Getting Started with Cisco Secure Email Gateway

This chapter contains the following sections:

What's New in AsyncOS 14.0

Table 1: Whats New in AsyncOS 14.0

Feature	Description
Integrating the Cisco Secure Email Gateway with Cisco Secure Awareness Cloud Service	The Cisco Secure Awareness cloud service allows you to effectively deploy phishing simulations, awareness training, or both to measure and report results. It empowers the security operations team to focus on real-time threats and not end-user mitigation. The Cisco Secure Awareness cloud service provides reports of Repeat Clickers - users who repeatedly click on any URL or attachment sent through emails. These users are identified via a phishing simulation campaign defined by the Cisco Secure Awareness cloud service. The ability to integrate your email gateway with the Cisco Secure Awareness cloud service helps an organization to: • Improve user awareness towards real-world phishing attacks. • Allow email administrators to configure stringent policies for set of users identified as “Repeat Clickers” by the Cisco Secure Awareness cloud service. For more information, see Integrating Email Gateway with Cisco Secure Awareness Cloud Service.

Feature	Description
Improved Phishing Detection in Email Gateway	The following are the enhancements made to improve phishing detection in your email gateway: • Sender Domain Reputation Filtering Enhancement • Default Scanning of URLs in Message Attachments **Sender Domain Reputation Filtering Enhancement**: You can configure your email gateway to block messages based on the SDR (Sender Domain Reputation) verdict at the SMTP conversation level. You can enable or disable SDR verification using the Mail Flow Policy configuration settings. **Note** By default, SDR verification is enabled for incoming mail flow policies and disabled for outgoing mail flow policies. **Default Scanning of URLs in Message Attachments**: By default, the email gateway scans URLs in message attachments for any malicious content early in the email pipeline (before the Anti-Spam engine). The ability to block messages based on the SDR verdict at the SMTP conversation level and default scanning of URLs in message attachments helps an organization to: • Improve efficacy detection in phishing and domain spoofing. • Detect phishing attacks early in the email pipeline based on the default action taken on the SDR reputation verdict. For more information, see Sender Domain Reputation Filtering and Defining Which Hosts Are Allowed to Connect Using the Host Access Table.

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, and French.
	
	You can create user-defined passphrases to open password-protected attachments in incoming or outgoing messages in any one of the following ways:
	
	• Security Services > Scan Behavior page in the web interface.
	
	• `scanconfig > protectedattachmentconfig` sub command in the CLI.
	
	In this release, the Content Scanner can scan the contents of password-protected attachments of the following file types only:
	
	• Adobe Portable Document Format (PDF) files.
	
	• MS Office file types:
	
	  • Word - .doc file format that supports 2002 to 2004 version and .docx file format that supports 2007 to 2016 version.
	
	  • Excel - .xls and .xlsx file formats that support 2007 to 2016 version.
	
	  • PowerPoint - .ppt or .pptx file formats that support 2007 to 2016 version.
	
	• Archive file types - .zip format.
	
	For more information, see Using Message Filters to Enforce Email Policies.

Feature	Description

Simple Network Management Protocol (SNMP) Enhancementss	The following are the enhancements made to the SNMP configuration settings:
	• Added new SNMP MIBs for additional monitoring.
	• Support for SNMPv3 traps:
	  • SNMPv3 supports all the three security levels – noAuthNoPriv, authNoPriv and authPriv.
	  • When both SNMPv3 and SNMPv2 are enabled, you need to select the required version for traps.
	  • A new option is added under `snmpconfig` CLI command to select the trap version when both SNMPv2 and SNMPv3 are enabled.
	
	For more information, see Managing and Monitoring Using the CLI .

New Report for mail policy details	A new report – **Mail Policy Details** is added in the new web interface of your email gateway. Use this report to view the number of messages that match a configured mail policy. For more information, see Using Email Security Monitor.
New Message Tracking Filter for mail policy details	A new message tracking filter -**Mail Policy** is added in the Message Tracking > Advanced Search > Message Event option in the new web interface of your email gateway. Use this option to search for incoming or outgoing messages that match the configured mail policy name entered in the 'Mail Policy Name' field.

