Getting Started with the Cisco Cloud Email Security

This chapter contains the following sections:

What's New in AsyncOS 13.0

Table 1: Whats New in AsyncOS 13.0

Feature	Description
Mailbox Auto Remediation on Microsoft Exchange online, Microsoft Exchange on-premise, hybrid, and multi-tenant deployments	A file can turn malicious anytime, even after it has reached user's mailbox. AMP can identify this as new information emerges and push retrospective alerts to your appliance. You can configure your appliance to perform auto-remedial actions on the messages in user mailbox when the threat verdict changes. The appliance can perform auto-remedial actions on the messages in the following mailbox deployments: • Microsoft Exchange online – mailbox hosted on Microsoft Office 365 • Microsoft Exchange on-premise – a local Microsoft Exchange server • Hybrid/Multiple tenant configuration – a combination of mailboxes configured across Microsoft Exchange online and Microsoft Exchange on-premise deployments For more information, see Automatically Remediating Messages in Mailboxes.

Feature	Description
FIPS Certification	Cisco Email Security Appliance will be FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #2984). For more information, see FIPS Management.
Single Sign-On (SSO) using SAML 2.0	The Cisco Email Security appliance now supports SAML 2.0 SSO to allow users can log in to the web interface (both legacy and the new web interface) of the appliance using the same credentials that are used to access other SAML 2.0 SSO enabled services within their organization. For more information, see System Administration.
Support for Unified Common Event Format (CEF)-based Logging	The Cisco Email Security appliance now supports a new type of log subscription – 'Consolidated Event Logs' that summarizes each message event in a single log line. This reduces the number of bytes of data (log information) sent to a Security Information and Event Management (SIEM) vendor for analysis. The Consolidated Event Logs are in the Common Event Format (CEF) log message format supported by all SIEM vendors. For more information, see Logging.
Ability to safe print message attachments.	You can configure your email gateway to provide a safe view (safe-printed PDF version) of a message attachment detected as malicious or suspicious. The safe view of the message attachment is delivered to the end user and the original attachment is stripped from the message. You can use the 'Safe Print' content filter action to safe print all message attachments that match a configured content filter condition. The ability to safe print message attachments in the email gateway, helps an organization to: • Prevent message attachments with malicious or suspicious content from entering an organization network. • View malicious or suspicious message attachments without being affected by the malware. • Deliver the original message attachment based on the end-user request. For more information, see Configuring Email Gateway to Safe Print Message Attachments.

Feature	Description
Integrating the Appliance with Cisco Threat Response	You can integrate your appliance with Cisco Threat Response, and perform the following actions in Cisco Threat Response: • View the message tracking data from multiple appliances in your organization. • Identify, investigate, and remediate threats observed in the message tracking. • Resolve the identified threats rapidly and provide recommended actions to take against the identified threats. • Document the threats to save the investigation, and enable collaboration of information among other devices. For more information, seeIntegrating with Cisco Threat Response.
Performing Threat Analysis using Casebooks	The Cisco Email Security appliance now includes the casebook and pivot menu widgets. **Note** If you are using the Microsoft Internet Explorer browser to access your appliance, you will not be able to use the casebook widget. You can perform the following actions in your appliance using the casebook and pivot menu widgets: • Add an observable to a casebook to investigate for threat analysis. • Pivot an observable to a new case, an existing case, or other devices registered in Cisco Threat Response (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis. For more information, see Integrating with Cisco Threat Response.
Improving User Experience by Collecting Feature Usage Statistics	The Cisco Email Security appliance now collects feature/interface usage statistics on the new web interface of the appliance that helps cisco improve overall user experience. All data collected is anonymized. If you want to opt-out of this feature, navigate to **System Administration > General Settings > Usage Analytics** page of the web interface to disable it. For more information, see Collecting Usage Statistics of the Appliance on the New Web Interface.

Feature	Description
Anti-Spam Scanning Configuration Enhancement	A new 'Aggressive' scanning profile is added to the Anti-Spam global settings. You can use this profile to assign a higher priority on incoming or outgoing messages detected as spam, and to accept a higher chance of false positives. You can enable this option in any one of the following ways: • **Security Services > IronPort Anti-Spam > Edit Global Settings** in the web interface. See Configuring IronPort Anti-Spam Scanning. • `antispamconfig` command in the CLI. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*. **Note** If aggressive scanning profile option is enabled, the mail policy adjustments to Anti-Spam thresholds have a larger impact than when a Normal Profile scanning is used. Therefore, you must review the existing Anti-Spam mail policy thresholds settings for the best balance of spam catch rate versus false positive potential.

