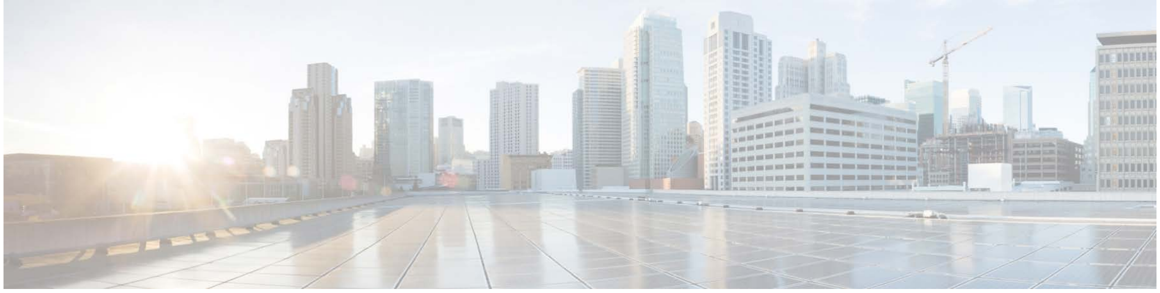

Release Notes for AsyncOS 16.0 for Cisco Secure Email Gateway - GD (General Deployment)

Published: October 3, 2024

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Regenerating SSH Keys for SCP Push Log Retrieval	Your Secure Email Gateway maintains separate host keys for the SCP Push log retrieval. It also allows you to regenerate SSH keys for the SCP Push log retrieval. You can regenerate SSH keys using the `LOGCONFIG` > `HOSTKEYCONFIG` > `REGENERATESCPKEYS` subcommand in the CLI. You can regenerate these new keys only through the CLI and not via the web interface. You must have Administrator, or Cloud Administrator privileges to regenerate these new keys. **Note** When you regenerate SSH keys, you need to update these new keys into the SCP log push server. You can verify these new keys using the `LOGCONFIG` > `HOSTKEYCONFIG` > `USER` subcommand in the CLI. The management of SSH keys varies depending on the scenarios: **New Install Scenario** When you net install the AsyncOS 16.0 version, a new SSH key is generated. **Upgrade Scenario** When you upgrade from AsyncOS 15.5.1 or earlier version to AsyncOS 16.0, you are prompted for consent to inquire if you want to regenerate SSH keys. If you choose to generate new keys, then a new key is generated, if not, the old key is retained. When you upgrade from AsyncOS 16.0 earlier version to AsyncOS 16.0 later version, you are not prompted for consent to inquire if you want to generate SSH keys. The available SSH key is retained. **Revert Scenario** When you revert from AsyncOS 16.0 to an earlier version, you will receive a warning message indicating if you need to replace SSH keys on the SCP push log server. If you have not generated new SSH keys, the warning message is not displayed, and you need not replace SSH keys on the SCP push log server. When you revert from the AsyncOS 16.0 later version to the AsyncOS 16.0 earlier version, the available SSH keys are retained. For more information, see Configuring Host Keys section of the *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway.*

Enhanced File Hash List Support for Content Filters	Your Secure Email Gateway now supports listing file hash lists created with the **MD5 Only** file hash type option, in addition to those created with the **SHA256** Only file hash type option for content filters. **Note** This enhancement is available only for content filters and not for message filters. It can be accessed only through the web interface. You can select the file hast list created with the MD5 Only file hash type option for content filters through the following pages of the web interface: • Navigate to **Mail Policies** -> **Incoming Content Filter** and click **Add Filter**. Under **Conditions**, click **Add Condition** and choose **Attachment File Info** from the **Add Condition** window. • Navigate to **Mail Policies** -> **Incoming Content Filter** and click **Add Filter**. Under **Actions**, click **Add Actions** and choose **Strip Attachment by File Info** from the **Add Actions** window. When you select the **File Hash List** radio button, the file hash lists created with the MD5 Only file hash type option are also listed along with file hash lists created with the SHA256 Only file hash type option. **Note** When you select the **External Threat Feeds** radio button, the file hash lists created using the **All of the above** file hash type option are listed for content filters. For more information, see the Content Filter Conditions and Content Filter Actions section of the *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway*.
Enhanced Alert Emails	You receive alert emails from Secure Email Gateway when you encounter issues with the following limits: • Disk Quota for Miscellaneous Services • Envelope Sender Rate Limit • File Analysis Upload Limit These Alert emails are enhanced to include a direct link to a comprehensive Tech Zone article. This Tech Zone article provides detailed solutions to address your technical inquiries.