Feature	Description
Enhanced Overview and Incoming Mail reporting pages	The following are the enhancements made to the Overview and Incoming Mail reporting pages in the legacy web interface of your email gateway: **Overview** report page: • Added new message category – Stopped by Domain Reputation Filtering in the Incoming Mail Summary section. • Changed Stopped by Reputation Filtering message category name to Stopped by IP Reputation Filtering in the Incoming Mail Summary section. **Incoming Mail** report page: • Added new column – Stopped by Domain Reputation Filtering in the Incoming Mail Details section. • Changed Stopped by Reputation Filtering column name to Stopped by IP Reputation Filtering in the Incoming Mail Details section. For more information, see Using Email Security Monitor.
Enhanced Mail Flow Summary and Mail Flow Details reporting pages	The following are the enhancements made to the Mail Flow Summary and Mail Flow Details reporting pages in the new web interface of your email gateway: **Mail Flow Summary** report page: • Added new category – Stopped by Domain Reputation Filtering in the Threat Messages graph section. • Changed Stopped by Reputation Filtering category name to Stopped by IP Reputation Filtering in the Threat Messages graph section. • Added new column – Stopped by Domain Reputation Filtering in the Threat Detection Summary section. • Changed Stopped by Reputation Filtering column name to Stopped by IP Reputation Filtering in the Threat Detection Summary section. **Mail Flow Details** report page: • Added new column – Stopped by Domain Reputation Filtering in the Incoming Mails section for IP Addresses, Domains, and Network Owners. • Changed Stopped by Reputation Filtering column name to Stopped by IP Reputation Filtering in the Incoming Mails section for IP Addresses, Domains, and Network Owners.

Feature	Description
Support for Internationalized Domain Name (IDN)	Cisco Secure Email Gateway can now receive and deliver messages with email addresses that contain IDN domains. Currently, your email gateway provides support of IDN domains for the following languages only: • **Indian Regional Languages**: Hindi, Tamil, Telugu, Kannada, Marati, Punjabi, Malayalam, Bengali, Gujarati, Urdu, Assamese, Nepali, Bangla, Bodo, Dogri, Kashmiri, Konkani, Maithili, Manipuri, Oriya, Sanskrit, Santali, Sindhi, and Tulu. • **European and Asian Languages**: French, Russian, Japanese, German, Ukrainian, Korean, Spanish, Italian, Chinese, Dutch, Thai, Arabic, and Kazakh. For more information, see System Administration.
Security Enhancements	AsyncOS 14.0 includes the following security enhancements: • The email gateway now sends the Cisco Technical Support requests over TLS. If your SMTP server is not using TLS, the requests are sent as plain text. • You can now configure your email gateway to send alerts over TLS. Use the following subcommand in the CLI to configure this functionality: `alertconfig > SETUP > Do you want to enable TLS support to send alert messages?.` For more information, see the CLI Reference Guide associated with this release.
New Remediation Report Status Widget	A new widget - 'Remediation Report Status' is added when you search and remediate messages in the Message Tracking page of the new web interface of your email gateway. Use this widget to check the status of the Remediation Report generation. For more information, see Remediating Messages in Mailboxes

Feature	Description
Support for New Content Matching Classifiers - National Identification Numbers for Southeast Asian countries	You can create a DLP policy using any one of the following new content matching classifiers - National Identification Numbers for Southeast Asian countries: • Indonesia KTP • Malaysia MyKad • Thailand ID • Philippines UMID • Singapore NRIC You can select the new content matching classifiers in the following pages of the web interface in your email gateway: • Go to Mail Policies > DLP Policy Manager > Add Custom Policy page > Predefined Custom Classifiers > **Policy Matching Details** option. • Go to Mail Policies > DLP Policy Manager > Add Custom Policy page > Create Custom Classifier > **Entity rule** option. • Go to Mail Policies > DLP Policy Manager >Add DLP Policy page > **Privacy Protection template** option. • Go to Mail Policies > DLP Policy Customizations > Add Custom Classifier page > **Entity rule** option.
Bias-Free Terminology Usage in Product and Related Documentation	We have removed the bias terms in the product and related documentation. The following are the list of bias terms replaced with the new bias-free terms: • whitelist' term replaced with 'allowed list' term • blacklist' term replaced with 'blocked list' term • master' term replaced with 'primary' term • slave' term replaced with 'secondary' term • blackhole' term replaced with 'sink hole' term

