Getting Started with Cisco Secure Email Gateway

This chapter contains the following sections:

What's New in AsyncOS 15.5.1

Table 1: Whats New in AsyncOS 15.5.1

Feature	Description
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 Listening for Connection Requests by Creating a Listener Using Web Interface.

Feature	Description
Monitoring Vault Service and Sending Alerts	

Feature	Description
	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. You can access the alert logs using one of the following ways: • Navigate to **System Administration** > **Alerts** page on the web interface, and click the **View Top Alerts** button. • Use the `displayalerts` command in the CLI. 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. **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. You will receive alert messages in the following scenarios: • 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. • If any of the services of your email gateway use the 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. 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. For information on an example of a successful vault health check and initialization log entry, see Successful Vault Health Check and Initialization. To restore the Vault service, you have to execute the Vault Recovery process. **Note** 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

Feature	Description
	configuration, see Saving Email Gateway's Configuration section in the Release Notes. For information on how to execute the Vault Recovery process, see Executing Vault Recovery Process to Resolve Vault Issues section in the Release Notes.
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 the CLI Reference Guide.
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 Defining Anti-Spam Policies.

Feature	Description
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 Enabling Sender Domain Reputation Filtering on 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

Feature	Description
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, and 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 in your email gateway using AsyncOS APIs. 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. 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.

Feature	Description
Synchronizing Configuration Changes between Machines in Different Clusters Simultaneously	You can synchronize configuration changes made to a logged-in machine in one cluster to all machines in a remote cluster simultaneously. The synchronization process occurs only when both clusters are in the same or different data centers of the same region. **Note** You can only synchronize configuration changes between machines at the cluster level and not at the group or machine level. **Note** You must move the machine to the group level to avoid the SPAM Quarantine IP configuration being synchronized over the intercluster. To enable this feature, contact your Cisco account manager. **Prerequisite**: Before you request your Cisco account manager to enable this feature, ensure the configuration is the same in all machines across the clusters. After the synchronization process is complete, if you make a configuration change in one machine, the same configuration is automatically replicated to all machines across the clusters. You can view the same in the System Logs. For more information see, Logging. **Note** You must not modify the cluster name after the inter-cluster connection process is complete. Make sure to have a unique name for the cluster.
Configure Threat Defense Connector for individual incoming mail policies.	You can now configure Threat Defense Connector for each incoming mail policies and also use separate message intake addresses for each 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 policy. For more information, see Integrating Secure Email Gateway with Threat Defense.

Feature	Description
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: • Detect phishing campaigns that use malware as attachments in messages with password-protection to target limited cyber-attacks. • Analyze messages that contain password-protected attachments for malicious activity and data privacy. The following languages are supported for this feature - English, Italian, Portuguese, Spanish, German, French, Japanese, and Korean. For more information, see Using Message Filters to Enforce Email Policies.
Region-based Polling for URL Retrospective Service	You can configure the URL Retrospective Service region to which the Secure Email Cloud Gateway connects for verdict updates. The Secure Email Cloud Gateway ESA can update the Retrospective Service regions and associated end-point URLs. For more information, see Setting Up URL Filtering.
File Analysis Server Region Enhancement	From this release onwards, the File Analysis Server region supports two new regions - Australia and Canada. You can configure File Analysis Server region in the following ways: • **Web Interface**: Navigate to **Security Services** > **File Reputation and Analysis** and click **Edit Global Settings**. • **CLI**: Use the `ampconfig` > `ADVANCED` command. For more information, see Enabling and Configuring File Reputation and Analysis Services.

Comparison of Web Interfaces, New Web Interface with Legacy Web Interface

The following table shows the comparison of the new web interface with the legacy interface:

