Getting Started with Cisco Email Security

This chapter contains the following sections:

What's New in AsyncOS 12.5

Table 1: Whats New in AsyncOS 12.5

Feature	Description
New Hardware Support	The AsyncOS 12.5 release for Cisco Email Security appliances supports the following hardware models: • C195 • C395 • C695 • C695F For more information, see https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet_c22-739910.html.
Improved Advanced Malware Protection (AMP) Quarantine Management	During the AMP engine scanning process, an attachment that receives an unknown verdict from the File Reputation service is sent for a pre-classification check and file analysis. During the pre-classification check phase, the message is now stored locally in your Email Security appliance and then sent to the Centralized Quarantine only when the attachment is sent for a complete file analysis. This improves the performance and reduces the overall load on the centralized quarantine.

Feature	Description
Ability to consume External Threat Feeds	You can now configure your Cisco Email Security appliance to consume external threat information in STIX format communicated over TAXII protocol. The ability to consume external threat information in the Cisco Email Security appliance, helps an organization to: • Proactively respond to cyber threats such as, malware, ransomware, phishing attacks, and targeted attacks. • Subscribe to external threat feeds or other devices on your organization's network that is capable of fetching external threat feeds in STIX format communicated over a TAXII protocol, and consume the threat information in your appliance. • Import dynamic information (for example, a dynamic list of URLs) in your appliance and configure mail policies or define message actions based on the dynamic information. • Improve the efficacy of the Cisco Email Security appliance. If you are using the Classic licensing mode and you do not have an External Threat Feeds feature key, you must contact the Cisco Global Licensing Operations (GLO) team to obtain the feature key as follows: **1.** Send an email to the GLO team (licensing@cisco.com) with the message subject as "Request for External Threat Feeds Feature Key", and provide your Product Authorization Key (PAK) file and Purchase Order (PO) details in the email. **2.** The GLO team provisions the feature key manually, and sends you an email with the license key to install on your appliance. **Note** If you switch to the Smart Licensing mode on your appliance, you are automatically provided with an External Threat Feeds feature key. For more information, see Configuring Email Gateway to Consume External Threat Feeds and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.

Feature	Description
Filtering Messages using Sender's Domain Reputation	Cisco Sender Domain Reputation (SDR) is a cloud service that provides a reputation verdict for email messages based on a sender's domain and other attributes The domain-based reputation analysis enables a higher spam catch rate by looking beyond the reputation of shared IP addresses, hosting or infrastructure providers, and derives verdicts based on features associated with fully qualified domain names (FQDNs) and other sender information in the SMTP conversation and message headers. For more information about SDR, contact Cisco Talos Security Intelligence and Research Group (Talos) at https://www.talosintelligence.com. For more information, see Sender Domain Reputation Filtering and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*..
Viewing malicious messages based on the threat name	In Message Tracking, you can now search for incoming or outgoing messages detected as malicious by the AMP engine based on the threat name. For more information, see Tracking Messages.
Enhancing User Experience using How-Tos Widget	The How-Tos is a contextual widget that provides in-app assistance to user in the form of walkthroughs to accomplish complex tasks on your appliance. **Note** 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 and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Support for Cisco AMP Threat Grid Clustering for File Analysis	You can now add standalone or clustered Cisco AMP Threat Grid appliances for file analysis in any one of the following ways: • **Security Services** > **File Reputation and Analysis** page in the web interface. See the File Reputation Filtering and File Analysis. • `ampconfig` command in the CLI. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.

Feature	Description
Configuring Threshold Settings for File Analysis	You can now set the upper threshold limit for the acceptable file analysis score. The files that are blocked based on the Threshold Settings are displayed as **Custom Threshold** in the **Incoming Malware Threat Files** section of the Advanced Malware Protection report. For more information, see File Reputation Filtering and File Analysis.
Viewing malicious messages based on the threat name	In Message Tracking, you can now search for incoming or outgoing messages detected as malicious by the AMP engine based on the threat name. For more information, see Tracking Messages.
DNS-based Authentication of Named Entities (DANE) support for Outgoing TLS Connections	You can now securely send messages to a valid recipient domain by enabling DNS-based Authentication of Named Entities (DANE) for your outgoing TLS connections on your appliance. The ability to securely send messages to the valid recipient domain helps an organization to ensure that business critical and confidential information is delivered to the intended recipient, provided the destination domain supports DANE. For more information, see Encrypting Communication with Other MTAs.