Feature	Description

New Web Interface for Reporting, Quarantine, and Tracking	The appliance now has a new web interface to search and view:
	• Email Threat Reports
	• File and Malware Reports
	• Connection and Flow Reports
	• User Reports
	• Filter Reports
	• Scheduled Reports
	• Archived Reports
	• For more information, see Email Security Monitor Pages on the New Web Interface.
	• **Spam Quarantine**
	  • You can now view and search for spam and suspected spam messages in **Quarantine > Spam Quarantine > Search** page in the web interface.
	  • You can view, add and search for domains added in the safelist and blocklist in **Quarantine** > **Spam Quarantine** > **Safelist** or **Blocklist** page in the web interface.
	For more information, see Spam Quarantine.
	• **Policy, Virus and Outbreak Quarantines**. You can view and search for policy, virus and outbreak quarantines in **Quarantine > Other Quarantine > Search** page on the web interface. For more information, see Policy, Virus, and Outbreak Quarantines.
	• **Message Tracking**. You can search for messages or a group of messages depending on your search criteria in **Tracking > Search** page in the web interface. For more information, see Tracking Messages.
	Important
	• Make sure that you have enabled AsyncOS API on the appliance.
	• Make sure that AsyncOS HTTPS API port is not enabled on multiple networkd interfaces.
	• By default, `trailblazerconfig` is enabled on the appliance.
	  • Make sure that the configured HTTPS port is opened on the firewall. The default HTTPS port is 4431.
	  • Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

Feature	Description
The `trailblazerconfig` CLI Command	You can use the `trailblazerconfig` command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface. **Note** By default, `trailblazerconfig` CLI command is enabled on your appliance. You can see the inline help by typing the command: `help trailblazerconfig`. For more information, see *Cisco Email Security Command Reference Guide*.
Message Tracking Enhancement	You can now search for messages based on the "`Reply-To`" header of the message. For more information, see Tracking Messages.
Advanced Malware Protection Report Enhancements	The Advanced Malware Protection report page has the following enhancements: • A new section - **Incoming Malware Files by Category** to view the percentage of blacklisted file SHAs received from the AMP for Endpoints console that are categorised as **Custom Detection**. The threat name of a blacklisted file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report. • A new section - **Incoming Malware Files by Category** to view the percentage of blacklisted file SHAs based on the threshold settings that are categorised as **Custom Threshold**. • You can click on the link in the More Details section of the report to view the file trajectory details of a blacklisted file SHA in the AMP for Endpoints console. • A new verdict – **Low Risk** is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the Incoming Files Handed by AMP section of the report. See Advanced Malware Protection Page.
Metrics Bar Widget	The Metrics Bar widget enables you to view the real time data of the file analysis done by the Cisco Threat Grid appliance on the Advanced Malware Protection report page. For more information, see Advanced Malware Protection Page.

Feature	Description
Ability to categorize IP addresses as persistent whitelist or blacklist	You can categorize the IP address that you use to access the appliance using SSH as a persistent whitelist or blacklist. If the appliance or the `ipblockd` service is restarted, the IP address in the persistent blacklist or whitelist is retained. You can use the `sshconfig > access` control sub command in the CLI to categorize the IP address as a persistent whitelist or blacklist. For more information, see the `sshconfig` section of the *CLI Reference Guide for AsyncOS 13.0 for Email Security Appliances*.
Forged Email Detection Enhancement	You can now create an exception list consisting of only full email addresses to bypass the Forged Email Detection content filter in **Mail Policies > Address Lists**. You can use this exception list in the Forged Email Detection rule if you want the appliance to skip email addresses from the configured content filter.
New Walkthroughs available on the How-Tos Widget	The How-Tos is a contextual widget that provides in-app assistance to users in the form of walkthroughs to accomplish complex tasks on your appliance. The following are the walkthroughs that are added in this release: • Single Sign-On Using SAML 2.0 • Remediate Malicious Messages in the Mailboxes Using Mailbox Auto Remediation • Provide a Safe View of Malicious or Suspicious Message Attachments. • Configure Unified Common Event Format (CEF) Logging. The list of walkthroughs is cloud updateable. Make sure that you clear your browser cache to view an updated version of the How-Tos widget and pop-up window. For more information, see the "Accessing the Appliance" chapter in the user guide or online help and the CLI Reference Guide for AsyncOS for Cisco Email Security Appliances. To view the list of How-Tos supported in each release, see Walkthroughs Supported in AysncOS for Cisco Email Security Appliances.

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**.
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.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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.
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, SBRS Score and Policy Match details.	-

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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, SBRS Score and Policy Match in Message Details	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is displayed in the Message Details section, on the appliance.	Sender Groups, Sender IP, SBRS 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 13.

Knowledge Base

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 Cloud Email Security appliances. 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 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://tools.cisco.com/RPF/register/register.do%20

Related Topics

- Cisco Notification Service , on page 11
- Knowledge Base, on page 12

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 Email Security 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 Email Security appliance 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 Security 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 Email Security appliances.

Related Topics

- Supported Languages, on page 14

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