Getting Started with Cisco Secure Email Gateway

This chapter contains the following sections:

What's New in AsyncOS 15.0

Table 1: Whats New in AsyncOS 15.0

Feature	Description
Improved Efficacy to Detect Threats	

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

Feature	Description
Enforcing TLS for Outgoing Messages at Sender or Recipient Level	The existing Destination Controls configuration allows you to override the TLS modes (such as TLS Mandatory, TLS Preferred, and so on) on a per-domain basis. If you need to enforce TLS for outgoing messages based on additional conditions such as – senders, recipients, and so on, you can now use the `X-ESA-CF-TLS-Mandatory` header. You can configure the "Content Filter – Add/Edit Header" action to add the `X-ESA-CF-TLS-Mandatory` header in the “Header Name:” field based on any content filter conditions and attach the content filter to an outgoing mail policy.
File Reputation Service Enhancement	From AsyncOS 15.x release onwards, the email gateway uses a new version of the AMP engine. This new AMP engine uses HTTPS (port 443) instead of TCP to ensure secure communication between your email gateway and Secure Endpoint Cloud. For more information, see File Reputation Filtering and File Analysis.
Obtaining Configuration Information using AsyncOS APIs	You can use the Configuration APIs to perform various operations (such as create, retrieve, update, and delete) in your email gateway. The various API categories for configuration are: • Authentication APIs • URL Lists APIs • Dictionary APIs • Host Access Table (HAT) APIs **Note** For Configuration APIs, the administrator and cloud administrator user roles are only supported. **Note** For Configuration APIs: • If you modify any of the APIs in the cluster mode, the changes apply to all the other machines in the cluster. • If you modify any of the APIs in the group mode, the changes apply to all the other machines in the group. • If you modify any of the APIs in the machine mode, the changes only apply to the specified machine. For more information, see the “Configuration APIs” section in the *AsyncOS 15.0 API for Cisco Secure Email Gateway - Getting Started Guide*.

Feature	Description
Customizing Graymail Unsubscribe Banner	You can customize the following settings of the Graymail Unsubscribe banner based on your organization's requirements: • Position of the banner • Color of the banner • Text color of the banner message • Contents of the banner message The banner message supports the following languages: English (United States), Italian, Chinese, Portuguese, Spanish, German, French, Russian, Japanese, Korean, and Chinese (Taiwan). **Note** There is no CLI support for the feature in this release. For more information, see Customizing Graymail Unsubscribe Banner based on Organizational Requirements.

Feature	Description

Removal of Old Splunk Database for Email Tracking Data	[**For on-premises users only**]: When you upgrade to Secure Email Gateway 15.0 and later, and if the email tracking data is contained in the Splunk database, the system deletes the Splunk database if you proceed with the upgrade.
	
	During the upgrade, a warning message indicating that the system will delete the Splunk database is displayed in the CLI or the web interface of your email gateway.
	
	Following is a sample warning message displayed at the time of the upgrade:
	
	`"From Secure Email Gateway 12.1.x version onwards, we have moved to a newer storage system for email tracking data.`
	`Generally, the old data is replaced with new data in the new storage system automatically.`
	`However, in some scenarios (for example, 'late upgrades', 'low mail flow' and 'tracking data', and so on),`
	`there could be traces of old data still present in the old storage system that is no longer supported.`
	`In your case it is, 7.1 MB, which was last updated in 01 Jul 2022.`
	`If you proceed with this upgrade process, the data in the old storage will be removed.`
	`You can choose to proceed with the upgrade or abort the upgrade.`
	`Do you want to proceed with the upgrade?[Y]"`
	
	Note The `debug` sub menu used to collect debug information for the Splunk database is removed from the `Diagnostic` > `Tracking` sub command in the CLI.
	
	[**For cloud users only**]:When you upgrade to Secure Email Gateway 15.0 and later, and if the email tracking data is contained in the Splunk database, the system deletes the Splunk database if you proceed with the upgrade.
	
	Note The `debug` sub menu used to collect debug information for the Splunk database is removed from the `Diagnostic` > `Tracking` sub command in the CLI.

FIPS Certification	Cisco Secure Email Gateway is FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #4036). For more information, see FIPS Management.

Feature	Description
Deleting Log Files from Email Gateway	You can now delete log files stored in the /data/pub/directories path of your email gateway. You can use the `logconfig` > `deletelogfile` sub command in the CLI to delete the log files. **Note** You can delete log files only if your email gateway is a standalone machine. For more information, see the "Example - Deleting Log Files" section of the CLI Reference Guide associated with this release.
New RAM Values for Secure Email Gateway Virtual Appliance Models	From AsyncOS 15.0 release onwards, there are new RAM values for the following Secure Email Gateway virtual appliance models deployed through KVM or VMWare ESXi: • C100V • C300V • C600V For details on the new RAM values applicable for each virtual appliance model, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

Feature	Description
New DLP Policy Pre-defined Classifiers	

Feature	Description
	The following new DLP policy pre-defined classifiers are added in the *Mail Policies > DLP Policy Manager > Add DLP Policy > Custom Policy > Add > Policy Matching Details* page of your web interface: • Bank Account Numbers (Austria IBAN) • Bank Account Numbers (Belgium IBAN) • Bank Account Numbers (Bulgaria IBAN) • Bank Account Numbers (Croatia IBAN) • Bank Account Numbers (Cyprus IBAN) • Bank Account Numbers (Czech Republic IBAN) • Bank Account Numbers (Denmark IBAN) • Bank Account Numbers (Estonia IBAN) • Bank Account Numbers (Finland IBAN) • Bank Account Numbers (Greece IBAN) • Bank Account Numbers (Hungary IBAN) • Bank Account Numbers (Ireland IBAN) • Bank Account Numbers (Latvia IBAN) • Bank Account Numbers (Lithuania IBAN) • Bank Account Numbers (Luxembourg IBAN) • Bank Account Numbers (Malta IBAN) • Bank Account Numbers (Poland IBAN) • Bank Account Numbers (Portugal IBAN) • Bank Account Numbers (Romania IBAN) • Bank Account Numbers (Slovakia IBAN) • Bank Account Numbers (Slovenia IBAN) • Bank Account Numbers (Spain IBAN) • Cambodia National ID • Cyprus National ID • Finland National ID • Malta National ID • Myanmar National ID • Portugal National ID

Feature	Description
	• Vietnam National ID
New Note for Removal of Weak Algorithms during System Upgrade	[Applicable to FIPS and non-FIPS modes]: During the system upgrade to AsyncOS 15.0 and later, a new Note statement is added to inform you that the system removes all weak algorithms in Ciphers, Keys, KEX, and MAC (if configured) after the upgrade process.
ECDSA Certificates Support for SSL Communication	You can now use the Elliptic Curve Digital Signature Algorithm (ECDSA) certificates that allow the combination of Elliptic Curve Diffie Hellman Ephemeral (ECDHE) algorithm for Key Exchange and ECDSA authentication to configure the following SSL services: • GUI HTTPS • Inbound SMTP

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.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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.
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.	-

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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.
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 , on page 13

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.
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 15.

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 14
- Knowledge Base, on page 14

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 16

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