Upgrading Image Analysis Engine to IA8.0	Your Secure Email Gateway is now enhanced with the latest Image Analysis (IA) Engine 8.0. This upgrade from the previous IA6.0 version significantly improves the accuracy of scanning scores. You will notice a score difference between the two versions, as IA8.0 employs advanced algorithms for more precise image analysis. **Note** As part of this update, the image sensitivity prompt is removed from the `imageanalysisconfig` -> `SETUP` CLI command. **Note** Image Analyzer 8.0 uses neural networks for image analysis, whereas Image Analyzer 6.0 relies on skin tone analysis. As a result, Image Analyzer 8.0 is more resource-intensive, leading to a performance degradation of approximately 10%. However, this is offset by a substantial improvement in efficacy.
Support for Bounce Verification, SMTP Call Ahead, and Message Filters using AsyncOS APIs	You can now use AsyncOS APIs to view and configure Bounce Verification, SMTP Call-Ahead, and Message Filters in your email gateway. For more information, see the "Configuration APIs" section of the *AsyncOS 16.0 API for Cisco Secure Email Gateway - Getting Started Guide*.
Integrating with Email Threat Defense for Microsoft Office Server (on-premises)	If you are using Microsoft Exchange Server (on-premises), you can now use Email Threat Defense API and Email Threat Defense API Polling to perform Mailbox Auto Remediation of convicted emails identified by Secure Email Threat Defense. This feature can be configured via GUI and CLI. For more information, see the *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway* and *CLI Reference Guide for AsyncOS 16.0 for Cisco Secure Email Gateway.*
Email Threat Defense Remediation Report	A new report - Email Threat Defense Remediation has been added to the Remediation Reports page. For more information on the Email Threat Defense Remediation report, see the Remediation Reports Page section of the *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway*.
Setting Priority for Message Headers	You can now choose to consider only selected priority header for Mail Policy Settings. This can be used if you want the mail policy to match only the priority selected in Match Priority.
Secure Email Relay in Smart Licensing for Virtual Gateways	Secure Email Relay feature lets you send large volumes of emails using the Secure Email Gateway. This feature is only available for accounts with Smart Licensing in virtual gateways, not for on-premises or cloud setups. For more information, see *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway.*

Support for Mail Transfer Agent Strict Transport Security (MTA-STS)	Mail Transfer Agent Strict Transport Security (MTA-STS) protocol enables Secure Email Gateway to determine and act on the TLS policy of a peer Mail Transfer Agent (MTA) for outbound emails, ensuring secure email transmission. You can enable MTA-STS support while configuring the Destination Controls in Secure Email Gateway. For more information, see Mail Transfer Agent Strict Transport Security section of the *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway*.
Transitioning from SecureX to XDR	Cisco SecureX is transitioning to an enhanced and more robust platform, Cisco XDR (Extended Detection and Response). As part of this transition, it is essential to integrate your Secure Email Gateway with the new XDR platform. For more information on how to integrate Secure Email Gateway with XDR, see *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway*.
Nutanix Support	Your Secure Email Gateway 16.0 now supports Nutanix. **Nutanix Version Details:** • Nutanix AOS: 6.5.5.7 • Nutanix Prism Central: pc.2022.6.0.10 For more information, see Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide available at https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.
ESXi 8.0 Support	Your Secure Email Gateway 16.0 now supports ESXi 8.0. For more information, see Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide available at https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

Feature	Description
Displaying Warning Messages for Non-Compliant X.509 Certificates	Your Secure Email Gateway now displays warning messages when you import a non-compliant X.509 certificate using the **Network** -> **Certificates** -> **Add Certificate** page on the web interface or `certconfig` -> `IMPORT` or `PASTE` command in the CLI. Despite the warnings, the certificate will still be uploaded. The warning messages are displayed for the following scenarios: • **Unregistered URI Schemes in SAN Field** - When you import an X.509 certificate that uses a URI with schemes that are not registered with IANA in the Subject Alternative Name (SAN) field, the following warning message is displayed: *Warning: The X.509 certificate must not use URIs with schemes that are not registered with IANA (such as 'invalid'). However, the certificate will still be uploaded.* • **SAN - CN Entry Mismatch** - When you import an X.509 certificate, it must contain at least one SAN entry exactly matching the CN entry, otherwise the following error message is displayed: *Warning: The X.509 certificate must contain at least one SAN entry exactly matching the CN entry: tlstest-SAN-has-no-CN.com. However, the certificate will be uploaded.* • **Incorrect IP Address Format in SAN field** - When you import an X.509 certificate with an IP address in the wrong format in the SAN field, the following warning message is displayed: *Warning: The X.509 certificate must not use IP addresses in the format '10.10.2.32' in the Subject Alternative Name (SAN) field. It must be in the format: 'ipAddress-type'. However, the certificate will still be uploaded.* • **Incorrect IP Address Format in CN field and SAN - CN Entry Mismatch** - When you import an X.509 certificate with an IP address in the wrong format in the CN field and if the X.509 certificate does not contain at least one SAN entry exactly matching the CN entry, the following warning message is displayed: *Warning: The X.509 certificate must not use IP addresses in the format '10.10.2.32' in the CommonName (CN) field for the Subject.* *The X.509 certificate must contain at least one SAN entry exactly matching the CN entry. However, the certificate will still be uploaded.* You can view consolidated warning messages on the Certificates (**Network** -> **Certificates**) page. **Note** When you upgrade or load the configuration file, consolidated warning messages are displayed on the Certificates page (**Network** -> **Certificates**) if the previous release had non-compliant X.509 certificates or if the configuration file contains non-compliant X.509 certificates.

