



Introduction

This chapter contains the following sections:

- [What's New in this Release, on page 1](#)
- [Changes in Behavior, on page 7](#)
- [Comparison of Web Interfaces with Previous Releases, on page 8](#)
- [Cisco Content Security Management Overview, on page 12](#)

What's New in this Release

This section describes the new features and enhancements in this release of AsyncOS for Cisco Content Security Management. For more information about the release, see the product release notes, which are available at the following URL:

<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html>.

If you are upgrading, you should also review release notes for other releases between your former release and this release, in order to see the features and enhancements that were added in those releases.

Table 1: What's New in AsyncOS 12.5

Feature	Description
Using Sub Configuration Masters	You can now configure subsets of a particular version of the Configuration Master to centrally manage the different policy configurations of your Web Security appliance. For more information, see Managing Web Security Appliances .

Table 2: What's New in AsyncOS 12.0

Feature	Description
New Web Interface for Reporting, Quarantine and Tracking	<p>The appliance now has a new web interface to search and view:</p> <ul style="list-style-type: none"> • Email Reports. You can now view email reports from the Reports drop-down based on the following categories: <ul style="list-style-type: none"> • Email Threat Reports • File and Malware Reports • Connection and Flow Reports • User Reports • Filter Reports <p>For more information, see chapter Using Centralized Email Security Reporting.</p> <ul style="list-style-type: none"> • Spam Quarantine <ul style="list-style-type: none"> • 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. <p>For more information, see chapter Spam Quarantine.</p> <ul style="list-style-type: none"> • Policy, Virus and Outbreak Quarantines. You can view and search for policy, virus and outbreak quarantines in Quarantine > Other Quarantine > Search page in the web interface. For more information, see chapter Centralized 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 chapter Tracking Messages. <p>Important</p> <ul style="list-style-type: none"> • Make sure that you have enabled AsyncOS API on the appliance. • You must login to the legacy web interface of the appliance. • If <code>trailblazerconfig</code> is enabled, the configured HTTPS port must be 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. • If <code>trailblazerconfig</code> is disabled, the AsyncOS API ports configured in Management Appliance > Network > IP Interfaces, are opened on the firewall. The default AsyncOS API HTTP/HTTPS port is 6080/6443.

Feature	Description
The <code>trailblazerconfig</code> CLI Command	<p>You can use the <code>trailblazerconfig</code> command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.</p> <p>Note By default, <code>trailblazerconfig</code> CLI command is enabled on your appliance. You can see the inline help by typing the command: <code>help trailblazerconfig</code>.</p> <p>For more information, see The trailblazerconfig Command.</p>
Encrypting sensitive information on the appliance	<p>You can use the <code>adminaccessconfig > encryptconfig</code> sub command in the CLI to configure encryption of sensitive information on your appliance.</p> <p>Note By default, the encryption is disabled on the appliance.</p>
Message Tracking Enhancement	<p>You can now search for messages based on the “Reply-To” header of the message.</p> <p>For more information, see Tracking Messages.</p>
Support for new features in AsyncOS 12.0 for Cisco Email Security Appliances	<p>You can now view the following reports on the Reporting page of the Security Management appliance:</p> <ul style="list-style-type: none"> • External Threat Feeds • Sender Domain Reputation <p>For more information, see Understanding the Email Reporting Pages on the New Web Interface.</p> <p>You can now view outgoing TLS connections summary for DANE Success and DANE Failure scenarios. For more information, see section SMTP DNS-based Authentication of Named Entities of the <i>User Guide or Online Help for AsyncOS 12.0 for Cisco Email Security Appliances</i>.</p> <p>You can now use the following message events to search for messages on the Message Tracking page of the Security Management appliance:</p> <ul style="list-style-type: none"> • External Threat Feeds • Sender Domain Reputation • DANE Failure

Feature	Description
<p>Advanced Malware Protection Report Enhancements</p>	<p>The Advanced Malware Protection report page has the following enhancements:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>See Advanced Malware Protection Page.</p>

Feature	Description
New Web Interface for Web Reporting and Tracking	<p>The appliance now has a new web interface to search and view:</p> <ul style="list-style-type: none"> • Web Reports <p>You can now view web based reports from the Reports drop-down based on the following categories:</p> <ul style="list-style-type: none"> • General Reports • Threats Reports <ul style="list-style-type: none"> • Web Tracking <p>You can search for web transactions depending on your search criteria. On your Security Management appliance, click on the Web dropdown and choose Tracking > Web Tracking Search page.</p> <p>Important</p> <ul style="list-style-type: none"> • Make sure that you have enabled AsyncOS API on the appliance. • You must login to the legacy web interface of the appliance. • If <code>trailblazerconfig</code> is enabled, the configured HTTPS port must be 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. • If <code>trailblazerconfig</code> is disabled, the AsyncOS API ports configured in Management Appliance > Network > IP Interfaces, are opened on the firewall. The default AsyncOS API HTTP/HTTPS port is 6080/6443. <p>For more information, see chapter Using Centralized Web Reporting and Tracking.</p>
Metrics Bar Widget	<p>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.</p> <p>For more information, see Advanced Malware Protection Page.</p>
HTTPS Reports Page	<p>You can now view the overall aggregation of the HTTP/HTTPS traffic and the summary of the ciphers based on the client and server side connection for each HTTP/HTTPS traffic, on the HTTPS Reports report page.</p> <p>For more information, see Using Centralized Web Reporting and Tracking.</p>