Feature	Description
Rebranded Product and Related Documentation	We have rebranded the product and related documentation as follows: • Cisco Email Security Appliance changed to *Cisco Secure Email Gateway* • Cisco Cloud Email Security Appliance changed to *Cisco Secure Email Cloud Gateway* • Cisco Content Security Management Appliance changed to *Cisco Secure Email and Web Manager*
AMP Upstream Proxy Settings for File Analysis	You can now configure an upstream proxy for file analysis. For more information, see File Reputation Filtering and File Analysis
Performing Remedial Actions on Messages in Cisco SecureX Threat Response	In Cisco SecureX Threat Response, you can now investigate and apply the following remedial actions on messages processed by your email gateway: • Delete • Forward • Forward and Delete For more information, see Integrating with Cisco SecureX Threat Response
Content Filter - Attachment File Info condition and Strip by Attachment File Info action Enhancements	A new option - **File Hash List** is added in the Content Filters - “Attachment File Info” condition and “Strip by Attachment File Info” action. Use this option to configure a content filter to take action on message attachments that match a specific file SHA-256 value in the selected file hash list. **Note** You can also configure this functionality using message filters. For more information, see Content Filters and Using Message Filters to Enforce Email Policies.

Feature	Description
Smart Software Licensing Enhancements	AsyncOS 14.0 includes the following smart software licensing enhancements: • In a clustered configuration, you can now enable smart software licensing and register all the machines simultaneously with the Cisco Smart Software Manager. • After you enabled smart software licensing and registered your email gateway with the Cisco Smart Software Manager, the Cisco Cloud Services portal is automatically enabled and registered on your email gateway. • If the Cisco Cloud Services certificate is expired, you can now download a new certificate from the Cisco Talos Intelligence Services portal using the `cloudserviceconfig` > `fetchcertificate` sub command in the CLI. • You can view details of the smart account created in the Cisco Smart Software Manager portal using the `smartaccountinfo` command in the CLI. For more information, see System Administration and Integrating with Cisco SecureX Threat Response.
No Support for Sender Domain Age functionality post AsyncOS 14.0 Release	There will be no support for the Sender Domain Age functionality post the AsyncOS 14.0 release. The Sender Domain Age functionality will be replaced with the Sender Maturity feature. Sender Maturity represents the Cisco Talos view of how mature a domain is as an email sender. The maturity value is tuned to enable threat detection regarding emails and generally does not reflect the domain age represented in "Whois-based domain age." Sender Maturity is set to a limit of 90 days, and beyond this limit, a domain is considered mature as an email sender, and no further details is provided. Sender Maturity is used to calculate the sender reputation. Immature domains are assigned lower reputation. Cisco Talos recommends you rely on sender reputation only for determining policy actions. Sender Maturity is exposed to fine-tune filters for specific, non-standard scenarios. **Note** Cisco Talos does not manually adjust maturity for domains but relies on automated systems and sensors to determine the most appropriate value.
Alert or Notification Banner for End-of-Life (EOL) or End-of-Service (EOS) AsyncOS Version or Hardware Model	You will now receive an alert or notification banner message on your email gateway web interface or CLI, if your email gateway is running on an End-of-Life (EOL) or End-of-Service (EOS) AsyncOS version or hardware model.

