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 Secure Email and Web Manager.

Table 1: What's New in AsyncOS 14.2

Feature	Description
New Sender Domain Reputation Verdicts	The Sender Domain Reputation (SDR) verdicts are updated in this release to accurately reflect the intended meaning and recommended usage. After you upgrade to AsyncOS 14.2.x release, the legacy SDR verdicts in the reporting and message tracking are replaced with the new SDR verdicts as follows: • Untrusted • Questionable • Neutral • Favorable • Trusted • Unknown The SDR reporting and message tracking results are updated with the new verdicts accordingly on upgrade. Make sure that you also upgrade your email gateway(s) to the latest 14.2 version that contains the new SDR verdicts. **Note** The SDR Reporting and Tracking AsyncOS APIs are updated to reflect the new SDR Threat Level and Category structure. **Note** The SDR Tracking Logs are updated to reflect the new SDR Threat Levels and Sender Maturity details.

Feature	Description
Managing Data Storage Time for Centralized Email Tracking Service	You can now configure your Secure Email and Web Manager to store the messages (data) in the Centralized Email Tracking database based on the number of days. You can configure this feature in any one of the following ways: • Use the **Apply Data Storage Time** option in **System Administration** > **Disk Management** > **Edit Data Disk Management** page of the legacy web interface. • Use the `Manage data based on the storage time` statement in `diskquotaconfig` > `edit` > `Centralized Email Tracking` sub command in the CLI. **Important**: From Secure Email and Web Manager 13.6.2 version, the Splunk database is no longer used for email tracking data. All new email tracking data is stored in the Lucene database. When you use this feature, the Splunk database that contains the email tracking data gets deleted automatically. **Action**: Make sure you take a backup of the email tracking data (if required). You can use the `backupconfig` command in the CLI to perform the backup action. For more information, see Scheduling Single or Recurring Backups. **Note** If your organization network has only one Secure Email and Web Manager, you need to deploy a new Virtual Machine (VM) in the network. For more information on how to deploy a virtual Secure Email and Web Manager, see Cisco Secure Email and Web Virtual Appliance Installation Guide. For more information, see Managing Data Storage Time.

Feature	Description
PVO Quarantine Threshold Alert	Secure Email and Web Manager sends an alert to the recipient when the number of PVO quarantine messages exceeds a user-defined threshold value set for a specific time duration and PVO quarantine. Secure Email and Web Manager ensures that you receive the alerts you set as an email. You can configure PVO quarantine threshold alerts, using the following ways: • Email > Message Quarantine > Policy Virus and Outbreak Quarantines page in the web interface • `quarantineconfig` command in the CLI For more information, see “PVO Quarantine Threshold Alert” section in the “Centralized Policy, Virus, and Outbreak Quarantines” chapter of the user guide.

Feature	Description
Configuring End-User Quarantine for Shared Mailbox	You can now access the End-User Quarantine (EUQ) of the Shared Mailbox and perform any actions on the spam quarantined messages when an administrator enables single sign-on to access EUQ and you have delegated access to that Shared Mailbox. It reduces the workload on administrators and assists in the timely delivery of quarantined messages. You can access EUQ to search the spam quarantine messages of the Shared Mailbox if you can log into EUQ through SAML 2.0 authentication. You can view the spam quarantined messages of your Primary Mailbox, and you can now add the Shared Mailbox to which you have access and view the spam quarantined messages of that Shared Mailbox. EUQ allows you to add multiple Shared Mailboxes and provides an option to view, search, release, release and add to safelist, and delete the spam quarantined messages. You can access the Shared Mailbox in the following ways: • Click **your email quarantine** or **View All Quarantined Messages** link provided in the Spam Quarantine Notification mail. • Log in to Secure Email and Web Manager EUQ using Spam Quarantine portal. For more information, see "Configuring End-User Quarantine for Shared Mailbox" section in the "Spam Quarantine" chapter of the user guide. **Note**:You can use this feature if you are an Office 365 user. This feature uses Microsoft Azure Active Directory API to provide access to End User Quarantine associated with shared mailboxes.
Support for new feature in AsyncOS 14.2 for Cisco Secure Email Cloud Gateway	**URL Retrospection Report page** - This report page shows URLs processed by the URL Retrospective Service. This page lists the malicious URLs, date and time when verdict is received from the URL Retrospective Service, and the remediation status of impacted messages. **Note** The URL Retrospection Report data is only available for Cloud admin users. For more information, see URL Retrospection Report page.