Feature	Description
Integrating the Appliance with Cisco Threat Response Portal	<p>You can integrate your appliance with Cisco Threat Response portal, and perform the following actions in Cisco Threat Response portal:</p> <ul style="list-style-type: none"> • 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 in the portal to save the investigation, and enable collaboration of information among other devices on the portal. <p>For more information, see Assigning Network and IP Addresses.</p>
Web Traffic Tap Policies	<p>Cisco Content Security Management appliance now allows you to set Web Traffic Tap Policies. You can define the Web Traffic Tap Policies based on which web traffic that passes through the Web Security appliance will be tapped.</p> <p>You must enable the Web Traffic Tap feature in Web Security appliance to set Web Traffic Tap Policies in Security Management appliance.</p> <p>The Web Overview report page now includes sections on Web Traffic Tap Status, Web Traffic Tap Summary, Tapped HTTP/HTTPS Traffic, and Tapped Traffic Summary. See Web Reporting Overview.</p>
Support for the Office 365 Web Service External URL Categories feature in AsyncOS for Cisco Web Security Appliances	<p>This release supports the Office 365 Web Service External URL Categories feature in AsyncOS for Cisco Web Security Appliances.</p> <p>For more information, see Using Centralized Web Reporting and Tracking.</p>

Changes in Behavior

Change in Report Pages	<p>The following reports are changed on the new web interface, in this release:</p> <ul style="list-style-type: none"> • Overview report page is renamed to Mail Flow Summary. • Outbreak Filters report page is renamed to Outbreak Filtering. • Virus Types report page is renamed to Virus Filtering. • Advanced Malware Protection, AMP File Analysis, AMP Verdict Updates and Mailbox Auto Remediation report pages are merged as Advanced Malware Protection. • Incoming Mail and Outgoing Senders report pages are merged as Mail Flow Details. • TLS Connections report page is renamed to TLS Encryption. • Geo-Distribution report page is renamed to Connection by Country. • Internal Users report page is renamed to User Mail Summary. • Web Interaction Tracking report page is renamed to Web Interaction. <p>For more information, see Understanding the Email Reporting Pages on the New Web Interface.</p>
Changes in Spam Quarantine	<p>The administrative users can now access the Spam Quarantine page on the new web interface of the appliance.</p> <p>You can click Quarantine > Spam Quarantine > Search page to access the Spam Quarantine page.</p> <p>The end-users can now access the Spam Quarantine portal on the new web interface, For more information, see Accessing the Web Interface.</p> <p>Note Local and externally-authenticated users cannot login to the end-user spam quarantine portal.</p> <p>You will now receive spam notifications with links to the new web interface. Make sure that you have enabled AsyncOS API HTTP/HTTPS ports and HTTP/HTTPS service on the appliance.</p> <p>If you are using spam quarantine on the any other interface (Data 1), then you must set it as the default interface.</p> <p>If the <code>trailblazerconfig</code> is enabled, then you must enable the AsyncOS API ports (HTTP/HTTPS) and HTTP/HTTPS service on the (Data 1) interface. If the <code>trailblazerconfig</code> is disabled, then you must enable the AsyncOS API ports (HTTP/HTTPS) on the (Data 1) interface.</p> <p>For more information, see The trailblazerconfig Command.</p>

Encrypting Passphrases	<p>After you upgrade to this release, you can encrypt the user's passphrases when updating the configuration files on the appliance.</p> <p>To encrypt the passphrase, do one of the following:</p> <ul style="list-style-type: none"> • On the System Administration > Configuration File page, select the Encrypt passphrases in the Configuration Files checkbox. • Use the <code>saveconfig</code> command in the CLI to encrypt the passphrase.
Changing the User's Passphrase After Expiry	<p>Users are prompted to change the passphrase after the user account is expired. For more information, see Changing the User's Passphrase After Expiry.</p>
Changes in Demo Certificates	<p>Prior to this release, the appliance was pre-configured with a demonstration certificate to enable the TLS connections. After you upgrade to this release, the appliance generates a unique certificate to enable TLS connection. The existing demonstration certificate that is used in the following configurations are replaced with the new certificate:</p> <ul style="list-style-type: none"> • Mail Delivery • LDAP • Networking • URL Filtering • SMTP Services






See also: [Comparison of Web Interfaces with Previous Releases, on page 8](#).