Feature	Description
Office 365 or Hybrid (Graph API) Remediation Account Profile Configuration Enhancement	You can now validate the client credentials for the Office 365 or Hybrid (Graph API) remediation account profile using the Client Secret value of the application generated on the Azure Management Portal. For more information, see Remediating Messages in Mailboxes .
Virtual Email Gateway Support for Amazon Web Services (AWS)	You can deploy Cisco Secure Email Virtual Gateway on Amazon Elastic Compute Cloud (EC2) on Amazon Web Services (AWS). Contact your Cisco sales representative with your AWS account details (username and region) to provision an AMI image.
Consolidated Event Logs Enhancement	Following are the enhancements made to the 'Consolidated Event Logs' log type: • A new log field - Message Size is added in the Consolidated Event Logs log type to view the message size in the single log line output. • You can now view the size of the attachment in the message in a single log line output **Steps**: **1.** Select the 'File(s) Details' log field when configuring the log subscription for the Consolidated Event Logs. **2.** Configure a message filter rule as follows : `Custom_ Log_Entry: if (true) { log-entry("$filesizes"); }` OR Configure the **Add Log Entry** content filter action by adding the customized text as '`$filesizes`.'
Support for Cloud Connector Logging	The email gateway now supports a new type of log subscription - **Cloud Connector Logs**. Use this log subscription to view information about Web Interaction Tracking data from Cisco Aggregator Server. Most of the information is present at the Info or Warning Level

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 email gateway sends the file reputation queries to the AMP server. If the email gateway 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 email gateway to receive responses when there are network latencies, issues related to the AMP server, and so on.
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 gateway 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.
Authentication Logs Enhancement	You can now view the user privilege role details (for example, ‘admin,’, ‘operator,’ and so on) of the logged-in user in the authentication logs.

Feature	Description
New Passphrase Rule for defining login passphrases	A new passphrase rule is added in your email gateway to define your login passphrase: `Avoid usage of passphrases that contain three or more repetitive or sequential characters, (for example, 'AAA@124,' 'Abc@123,' and so on.)` You can configure this passphrase rule in any one of the following ways: • System > Administration > Users > Local User Account & Passphrase Settings > **Reject three or more repetitive or sequential characters in passphrases** check box in the web interface. • `userconfig` > `POLICY` > `PASSWORDSTRENGTH` > `Reject passphrases that contain three or more repetitive or sequential characters? [Y]>` command in the CLI
Creating system-generated passphrases	In addition to creating a login passphrase manually, you can now also create a system-generated passphrase to log in to your email gateway. You can configure the system-generated passphrase in any one of the following ways: • Options > Change Passphrase page in the web interface. • System Administration > System Setup Wizard page in the web interface. • System Administration > Users > Add Local User page in the web interface. • `passphrase` or `passwd` commands in the CLI For more information, see Setup and Installation.
Performing FQDN Validation for Certificates	You can configure your email gateway to perform FQDN validation for certificates in the following scenarios: • Importing a custom certificate. • Creating a self-signed S/MIME certificate. • Creating a self-signed certificate. • Importing a custom Certificate Authority (CA) list. **Note** You can also perform FQDN validation for email gateway certificates that contain IDN domains. For more information, see S/MIME Security Services and Encrypting Communication with Other MTAs.

Feature	Description
Performing FQDN Validation for Peer Certificate during SSL Communication	You can configure your email gateway to perform FQDN validation for peer certificate in System Administration > SSL Configuration page in the web interface. The FQDN validation is applicable for the following services: • Outbound SMTP • LDAP • Updater • Alert over TLS **Note** You can perform FQDN validation for peer certificates that contain IDN domains for the Outbound SMTP services only. For more information, see System Administration.
Performing x509 Validation for Peer Certificate during SSL Communication	You can configure your email gateway to perform x509 validation for peer certificate in System Administration > SSL Configuration page in the web interface. The x509 validation is applicable for the following services: • Outbound SMTP • LDAP • Updater • Alert over TLS For more information, see System Administration.
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 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 19.

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 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 17
- Knowledge Base, on page 17

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 20

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