Feature	Description
No Support of Splunk database for Email Tracking Data	When you log in to Secure Email and Web Manager through the web interface or the CLI, you may see the following message if you are using the Splunk database for email tracking data: *"You have x GB of email tracking data in the Splunk database. From Secure Email and Web Manager 13.6.2 version, the Splunk database is no longer used for email tracking data. All new email tracking data is stored in the Lucene database. There will be no support of the Splunk database for email tracking data in the future General Availability (GA) release of Secure Email and Web Manager."* **Action**: Make sure you take a backup of the email tracking data (if required). You can use the `backupconfig` command in the CLI to perform the backup action. For more information, see Scheduling Single or Recurring Backups. **Note** If your organization network has only one Secure Email and Web Manager, you need to deploy a new Virtual Machine (VM) in the network. For more information on how to deploy a virtual Secure Email and Web Manager, see Cisco Secure Email and Web Virtual Appliance Installation Guide.
Enhancements on Grouping Appliances for File Analysis Reporting	Cisco Secure Email and Web Manager now uses the Smart Account ID to group appliances in your organization and to view the file analysis result of all appliances. When Smart Licensing is enabled on Cisco Secure Email and Web Manager, and you configure the appliance group for file analysis reporting, the system automatically registers Smart Account ID as the Appliance Group ID. You can change the Appliance Group ID at any time, and the change takes effect immediately without a Commit action. For more information, see (Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Results. **Note**: This feature is only available for on-premises admin users.

Feature	Description
Smart Software Licensing Enhancements	Following are the enhancements made to the Smart Software Licensing feature: • **License Reservation**: You can reserve licenses for features enabled in Secure Email and Web Manager without connecting to the Cisco Smart Software Manager (CSSM) portal. This is mainly beneficial for users that deploy Secure Email and Web Manager in a highly secured network environment with no communication to the Internet or external devices. For more information, see Overview and Reserving Feature Licenses. • **Device Led Conversion**: After you register Secure Email and Web Manager with smart licensing, all existing, valid classical licenses are automatically converted to smart licenses using the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal. For more information, see Overview. **Note**: This feature is only available for on-premises admin users.
Modification of Classic Licensing - Expiration Date in Web Interface and CLI	From this release onwards, the existing 'Expiration Date' column header in the web interface and CLI for classic licensing is modified as follows – "*Expiration Date (including grace period)"* to indicate that the grace period is included in the expiration date. **Note**: All alert messages and mail logs are modified to display the expiration date, including the grace period for a feature key.
Enable Syslog Disk Buffer with Configurable Size	[Applicable for TCP protocol only]: Select this check box to configure a local disk buffer for a syslog push log subscription to allow secure email and web manager to cache log events when the remote syslog server is unavailable. When the syslog server becomes available, the secure email web manager begins to send all the data in the buffer for that log subscription to the syslog server. For more information, see Log Retrieval

Cisco Secure Email and Web Manager Overview

AsyncOS for Cisco Secure Email and Web Manager 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 gateways. 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 Secure Email and Web Manager 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 Secure Email and Web Manager appliance is not involved in centralized email management, or 'clustering' of Email Gateway.

- **Centralized Upgrade Management:** You can simultaneously upgrade multiple Web Security appliances (WSAs) using a single Secure Email and Web Manager Appliance (SMA).
- **Backup of data**: Back up the data on your Secure Email and Web Manager 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 Secure Email and Web Manager appliance or spread the load across multiple appliances.