Feature	Description
Support for Smart Software Licensing	Smart Software Licensing enables you to manage and monitor Cisco Email Security appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM), which is the centralized database that maintains the licensing details of all the Cisco products that you purchase and use. The following are the advantages when you switch from the Classic Licensing mode to the Smart Licensing mode on your appliance: • You can handle the Product Authorization Key (PAK) licenses between the physical and virtual appliances easily, which was difficult in the Classic Licensing mode. • You can easily migrate the software licenses between devices or virtual accounts in your organization. • You do not need to manage or keep a copy of the PAK files on your appliance. • You can restrict the user access on the Smart Licensing account. **Caution** After you enable the Smart Licensing feature on your appliance, you will not be able to roll back from Smart Licensing to Classic Licensing mode. For more information, see System Administration and the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Forged Email Detection	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 List**. 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. For more information, see the “Content Filters” chapter in the user guide.

Feature	Description
Log Subscription Enhancement	You can use the Rate Limit option to configure the maximum number of logged events in the log file, within the specified time range (in seconds). The default time range value is 10 seconds. Use the **System Administration > Log Subscriptions** page in the web interface or the logconfig command in CLI to set the rate limit. For more information, see the "Logging" chapter in the user guide.
Configuring content and message filters to handle messages that skipped DMARC verification	You can configure your appliance to take actions on the messages that skipped the DMARC verification. Use the following settings in the Other Header content filter to categorize the messages that skipped the DMARC verification: • Add the Header Name as X-Ironport-Dmarc-Check-Result • Select Header Value, choose Equals, and add any one of the following values - validskip, invalidskip, temperror, and permerror The following is an example of a message filter rule syntax that is used to categorize a message that skipped the DMARC verification: Quarantine_messages_DMARC_skip: if(header("X-Ironport-Dmarc-Check-Result") == "^validskip$") { quarantine("Policy"); } For more information on the header values used in the content and message filters, contact Cisco TAC.
Ability to view or delete Cisco Content Security Management appliance connection parameters and host keys	You can now view or delete the Cisco Content Security Management appliance connection parameters and host keys in your appliance by using the `smaconfig` CLI command.

Feature	Description
Intelligent Multi-Scan Enhancement	Intelligent Multi-Scan (IMS) is a high performant multi-layer anti-spam solution. Email Security appliance provides an updated IMS engine with this release. This engine has a different combination of anti-spam engines that can increase the spam catch rates. To use the updated IMS engine, you must add the IMS feature key and accept the license in your appliance. For the existing IMS users, all the mail policies for IMS are migrated to work seamlessly with the updated IMS engine. For more information, see Managing Spam and Graymail.
Minimum Scores for Entity-based Rules of Custom Classifiers for Custom DLP Policies	You can now use the recommended minimum scores or choose to override the minimum score for entity-based rules, when you create custom classifiers for custom DLP policies. You can use the minimum score for an entity-based rule instead of the configured weight of the rule. The minimum score differentiates the partial and the full matches, and calculates the score accordingly. This helps in reducing the number of false positives and false negatives. To configure the minimum score: 1. Go to **Mail Policies > DLP Policy Customizations > Custom Classifiers Settings** section and select the **Use recommended minimum scores for entity-based rules** check box. 2. Go to **Mail Policies > DLP Policy Customizations > Add Custom Classifier** (or review an existing custom classifier) and enter the minimum score. For more information, see Data Loss Prevention.

Where to Find More Information

Cisco offers the following resources to learn more about your appliance :

- Documentation , on page 8
- Training, on page 8
- Cisco Notification Service , on page 9
- Knowledge Base, on page 9

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 10.

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://idreg.cloudapps.cisco.com/idreg/register.do

Related Topics

- Cisco Notification Service , on page 9
- Knowledge Base, on page 9

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 11

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