Table 2: Comparison of New Web Interface with legacy interface

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Landing Page	After you log in to the email gateway, the Mail Flow Summary page is displayed.	After you log in to the email gateway, the My Dashboard page is displayed.
Reports Drop-down	You can view reports for your email gateways from the Reports drop-down.	You can view reports for your email gateway from the **Monitor** menu.
My Reports Page	Choose **My Reports** from the Reports drop-down.	You can view the My Reports page from **Monitor** > **My Dashboard**.
Mail Flow Summary Page	The **Mail Flow Summary** page includes trend graphs and summary tables for incoming and outgoing messages.	The **Incoming Mail** includes graphs and summary tables for the incoming and outgoing messages.
Advanced Malware Protection Report Pages	The following sections are available on the **Advanced Malware Protection** report page of the Reports menu: • Summary • AMP File Reputation • File Analysis • File Retrospection • Mailbox Auto Remediation	The email gateway has the following **Advanced Malware Protection** report pages under **Montior** menu: • Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Mailbox Auto Remediation
Outbreak Filters Page	The Past Year Virus Outbreaks and Past Year Virus Outbreak Summary are not available in the **Outbreak Filtering** report page of the new web interface.	The **Monitor** > **Outbreak Filters** page displays the Past Year Virus Outbreaks and Past Year Virus Outbreak Summary.
Spam Quarantines (Administrative and End Users)	Click **Quarantine** > **Spam Quarantine** > **Search** in the new web interface. The end users can access the spam quarantine using the URL: `https://example.com:<https-api-port>/euq-login` where `example.com` is the appliance hostname and `<https-api-port>` is the AsyncOS API HTTPS port opened on the firewall.	You can view spam quarantine from the **Monitor** > **Spam Quarantine** menu.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Policy, Virus and Outbreak Quarantines	Click **Quarantine** > **Other Quarantine** in the new web interface. You can only view Policy, Virus and Outbreak Quarantines in the new web interface.	You can view, configure and modify the Policy, Virus and Outbreak Quarantines on the email gateway using the **Monitor** > **Policy, Virus and Outbreak Quarantines**.
Select All Action for Messages in Quarantine	You can select multiple (or all) messages and perform a message action such as delete, delay, release, move, etc.	You cannot select multiple messages to perform a message action.
Maximum Download Limit for Attachments	The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.	-
Rejected Connections	To search for rejected connections, click **Tracking** > **Search** > **Rejected Connection** tab on the .	-
Query Settings	The Query Settings field of the Message Tracking feature is not available on the .	You can set the query timeout in the Query Settings field of the Message Tracking feature.
Message Tracking Data Availability	Click the gear icon on the upper right side of the page the web interface to access Message Tracking Data Availability page.	You can view the missing-data intervals for your email gateway.
Show Additional Details of Messages	You can view additional details of a message such as Verdict Charts, Last State, Sender Groups, Sender IP, IP Reputation Score and Policy Match details.	-
Verdict Charts and Last State Verdicts	Verdict Chart displays information of the various possible verdicts triggered by each engine in your email gateway. Last State of the message determines the final verdict triggered after all the possible verdicts of the engine.	Verdict Charts and Last State Verdicts of the messages are not available.
Message Attachments and Host Names in Message Details	Message attachments and host names are not displayed in the Message Details section of the message on the email gateway.	Message attachments and host names are displayed in the Message Details section of the message.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Sender Groups, Sender IP, IP Reputation Score and Policy Match in Message Details	Sender Groups, Sender IP, IP Reputation Score, and Policy Match details of the message is displayed in the Message Details section, on the email gateway.	Sender Groups, Sender IP, IP Reputation Score, and Policy Match of the message is not available in the Message Details section of the message.
Direction of the Message (Incoming or Outgoing)	Direction of the message (incoming or outgoing) is displayed in the message tracking results page, on the email gateway.	Direction of the message (incoming or outgoing) is not displayed in the message tracking results page.

Where to Find More Information

Cisco offers the following resources to learn more about your email gateway:

Documentation

You can access the online help version of this user guide directly from the appliance GUI by clicking Help and Support in the upper-right corner.

The documentation set for the Cisco Secure Email Gateway includes the following documents and books:

- Release Notes
- Quick Start Guide for your Cisco Email Security Appliance model
- Hardware Installation or Hardware installation and maintenance guide for your model or series
- *Cisco Content Security Virtual Appliance Installation Guide*
- *User Guide for AsyncOS for Cisco Secure Email Gateway* (this book)
- *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*
- AsyncOS API for Cisco Secure Email Gateway - Getting Started Guide

Documentation for all Cisco Content Security products is available from:

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.

Documentation For Cisco Content Security Products	Location
Cisco Email Security	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd- products-support-series-home.html
Cisco Web Security	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products- support-series-home.html
Cisco Content Security Management	http://www.cisco.com/c/en/us/support/security/content-security-management- 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 IronPort Encryption	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

Training

More information about training is available from:

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

Cisco Notification Service

Sign up to receive notifications relevant to your Cisco Content Security Appliances, such as Security Advisories, Field Notices, End of Sale and End of Support statements, and information about software updates and known issues.

You can specify options such as notification frequency and types of information to receive. You should sign up separately for notifications for each product that you use.

To sign up, visit http://www.cisco.com/cisco/support/notifications.html

A Cisco.com account is required. If you do not have one, see Registering for a Cisco Account , on page 14.

Knowledge Base

Procedure

Step 1 Go to the main product page (http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html)

Step 2 Look for links with **TechNotes** in the name.

Cisco Support Community

The Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general email and web security issues, as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community on the Customer Support Portal at the following URLs:

- For email security and associated management:

  https://supportforums.cisco.com/community/5756/email-security

- For web security and associated management:

  https://supportforums.cisco.com/community/5786/web-security

Cisco Customer Support

Do not contact Cisco Customer Support for help with Cisco Secure Email Cloud Gateway. See the Cisco IronPort Hosted Email Security / Hybrid Hosted Email Security Overview Guide for information on getting support for Cloud/Hybrid Email Security appliances.

