Size Values in New DKIM Verification profile | From this release onwards, the 512 and 768 key bits size values are no longer supported when you create a new DKIM verification profile. |
| | ✎ **Note** The existing DKIM verification profiles created with 512 and 768 key size values are still supported on upgrade to this release. |
| TLS 1.3 Support for SSL Services | You can now configure TLS 1.3 for the following TLS services in your email gateway: |
| | • GUI HTTPS |
| | • Inbound SMTP |
| | • Outbound SMTP |
| | The email gateway only supports the following TLS ciphers when you configure TLS 1.3 for the "GUI HTTPS," "Inbound SMTP," and "Outbound SMTP" TLS services: |
| | • `TLS_AES_128_GCM_SHA256` |
| | • `TLS_AES_256_GCM_SHA384` |
| | • `TLS_CHACHA20_POLY1305_SHA256` |
| | ✎ **Note** The email gateway does not allow you to modify the ciphers used for TLS 1.3. |
| | After you configure TLS 1.3, you can use it for TLS communication across the legacy or new web interfaces of your email gateway and the API services. |

| | |
|---|---|
| Obtaining File Hash Lists, RAT, SMTP Routes, Save and Load Configuration, Address List, and Incoming Mail Policy Users Information using AsyncOS APIs | You can now obtain information about File Hash Lists, Recipient Access Table (RAT) entries, SMTP Routes, Save and Load Configuration, Address List, and Incoming Mail Policy Users information in your email gateway using AsyncOS APIs.<br><br>For more information, see the "Configuration APIs" section of the *AsyncOS 15.5.1 API for Cisco Secure Email Cloud Gateway - Getting Started Guide*. |
| 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.<br><br>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.<br><br>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. |
| Scanning Password-Protected Attachments in Messages | You can configure the Content Scanner in your email gateway to scan the contents of password-protected attachments in incoming or outgoing messages. The ability to scan password-protected message attachments in the email gateway helps an organization to:<br><br>• Detect phishing campaigns that use malware as attachments in messages with password-protection to target limited cyber-attacks.<br><br>• Analyze messages that contain password-protected attachments for malicious activity and data privacy.<br><br>The following languages are supported for this feature - English, Italian, Portuguese, Spanish, German, French, Japanese, and Korean.<br><br>For more information, see "Using Message Filters to Enforce Email Policies" in the *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |
| Region-based Polling for URL Retrospective Service | You can configure the URL Retrospective Service region to which the Secure Email Gateway connects for verdict updates. The Secure Email Gateway ESA can update the Retrospective Service regions and associated end-point URLs.<br><br>For more information, see the "Setting Up URL Filtering" section in the *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |
| File Analysis Server Region Enhancement | From this release onwards, the File Analysis Server region supports two new regions - Australia and Canada.<br><br>You can configure File Analysis Server region in the following ways:<br><br>• **Web Interface**: Navigate to **Security Services** > **File Reputation and Analysis** and click **Edit Global Settings**.<br><br>• **CLI**: Use the `ampconfig` > `ADVANCED` command.<br><br>For more information, see the "Enabling and Configuring File Reputation and Analysis Services" section in the "File Reputation Filtering and File Analysis" chapter of the *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. |

# Changes in Behavior

| | |
|---|---|
| Application SSH Client Algorithm Support | The following application SSH client algorithms are supported when you add an email gateway to a cluster. |
| | [**Non-FIPS Mode**] |
| | The following cipher algorithm, MAC method, and KEX algorithm are added to your Secure Email and Web Manager by default in addition to the existing algorithms: |
| | • Cipher algorithms - `aes128-ctr` |
| | • MAC methods - `hmac-sha2-256` |
| | • KEX algorithms - `diffie-hellman-group14-sha256` |
| | [**FIPS Mode**] |
| | The following cipher algorithm and MAC method are added to your Secure Email and Web Manager by default in addition to the existing algorithms: |
| | • Cipher algorithms - `aes128-ctr` |
| | • MAC methods - `hmac-sha2-256` |
| Prompt Statement Changes - FIPS Mode | From this release onwards, the prompt statements that you receive, when you enable FIPS mode, and when you enable MINIMIZEDATA in FIPS mode, are modified to include only SMTP instead of SMTP DANE. These statements are modified as the MINIMIZEDATA option under FIPS configuration is not specific to SMTP DANE and is common for SMTP. |
| | **Modified Prompt Statement - Enabling FIPS Mode** |
| | *Do you want to minimize FIPS restriction on SMTP in the email gateway ? [N]>* |
| | **Modified Prompt Statement - Enabling MINIMIZEDATA in FIPS Mode** |
| | *FIPS restriction is currently enforced for SMTP in the email gateway.* |
| | *When you change FIPS restriction, the email gateway reboots immediately. No commit is required.* |
| | *Do you want to minimize FIPS restriction on SMTP in the email gateway ? [N]>* |
| No Support for `aes192-cbc` Cipher in FIPS Mode | From this release onwards, the `aes192-cbc` cipher is not supported for both the SSH server and client in the FIPS mode. If you want to enable FIPS mode in AsyncOS 15.5.1, you must remove the `aes192-cbc` cipher using the `sshconfig`->`SSHD` subcommand in the CLI. |
| | **Note** If your email gateway is in FIPS mode and it is upgraded to the AsyncOS 15.5.1 release, the `aes192-cbc` cipher is removed by default. |

