



Getting Started with Cisco Secure Email Gateway

This chapter contains the following sections:

- [What's New in AsyncOS 14.2, on page 1](#)
- [Comparison of Web Interfaces, New Web Interface with Legacy Web Interface , on page 4](#)
- [Where to Find More Information, on page 6](#)
- [Cisco Secure Email Gateway Overview, on page 9](#)

What's New in AsyncOS 14.2

Table 1: Whats New in AsyncOS 14.2

Feature	Description
URL Retrospective Verdict and URL Remediation	<p>The URLs with unknown reputation can turn malicious anytime, even after it has reached the user's mailbox. You can configure URL filtering on your email cloud gateway to send alerts based on the URL retrospective verdicts received from Talos. You can also configure your email gateway to perform auto-remedial actions on the messages in user mailbox when the URL verdict changes from unknown to malicious.</p> <p>For more information, see chapter Protecting Against Malicious or Undesirable URLs.</p>

Feature	Description
Sender Maturity	<p>In this release, the legacy Sender Domain Reputation (SDR) Domain Age functionality is replaced with Sender Maturity. Sender Maturity is an important feature to establish sender reputation. Sender Maturity is automatically generated for spam classification based on multiple sources of information and can differ from “Whois-based domain age.”</p> <p>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.”</p> <p>Sender Maturity is set to a limit of 30 days, and beyond this limit, a domain is considered mature as an email sender, and no further details are provided.</p> <p>Note From this release onwards, the 'SDR Domain Age' configured filters are automatically updated to the 'SDR Sender Maturity' filters. The filters with an invalid value for Sender Maturity are marked as 'inactive' after the upgrade. Make sure you review and modify the message and content filters accordingly.</p> <p>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.</p> <p>Note Cisco Talos does not manually adjust maturity for domains but relies on automated systems and sensors to determine the most appropriate value.</p> <p>For more information, see Sender Domain Reputation Filtering.</p>

Feature	Description
New Sender Domain Reputation Verdicts	<p>From this release onwards, the Sender Domain Reputation verdicts are updated to accurately reflect the intended meaning and recommended usage.</p> <p>During the upgrade, the system automatically updates the Sender Domain Reputation message or content filter configurations to reflect the new verdicts. Make sure you review and configure the message or content filters accordingly.</p> <p>For more information about the recommended actions, you can take for each new SDR verdict, see the "SDR Verdicts" section in Sender Domain Reputation Filtering.</p> <p>After you upgrade to AsyncOS 14.2.x release, the legacy SDR verdicts in the content or message filters, reporting, and message tracking are replaced with the new SDR verdicts as follows:</p> <ul style="list-style-type: none"> • Untrusted • Questionable • Neutral • Favorable • Trusted • Unknown <p>Note The SDR Reporting and Tracking AsyncOS APIs are updated to reflect the new SDR Threat Level and Category structure.</p> <p>Note The SDR Mail and Tracking Logs are updated to reflect the new SDR Threat Levels and Sender Maturity details.</p> <p>For more information, see Sender Domain Reputation Filtering.</p>
Sender Domain Reputation (SDR) Filtering Improvements	<p>In this release, the user experience and overall quality of the SDR service is enhanced with performance improvements, increased availability, and deployment of SDR.</p>

Feature	Description
TLS Certificate Enhancement for Destination Control	<p>You can now choose a different certificate other than the certificate configured in the 'Default' destination control entry for specific domains.</p> <p>You can choose a different certificate in any one of the following ways:</p> <ul style="list-style-type: none"> • Edit the corresponding destination control entry and select a different certificate using the TLS certificate option in the web interface. • Use the <code>destconfig > new</code> or <code>edit</code> sub commands in the CLI to select a certificate when you create or edit a destination control entry. <p>For more information, see Controlling TLS.</p>
Modification of Classic Licensing - Expiration Date in Web Interface and CLI	<p>From this release onwards, the existing 'Expiration Date' column header in the web interface and CLI for classic licensing is modified as follows – “<i>Expiration Date (including grace period)</i>” to indicate that the grace period is included in the expiration date.</p> <p>Note All alert messages and mail logs are modified to display the expiration date, including the grace period for a feature key.</p>

