Getting Started with Cisco Email Security

This chapter contains the following sections:

What's New in AsyncOS 13.5.2

Table 1: Whats New in AsyncOS 13.5.2

Feature	Description
Cisco SecureX Integration	Cisco Email Security appliance now supports integration with Cisco SecureX. Cisco SecureX is a security platform embedded with every Cisco security product. The integration of the Email Security appliance with Cisco SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration. Cisco SecureX unifies visibility of security infrastructure, enables automation, accelerates incident response workflows, and improves threat detection. The distributed capabilities of Cisco SecureX are available in the form of applications (apps) and tools in the Cisco SecureX Ribbon. For more information, see Integrating with Cisco SecureX Threat Response. You can also access the “Integrate Cisco Email Security Gateway with Cisco SecureX or Cisco Threat Response” walkthrough by clicking the How-Tos widget on the web interface of your appliance.

Feature	Description
Configuring Custom SMTP Helo for SMTP Conversation	A new option is added in the `interfaceconfig > edit` subcommand in the CLI to configure custom SMTP Helo. You can use the new CLI option to modify the default interface hostname used for the SMTP Helo.
New Cisco Talos Email Status Portal	The Cisco Talos Email Status Portal replaces the legacy Cisco Email Submission and Tracking Portal. The Cisco Talos Email Status Portal is a web-based tool for monitoring the status of email submissions from end-users. **Important** • Users of the legacy portal can still access their previous submissions in the new portal • You will not be able to submit samples of spam, phish, ham, marketing or non-marketing emails that may have been misidentified by your email appliance in the new portal. For more information on how to submit email samples, see the How to Submit Email Messages to Cisco document at https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html. For more information, see Managing Spam and Graymail.
Enhancement to Messages with File Analysis Pending functionality	A new option - **Drop Message Attachments while File Analysis Verdict Pending** is added under **Messages with File Analysis Pending** section (**Mail Policies** > **Incoming Mail Policies** and click the link in the Advanced Malware Protection column of the mail policy to modify. Now, you can choose whether to drop attachments in case of any file analysis verdict pending while delivering the final message from the appliance. The default option is 'No'. If you set the option as 'Yes', the Processing Details section of the Message Tracking (**Monitor** >**Message Tracking**) displays the details related to the message attachments dropped when the file analysis verdict is pending. The Mail logs also display the log details of the message attachments dropped when the file analysis verdict is pending based on the configured AMP policy.' You can also enable this option using the `policyconfig` command in the CLI. For more information, see File Reputation Filtering and File Analysis.

Feature	Description
Enhancement for Request Retry Method of File Reputation Service:	You can now set the reputation query timeout value within the range of 20–30 seconds while configuring the file reputation and analysis services (Security Services > File Reputation and Analysis). The default value is 20, which is the minimum value. During the configured query timeout, the appliance sends the file reputation queries to the AMP server. If the appliance fails to receive response from the AMP server, it retries by sending the query again to the AMP server. The query timeout includes the time taken for the first query request and the retry request. The retry method enables the appliance to receive responses when there are network latencies, issues related to the AMP server, and so on.
Configuring Email Gateway to consume SecureX Threat Response Feeds	You can configure your email gateway to consume threat feeds from the Cisco SecureX Threat Response portal. The Cisco SecureX Threat Response portal allows you to create custom feeds for the continuous gathering of observables and to consume them in your email gateway using the feed URL. A feed is a simple list of observables in JSON format. The feeds are created and managed in the **Intelligence** > **Feeds** page in the SecureX Threat Response portal. For more information, see Configuring Email Gateway to Consume External Threat Feeds.

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 appliance , the Mail Flow Summary page is displayed.	After you log in to the appliance, the My Dashboard page is displayed.
Reports Drop-down	You can view reports for your appliances from the Reports drop-down.	You can view reports for your appliance 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**.

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

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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 appliance .
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 appliance . 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 appliance.	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 appliance.	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 appliance.	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 appliance :

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 Email Security appliances 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 Email Security Appliances* (this book)
- *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*
- AsyncOS API for Cisco Email Security Appliances - 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 8.

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

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 appliance . 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 7
- Knowledge Base, on page 7

Cisco Email Security Appliance 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 appliance 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 appliance. 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 Eappliance 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 appliance 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 Security Management appliance to consolidate reporting, tracking, and quarantine management for multiple Eappliances .

Related Topics

- Supported Languages, on page 10

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