Comparison of Web Interfaces with Previous Releases


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

Table 3: Comparison of New Web Interfaces with Previous Releases

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Landing Page	<p>After you log in to the Cloud Email Security Management Console, the Mail Flow Summary page is displayed.</p>	<p>After you log in to the appliance, the System Status page is displayed.</p>
Product Drop-down	<p>You can switch between the Email Security Appliance and the Web Security Appliance from the Product drop-down.</p> <p>For more information, see Using the Interactive Report Pages.</p>	<p>You can use the Email or Web tab to switch between the Email Security Appliance and the Web Security Appliance.</p>

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Reports Drop-down	You can view reports for your Email and Web Security Appliances from the Reports drop-down. For more information, see Using the Interactive Report Pages .	You can view reports for your Email and Web Security Appliances from the Reporting drop-down menu.
Management Appliance Tab	Click  on the Cloud Email Security Management Console to access the Management Appliance tab.	You can enable and configure reporting, message tracking and quarantines, as well as configure network access, and monitor system status.
My Reports Page	Click  on the Cloud Email Security Management Console and choose Email > Reporting > My Reports to access the My Reports page.	You can customize your reports dashboard by assembling charts (graphs) and tables from existing report pages.
Reporting Data Availability Page	Click  on the Cloud Email Security Management Console and choose Email > Reporting > Reporting Data Availability to access the Reporting Data Availability page.	You can view, update and sort data to provide real-time visibility into resource utilization and email traffic trouble spots.
Scheduling & Archiving Reports	Click  on the Cloud Email Security Management Console and choose Email > Reporting > Scheduled Reports to schedule your reports. Click  on the Cloud Email Security Management Console and choose Email > Reporting > Archive Reports to archive your reports.	You can schedule reports using the Email > Reporting > Scheduled Reports page, and archive your reports using the Email > Reporting > Archived Report page of the Security Management appliance.
Reporting Overview Page	The Email Reporting Overview page on the Security Management appliance has been redesigned as Mail Flow Summary page in the new web interface. The Mail Flow Summary page includes trend graphs and summary tables for incoming and outgoing messages.	The Email Reporting Overview page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Overview page 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	The following sections are available on the Advanced Malware Protection report page of the Reports menu: <ul style="list-style-type: none"> • Summary • AMP File Reputation • File Analysis • File Retrospection • Mailbox Auto Remediation 	The Email > Reporting drop-down menu of the Security Management appliance has the following Advanced Malware Protection report pages: <ul style="list-style-type: none"> • 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 Email > Reporting 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: <a href="https://example.com:<https-api-port>/aui-login">https://example.com:<https-api-port>/aui-login 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.	-
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.
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.	-

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 Cloud Email Security Management Console.	-
Query Settings	The Query Settings field of the Message Tracking feature is not available on the Cloud Email Security Management Console.	You can set the query timeout in the Query Settings field of the Message Tracking feature.
Message Tracking Data Availability	Click  on the Cloud Email Security Management Console and choose Email > Message Tracking > Message Tracking Data Availability 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.	-
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 Cloud Email Security Management Console	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 Cloud Email Security Management Console.	Sender Groups, Sender IP, SBRS Score, and Policy Match of the message is not available in the Message Details section of the message.

Web Interface Page or Element	New Web Interface	Legacy Web Interface
Direction of the Message (Incoming or Outgoing)	Direction of the message (incoming or outgoing) is displayed in the message tracking results page, on the Cloud Email Security Management Console.	Direction of the message (incoming or outgoing) is not displayed in the message tracking results page.

Cisco Content Security Management Overview

AsyncOS for Cisco Content Security Management incorporates the following features:

- **External Spam Quarantine:** Hold spam and suspected spam messages for end users, and allow end users and administrators to review messages that are flagged as spam before making a final determination.
- **Centralized Policy, Virus, and Outbreak Quarantines:** Provide a single interface for managing these quarantines and the messages quarantined in them from multiple Email Security appliances. Allows you to store quarantined messages behind the firewall.
- **Centralized reporting:** Run reports on aggregated data from multiple Email and Web Security appliances. The same reporting features available on individual appliances are available on Security Management appliances.
- **Centralized tracking:** Use a single interface to track email messages and web transactions that were processed by multiple Email and Web Security appliances.
- **Centralized Configuration Management for Web Security appliances:** For simplicity and consistency, manage policy definition and policy deployment for multiple Web Security appliances.



Note The Security Management appliance is not involved in centralized email management, or ‘clustering’ of Email Security appliances.

- **Backup of data:** Back up the data on your Security Management appliance, including reporting and tracking data, quarantined messages, and lists of safe and blocked senders.

You can coordinate your security operations from a single Security Management appliance or spread the load across multiple appliances.