Comparison of Web Interfaces, New Web Interface with Legacy Web Interface

The following table shows the comparison of the new web interface with the legacy interface:

Table 2: Comparison of New Web Interface with legacy interface

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Landing Page	After you log in to the email gateway, the Mail Flow Summary page is displayed.	After you log in to the email gateway, the My Dashboard page is displayed.
Reports Drop-down	You can view reports for your email gateways from the Reports drop-down.	You can view reports for your email gateway from the Monitor menu.
My Reports Page	Choose My Reports from the Reports drop-down.	You can view the My Reports page from Monitor > My Dashboard .
Mail Flow Summary Page	The Mail Flow Summary page includes trend graphs and summary tables for incoming and outgoing messages.	The Incoming Mail includes graphs and summary tables for the incoming and outgoing messages.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Advanced Malware Protection Report Pages	<p>The following sections are available on the Advanced Malware Protection report page of the Reports menu:</p> <ul style="list-style-type: none"> • Summary • AMP File Reputation • File Analysis • File Retrospection • Mailbox Auto Remediation 	<p>The email gateway has the following Advanced Malware Protection report pages under Monitor menu:</p> <ul style="list-style-type: none"> • Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Mailbox Auto Remediation
Outbreak Filters Page	<p>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.</p>	<p>The Monitor > Outbreak Filters page displays the Past Year Virus Outbreaks and Past Year Virus Outbreak Summary.</p>
Spam Quarantines (Administrative and End Users)	<p>Click Quarantine > Spam Quarantine > Search in the new web interface.</p> <p>The end users can access the spam quarantine using the URL:</p> <p><code>https://example.com:<https-api-port>/eq-login</code></p> <p>where <code>example.com</code> is the appliance hostname and <code><https-api-port></code> is the AsyncOS API HTTPS port opened on the firewall.</p>	<p>You can view spam quarantine from the Monitor > Spam Quarantine menu.</p>
Policy, Virus and Outbreak Quarantines	<p>Click Quarantine > Other Quarantine in the new web interface.</p> <p>You can only view Policy, Virus and Outbreak Quarantines in the new web interface.</p>	<p>You can view, configure and modify the Policy, Virus and Outbreak Quarantines on the email gateway using the Monitor > Policy, Virus and Outbreak Quarantines.</p>
Select All Action for Messages in Quarantine	<p>You can select multiple (or all) messages and perform a message action such as delete, delay, release, move, etc.</p>	<p>You cannot select multiple messages to perform a message action.</p>
Maximum Download Limit for Attachments	<p>The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.</p>	-

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Rejected Connections	To search for rejected connections, click Tracking > Search > Rejected Connection tab on the .	-
Query Settings	The Query Settings field of the Message Tracking feature is not available on the .	You can set the query timeout in the Query Settings field of the Message Tracking feature.
Message Tracking Data Availability	Click the gear icon on the upper right side of the page the web interface to access Message Tracking Data Availability page.	You can view the missing-data intervals for your email gateway.
Show Additional Details of Messages	You can view additional details of a message such as Verdict Charts, Last State, Sender Groups, Sender IP, IP Reputation Score and Policy Match details.	-
Verdict Charts and Last State Verdicts	Verdict Chart displays information of the various possible verdicts triggered by each engine in your email gateway. Last State of the message determines the final verdict triggered after all the possible verdicts of the engine.	Verdict Charts and Last State Verdicts of the messages are not available.
Message Attachments and Host Names in Message Details	Message attachments and host names are not displayed in the Message Details section of the message on the email gateway.	Message attachments and host names are displayed in the Message Details section of the message.
Sender Groups, Sender IP, IP Reputation Score and Policy Match in Message Details	Sender Groups, Sender IP, IP Reputation Score, and Policy Match details of the message is displayed in the Message Details section, on the email gateway.	Sender Groups, Sender IP, IP Reputation Score, and Policy Match of the message is not available in the Message Details section of the message.
Direction of the Message (Incoming or Outgoing)	Direction of the message (incoming or outgoing) is displayed in the message tracking results page, on the email gateway.	Direction of the message (incoming or outgoing) is not displayed in the message tracking results page.