# Upgrade Paths

You can upgrade to release 15.5.1-055 from the following versions:

| | | |
|---|---|---|
| • 15.5.1-001 | • 15.5.0-048 | • 15.0.1-105 |
| • 15.0.1-030 | • 15.0.0-104 | • 15.0.0-097 |
| • 14.3.0-209 | • 14.3.0-032 | • 14.3.0-020 |
| • 14.2.3-102 | • 14.2.3-031 | • 14.2.3-027 |
| • 14.2.2-004 | • 14.2.1-020 | • 14.2.0-620 |

# 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

- The following hardware models are supported for this release:
  - C195
  - C395
  - C695
  - C695F
- The following virtual models are supported for this release:
  - C100v
  - C300v
  - C600v

**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

- C190, C390, and C690
- 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 10.

**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 22, 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:

## Saving Email Gateway's Configuration

If encryption is enabled on your email gateway, we recommend you save a copy of your email gateway's configuration before or after you upgrade to AsyncOS 15.5.1.

You can load the saved email gateway's configuration to restore the previous configuration of your device after you execute the Vault Recovery process to restore the Vault service.

You can save the device's configuration using the following ways:

- Navigate to **System Administration** > **Configuration File** and **select Encrypt passphrases in the configuration files**.
- Use the `saveconfig` command in the CLI and type **2** to select the **Encrypt passphrases** option.

## Executing Vault Recovery Process to Resolve Vault Issues

If your email gateway (on Hardware, On Premises, CES, AWS, KVM, Azure, or Hyper-V) encounters Vault-related issues before or after you upgrade to AsyncOS 15.5.1, then you must execute Vault Recovery process to resolve these issues. Perform the following steps to execute the Vault Recovery process:

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.** `1 (encryption enabled) or 2 (encryption disabled)`

4. Log in to your email gateway with administrator user credentials and reboot the device after the Vault Recovery process is complete.

5. [**Only for Cluster Setup**] Rejoin the email gateway to the cluster after the Vault recovers and the device reboot is complete.

6. [**Only If Encryption is Enabled**] Load a copy of the device's configuration that you had saved earlier to restore previous configuration.

7. Monitor your email gateway for a couple of hours for any Vault service alerts.

Your email gateway recovers, and the vault is reinitialized. Now, you can connect to the device without any issues.

---

**Note** **Encryption Disabled**

In this scenario, all the system configuration settings are retained.

**Encryption Enabled**

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 have to 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]>
```

## 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 |

| Hostname | IPv4 | IPv6 |
|---|---|---|
| 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 15.5.1 release integrates Cisco FIPS Object Module 7.3a, which is currently undergoing FIPS certification review (as of April 2024).

## 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 and .
- If you are upgrading a virtual email gateway, see .

**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 20.

- 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

- Configuring HTTP or HTTPS Proxies with Smart Software Licensing Enabled, page 18
- TLS Mail Delivery Failure in FIPS Mode, page 19
- Activating File Reputation Service for Secure Endpoint Private Cloud, page 19
- DLP Service Status Check, page 19
- Scanning Password-Protected Attachments in Email Gateway, page 19
- Intelligent Multi-Scan and Graymail Global Configuration Changes, page 19

## Configuring HTTP or HTTPS Proxies with Smart Software Licensing Enabled

When you configure HTTP or HTTPS proxies with authentication using a username that includes a domain or realm while enabling Smart Software Licensing, the engine updates fail. This behavior is a known issue.

Defect ID - CSCwi11926

To resolve this issue and for successful engine updates to occur, you must perform the following sequence of steps:

1. Configure HTTP or HTTPS proxies with authentication on the **Security Services** > **Service Updates** page.

**Note** Make sure the username you enter does not contain a domain or realm. For example, in the **Username** field, enter only the username instead of DOMAIN\username.

2. Enable and register Smart Software Licensing, and then request for the license.

3. Click **Update Now** to initiate the engine updates.

   Now, the engine updates are successful.

## TLS Mail Delivery Failure in FIPS Mode

If TLS mail deliveries fail in FIPS mode when DHE ciphers are negotiated, you must enable MINIMIZEDATA using the `MINIMIZEDATA` subcommand under the `fipsconfig` CLI command. For more information on the `fipsconfig` -> `MINIMIZEDATA` subcommand, see "Minimizing FIPS Restriction on SMTP in FIPS Mode" section in the FIPS Management chapter of the *User Guide for AsyncOS 15.5.1 for Secure Email Gateway.*

## 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 20.

## 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

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=15.5.0,15.5.1&prdNam=Cisco%20Secure%20Email%20Gateway |
|---|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.5.1-055&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, 15.5.1-055

**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.

# Software Lifecycle Support Statement

For information about software time-based release model and software release support timelines, see Software Lifecycle Support Statement.

# 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 email gateway. For instructions, see the User Guide or online help.