Introduction

This chapter contains the following sections:

What's New in this Release

This section describes the new features and enhancements in this release of AsyncOS for Cisco Content Security Management.

Table 1: What's New in AsyncOS 14.1

Feature	Description
New System Health Status Dashboard	In AsyncOS 14.0, you can now view the current status and configuration of the Web Security appliance in a page. You must choose Monitoring > System Health to monitor the system status of the Web security appliances. For more information, see System Health Dashboard on the New Web Interface.
Export Tracking Data	In AsyncOS 14.1.0, export tracking has been enhanced as: • View additional fields to perform analysis and investigation on related mails using the Export file option along with message details. • When you perform an export, the maximum number of rows you can view is now set to 50000. For more information, see Exporting Message Service .
Quarantine Custom Access Role	Administrators can create custom roles with read-only option for Quarantine messages. The read-only option prevents users from deleting or releasing messages and only have read-only access to quarantine.

Feature	Description
Spam Quarantine Threshold Alert	AsyncOS 14.1.0 sends alerts when a certain number of spam messages are quarantined in a specified duration. The alerts are also entered in the syslogs on generation. In addition to this, Cisco Secure Email and Web Manager triggers an alert once the quarantine threshold is reached.
Single Pane of Glass	AsyncOS 14.1.0 enables you to save more time without having to perform multiple logins in multiple Cisco Secure Email and Web Managers. You can view the reporting, tracking, and quarantine pages of individual Cisco Secure Email and Web Manager on a primary appliance. To perform this, you can select the required Cisco Secure Email and Web Manager from the drop-down listed on the Tracking, Reporting, and Quarantine page. For more information, see Single Pane of Glass.
Smart Licensing re-registration	You can reregister your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal based on any one of the following scenarios: • If you are unable to view or manage the devices added to the Cisco Cloud Services portal when you automatically register your email gateway with the Cisco Cloud Services portal. • If your Smart Account and Cisco Cloud Services Account are not linked when you automatically register your appliance with the Cisco Cloud Services portal. For more information, see Reregistering with Cisco Cloud Service Portal.
New Parameters for Syslog Push- Log Retrieval Method	Following are the new parameters that you need to use to configure the Syslog Push log retrieval method in your Cisco Secure Email and Web Manager: • Port number of the remote Syslog server. • Maximum size of the log message that is sent to the remote Syslog server. • [For TCP protocol only]: TLS connection between Cisco Secure Email and Web Manager and the remote Syslog server.

Table 2: What's New in AsyncOS 14.0

Feature	Decsription
Enhanced Overview and Incoming Mail reporting pages	The following are the enhancements made to the Incoming Mail reporting pages in the legacy web interface of your appliance: 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 Centralized Email Security Reporting
New System Health Status Dashboard	You can now view the current status and configuration of the Web Security appliance in a page. You must choose **Monitoring** > **System Health** to monitor the system status of the Web security appliances. For more information, see System Health Dashboard on the New Web Interface.
Working with Certificates	The appliance uses stored trusted certificate authorities to verify a certificate from a remote domain to establish the credentials of the domain. You can configure the security management appliance to use the following trusted certificate authorities: • System List • Custom List For more information, see Common Administrative Tasks

Feature	Decsription
Smart Licensing	Cloud Service will be enabled and Appliance will be registered automatically when smart licensing is enabled and registered. • To enable or disable Cisco SecureX and Cisco Threat response, the option is introduced under the generalconfig command. • The command threstresponseconfig will display the warning message "Enter general config command to Enable/Disable of Cisco SecureX/ Threat Response feature". • The command smartaccountinfo is introduced for getting the Smart account information. • When you enable CloudServices, Cisco SecureX will be enabled automatically and Cisco Securex will be disabled when CloudServices is disabled. For more information, see Integrating with Cisco SecureX or Cisco Threat Response.
Enabling Cisco SecureX or Threat Response on Content Security Gateway	You must use the general configuration settings to enable Cisco SecureX or Threat Response on Content Security Gateway. For more information, see Integrating with Cisco SecureX or Cisco Threat Response.
New report for mail policy details	A new report – Mail Policy Details is added in the new web interface of your appliance. Use this report to view the number of messages that match a configured mail policy. For more information, see Using Centralized Email Security Reporting
Performing Remedial Actions on Messages in Cisco Threat Response	In Cisco Threat Response, you can now investigate and apply the following remedial actions on messages processed by your appliance: • Delete • Forward • Forward and Delete For more information, see Integrating with Cisco SecureX or Cisco Threat Response.

Feature	Decsription
Support for Internationalized Domain Name (IDN)	AsyncOS 14.0 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 Introduction, on page 1
SPAM Notification	A new field Custom Logo Position is included that enables you to add the same logo to the SPAM notification email at the given position.
Rebranded Product and Related Documentation	We have rebranded the product, and related documentation from “Cisco Content Security Management” to “Cisco Secure Email and Web Manager.”
Passphrases	A new passphrase rule is added in your Email and Web Manager to define your login passphrase: For more information, see Common Administrative Tasks
FQDN	For a X.509 certificate, the FQDN validation validates the common name field (CN) of that certificate's subject distinguished name and the subjectAltName extension of type dNSName (SAN:dNSName) For more information, see Common Administrative Tasks

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.

- **Centralized Upgrade Management:** You can simultaneously upgrade multiple Web Security appliances (WSAs) using a single Security Management Appliance (SMA).
- **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.
- **Support for Internationalized Domain Name (IDN):** AsyncOS 14.0 can now receive and deliver messages with email addresses that contain IDN domains. Currently, your content security 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 this release, you can only configure few features using IDN domains in your content security gateway.

- SMTP Routes Configuration Settings- Add or edit IDN domains, Export or import SMTP routes using IDN domains.
- Reporting Configuration Settings: View IDN data - usernames, email addresses, and domains) in the reports.
- Message Tracking Configuration Settings: View IDN data- usernames, email addresses, and domains) in message tracking.
- Policy, Virus, and Outbreak Quarantine Configuration Settings: View messages with IDN domains that may be transmitting malware, as determined by the anti-virus engine, View messages with IDN domains caught by Outbreak Filters as potentially being spam or malware, View messages with IDN domains caught by message filters, content filters, and DLP message actions.
- Spam Quarantine Configuration Settings- View messages with IDN domains detected as spam or suspected spam, Add email addresses with IDN domains to the safelist and blocklist categories.

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