Cisco TAC: http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Support site for legacy IronPort: http://www.cisco.com/c/en/us/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.

Third Party Contributors

See Open Source licensing information for your release on this page: http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html .

Some software included within Cisco AsyncOS is distributed under the terms, notices, and conditions of software license agreements of FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc., and other third party contributors, and all such terms and conditions are incorporated in Cisco license agreements.

The full text of these agreements can be found here:

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.

Portions of the software within Cisco AsyncOS is based upon the RRDtool with the express written consent of Tobi Oetiker.

Portions of this document are reproduced with permission of Dell Computer Corporation. Portions of this document are reproduced with permission of McAfee, Inc. Portions of this document are reproduced with permission of Sophos Plc.

Cisco Welcomes Your Comments

The Cisco Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address:

contentsecuritydocs@cisco.com

Please include the product name, release number, and document publication date in the subject of your message.

Registering for a Cisco Account

Access to many resources on Cisco.com requires a Cisco account.

If you do not have a Cisco.com User ID, you can register for one here: https://idreg.cloudapps.cisco.com/idreg/register.do

Related Topics

- Cisco Notification Service , on page 12
- Knowledge Base, on page 12

Cisco Secure Email Gateway Overview

The AsyncOS™ operating system includes the following features:

- **Anti-Spam** at the gateway, through the unique, multi-layer approach of SenderBase Reputation Filters and Cisco Anti-Spam integration.
- **Anti-Virus** at the gateway with the Sophos and McAfee Anti-Virus scanning engines.
- **Outbreak Filters™**, Cisco's unique, preventive protection against new virus, scam, and phishing outbreaks that can quarantine dangerous messages until new updates are applied, reducing the window of vulnerability to new message threats.
- **Policy, Virus, and Outbreak Quarantines** provide a safe place to store suspect messages for evaluation by an administrator.
- **Spam Quarantine** either on-box or off, providing end user access to quarantined spam and suspected spam.
- **Email Authentication**. Cisco AsyncOS supports various forms of email authentication, including Sender Policy Framework (SPF), Sender ID Framework (SIDF), and DomainKeys Identified Mail (DKIM) verification of incoming mail, as well as DomainKeys and DKIM signing of outgoing mail.
- Cisco **Email Encryption**. You can encrypt outgoing mail to address HIPAA, GLBA and similar regulatory mandates. To do this, you configure an encryption policy on the email gateway and use a local key server or hosted key service to encrypt the message.
- **Email Security Manager**, a single, comprehensive dashboard to manage all email security services and applications on the email gateway. Email Security Manager can enforce email security based on user groups, allowing you to manage Cisco Reputation Filters, Outbreak Filters, Anti-Spam, Anti-Virus, and email content policies through distinct inbound and outbound policies.
- **On-box message tracking**. AsyncOS for Email includes an on-box message tracking feature that makes it easy to find the status of messages that the E email gateway processes.
- **Mail Flow Monitoring** of all inbound and outbound email that provides complete visibility into all email traffic for your enterprise.
- **Access control** for inbound senders, based upon the sender's IP address, IP address range, or domain.
- Extensive **message and content filtering** technology allows you to enforce corporate policy and act on specific messages as they enter or leave your corporate infrastructure. Filter rules identify messages based on message or attachment content, information about the network, message envelope, message headers, or message body. Filter actions allow messages to be dropped, bounced, archived, blind carbon copied, or altered, or to generate notifications.

- **Message encryption via secure SMTP over Transport Layer Security** ensures messages traveling between your corporate infrastructure and other trusted hosts are encrypted.
- **Virtual Gateway™** technology allows the email gateway to function as several email gateways within a single server, which allows you to partition email from different sources or campaigns to be sent over separate IP addresses. This ensures that deliverability issues affecting one IP address do not impact others.
- **Protection against malicious attachments and links** in email messages, provided by multiple services.
- Use **Data Loss Prevention** to control and monitor the information that leaves your organization.

AsyncOS supports RFC 2821-compliant Simple Mail Transfer Protocol (SMTP) to accept and deliver messages.

Most reporting, monitoring, and configuration commands are available through both the web-based GUI via HTTP or HTTPS. In addition, an interactive Command Line Interface (CLI) which you access from a Secure Shell (SSH) or direct serial connection is provided for the system.

You can also set up a Cisco Secure Email and Web Manager to consolidate reporting, tracking, and quarantine management for multiple E email gateways.

Related Topics

- Supported Languages, on page 15

Supported Languages

AsyncOS can display its GUI and CLI in any of the following languages:

- English
- French
- Spanish
- German
- Italian
- Korean
- Japanese
- Portuguese (Brazil)
- Chinese (traditional and simplified)
- Russian