Where to Find More Information

Cisco offers the following resources to learn more about your email gateway:

- [Documentation](#) , on page 7

- [Training](#), on page 7
- [Cisco Notification Service](#) , on page 8
- [Knowledge Base](#), on page 8
- [Cisco Support Community](#), on page 8
- [Cisco Customer Support](#), on page 8
- [Third Party Contributors](#), on page 9
- [Cisco Welcomes Your Comments](#), on page 9
- [Registering for a Cisco Account](#) , 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 Secure Email Gateway includes the following documents and books:

- Release Notes
- Quick Start Guide for your Cisco Email Security Appliance model
- Hardware Installation or Hardware installation and maintenance guide for your model or series
- *Cisco Content Security Virtual Appliance Installation Guide*
- *User Guide for AsyncOS for Cisco Secure Email Gateway* (this book)
- *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*
- AsyncOS API for Cisco Secure Email Gateway - Getting Started Guide

Documentation for all Cisco Content Security products is available from:

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.
Cisco Email Security	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco Web Security	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Content Security Management	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
CLI reference guide for Cisco Content Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort Encryption	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

Training

More information about training is available from:

- <http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html>
- <http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html>

Cisco Notification Service

Sign up to receive notifications relevant to your Cisco Content Security Appliances, such as Security Advisories, Field Notices, End of Sale and End of Support statements, and information about software updates and known issues.

You can specify options such as notification frequency and types of information to receive. You should sign up separately for notifications for each product that you use.

To sign up, visit <http://www.cisco.com/cisco/support/notifications.html>

A Cisco.com account is required. If you do not have one, see [Registering for a Cisco Account](#) , on page 9.

Knowledge Base

Procedure

- Step 1** Go to the main product page (<http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html>)
- Step 2** Look for links with **TechNotes** in the name.
-

Cisco Support Community

The Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general email and web security issues, as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community on the Customer Support Portal at the following URLs:

- For email security and associated management:
<https://supportforums.cisco.com/community/5756/email-security>
- For web security and associated management:
<https://supportforums.cisco.com/community/5786/web-security>

Cisco Customer Support

Do not contact Cisco Customer Support for help with Cisco Secure Email Cloud Gateway. See the Cisco IronPort Hosted Email Security / Hybrid Hosted Email Security Overview Guide for information on getting support for Cloud/Hybrid Email Security appliances.

Cisco TAC: <http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Support site for legacy IronPort: <http://www.cisco.com/c/en/us/services/acquisitions/ironport.html>

For non-critical issues, you can also access customer support from the email gateway. For instructions, see the User Guide or online help.

Third Party Contributors

See Open Source licensing information for your release on this page:

<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html> .

Some software included within Cisco AsyncOS is distributed under the terms, notices, and conditions of software license agreements of FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc., and other third party contributors, and all such terms and conditions are incorporated in Cisco license agreements.

The full text of these agreements can be found here:

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.

Portions of the software within Cisco AsyncOS is based upon the RRDtool with the express written consent of Tobi Oetiker.

Portions of this document are reproduced with permission of Dell Computer Corporation. Portions of this document are reproduced with permission of McAfee, Inc. Portions of this document are reproduced with permission of Sophos Plc.

Cisco Welcomes Your Comments

The Cisco Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address:

contentsecuritydocs@cisco.com

Please include the product name, release number, and document publication date in the subject of your message.

Registering for a Cisco Account

Access to many resources on Cisco.com requires a Cisco account.

If you do not have a Cisco.com User ID, you can register for one here: <https://idreg.cloudapps.cisco.com/idreg/register.do>

Related Topics

- [Cisco Notification Service](#) , on page 8
- [Knowledge Base](#), on page 8

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 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