Changes in Behavior

Changes in Behavior	Description
Enhanced Security for Invalid User Error Messages	From this release onwards, the error message displayed to invalid users has been made more generic. This change prevents the identification of valid and invalid account names, thereby enhancing the product's security posture and resiliency.
Changes to Default Settings for Usage Analytics	Before this release, Usage Analytics was enabled by default on the Secure Email Gateway. After you upgrade to this release, Usage Analytics is disabled by default on the Secure Email Gateway.
S/MIME Harvested Key Integration	Prior to this release, users had to manually copy the harvested public keys to the email gateway to verify S/MIME signed messages. From this release onwards, manual copying of the harvested public key is no longer required. The Secure Email Gateway now automatically integrates the harvested public keys to verify signed messages.
Error Message for SP Certificate Expiry	Before this release, the Secure Email Gateway did not display any error message when the Service Provider (SP) certificate expired. After you upgrade to this release, your Secure Email Gateway displays an error message to notify you when the SP certificate expires.
Alert Messages for CA Certificates Expiry	Before this release, you did not receive any alert message from when Certificate Authority (CA) certificates (added using the `updateconfig` -> `TRUSTED_CERTIFICATES` CLI subcommand) were about to expire or had already expired. After you upgrade to this release, you receive alert messages whenever CA certificates (added using the `updateconfig` -> `TRUSTED_CERTIFICATES` CLI subcommand) are about to expire or have expired.
Alert for File Analysis Certificate Expiry	Before this release, an alert was not triggered when the File Analysis certificate expired. Now, the following alert will be displayed if the certificate expires: "The File Analysis server is not reachable. The AMP File Analysis server CA certificate has expired or is invalid."
TLS 1.0 and TLS 1.1 deprecation from AsyncOS for Secure Email Gateway and starting version 16.5	From AsyncOS 16.5 release onwards, the TLS versions 1.0 and 1.1 will be removed from CLI and GUI configuration options. You can use TLS 1.2 and 1.3 for permit email delivery and receiving available from the **`sslconfig`** CLI command and **System Administration** > **SSL Configuration** menu on the UI. For more information on how to update TLS versions, see "System Administration" section of the *User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway*.

Upgrade Paths

You can upgrade to release 16.0.0-050 from the following versions:

- 14.3.0-032
- 15.0.0-104
- 15.0.1-030
- 15.0.1-105
- 15.0.2-034
- 15.5.1-055
- 15.5.2-018
- 15.5.2-012
- 15.5.2-021
- 16.0.0-043

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, and C695F
- The following virtual models are supported for this release: C100v, C300v, and 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 are 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 9.

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 21, 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, page 10
- Executing Vault Recovery Process to Resolve Vault Issues, page 10
- Saving Email Gateway's Configuration, page 10
- Features Configurable using IDN Domains in Email Gateway, page 12
- New Categories and New Names for Existing URL Reputation Verdicts, page 14
- Firewall Settings to Access Cisco Talos Services, page 14
- Firewall Settings to Access Cisco Advanced Phishing Protection Cloud Service, page 15
- Enabling Service Logs on Email Gateway, page 15
- Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels, page 15
- FIPS Compliance, page 13
- Upgrading Deployments with Centralized Management (Clustered Appliances), page 15
- Upgrading From a Release Other Than the Immediate Previous Release, page 16
- Configuration Files, page 16
- IPMI Messages During Upgrade, page 16

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.

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 Lists of Fixed Issues, page 14 and Installation and Upgrade Notes, page 7.
- If you are upgrading a virtual email gateway, see Upgrading a Virtual Appliance, page 9.

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 19.
- 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 17
- Activating File Reputation Service for Secure Endpoint Private Cloud, page 18
- DLP Service Status Check, page 18
- Scanning Password-Protected Attachments in Email Gateway, page 18
- Intelligent Multi-Scan and Graymail Global Configuration Changes, page 18

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.

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 Fixed Issues, page 14.

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 19
- Known and Fixed Issues in Release 16.0.0-050, page 19
- Finding Information about Known and Resolved Issues, 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.

Known and Fixed Issues in Release 16.0.0-050

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&prdNam=Cisco%20Secure%20Email%20Gateway&rls=16.0.0
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=16.0.0-050&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, 16.0.0-050

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.

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.