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 15.0

Feature	Description
[On-premises only] FIPS Compliance	Cisco Secure Email and Web Manager is FIPS compliant and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #4036). **Note** The Cisco Secure Email and Web Manager FIPS Certification only applies to email gateway integration and not to Secure Web Appliance integration. **Note** There is no support for the TLS v1.0 method if your Secure Email and Web manager is in the FIPS mode. For more information, see FIPS Management.
Single Log Line (SLL)	The SLL feature creates, indexes, and stores the email tracking data as a single log line or a flattened model. Therefore, you can execute a query and get a response quickly. This feature boosts the tracking query or search performance through fast response, low memory, and CPU usage. This feature is only applicable to post-upgrade email tracking data.

Feature	Description
Configuring CRL Sources	The Secure Email and Web Manager checks a list of revoked certificates called a Certificate Revocation List (CRL) as part of its certificate verification to ensure that the user's certificate has not been revoked. You need to keep an up-to-date version of this list on a server, and the Secure Email and Web Manager downloads it on a schedule you create. You can manually update the list too. You can configure CRL sources using the following ways: • Navigate to **Network** >**CRL Sources** > **Add CRL Source** > **Add CRL (Certificate Revocation Lists) Source** window in the legacy web interface. • Use the `Certconfig` > `CRL` subcommand in the CLI. For more information on Configuring CRL Sources, see Configuring CRL Sources.

Feature	Description
Removal of Old Splunk Data	When you upgrade to Secure Email and Web Manager 15.0 and later, and if email tracking data is contained in the Splunk database, the system will delete the Splunk database and binaries if you proceed with the upgrade. **Note** From the Secure Email and Web Manager 13.6.2 release onwards, the Splunk database is no longer used for storing email tracking data. All new email tracking data is stored in the Lucene database. After you upgrade to Secure Email and Web Manager 15.0, all tracking data before the upgrade to Secure Email and Web Manager 13.6.2 will be removed and cannot be recovered. During the upgrade to Secure Email and Web Manager 15.0 and later, a warning message indicating that the system will delete the Splunk database is displayed in the CLI or on the web interface of your Secure Email and Web Manager. **Sample Warning Message** *"From the Secure Email and Web Manager 13.6.2 version onwards, we have moved to a newer storage system for email tracking data. Generally, the old data is replaced with new data in the new storage system automatically. However, in some scenarios (for example, late upgrades, low mail flow and tracking data, and so on), there could be traces of old data still present in the old storage system that is no longer supported.* *In your case, it is 19 MB, which was last updated on 11 Aug 2022.* *You can take a back up 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 the 'Scheduling Single or Recurring Backups' section in the 'Common Administrative Tasks' chapter of the user guide.* *If you proceed with this upgrade process, your Splunk email tracking data will be deleted.* *You can choose to proceed with the upgrade or abort the upgrade.* *Do you agree to proceed with this upgrade? [Y]"* **Note** The warning message is only displayed for on-premises admin users. **Note** The **debug** submenu used to collect debug information for the Splunk database will be removed from the `Diagnostic > Tracking` subcommand in the CLI.

Feature	Description
Resetting the Network Configuration to the Initial Manufacturer Value	You can now reset the network configuration to the initial manufacturer value using the `Diagnostic > Reload` subcommand. The `Diagnostic > Reload` subcommand restores factory configuration and purges user configuration. This subcommand completely wipes the existing user and configuration data. Due to this, you can use the same installation and configuration methods for these devices as for the new devices. A new subcommand Reload Status that displays the status of the execution of the last Reload subcommand is added to the Diagnostic command. For more information on these subcommands, see Diagnostic - Reload Subcommand and Diagnostic - Reload Status Command.
Performing X.509 Validation for Peer Certificate during TLS Communication	You can configure your Secure Email and Web Manager to perform X.509 validation for peer certificates. The X.509 validation is applicable for the following services: • Outbound SMTP • LDAP • Updater • Alert over TLS • Syslog Server • Smart Licensing Server • SSE Connector • SSE Server For more information, see the X.509 Certificate.
New RAM Value for Secure Email and Web Manager Virtual Appliance Model	From AsyncOS 15.0 release onwards, there is a new RAM value for the M600v Secure Email and Web Manager virtual appliance model deployed through KVM or VMWare ESXi. For more information on the new RAM value applicable for the virtual appliance model, see the Cisco Content Security Virtual Appliance Installation Guide, available at https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html

Feature	Description
[On-premises only] Generation 2 Deployment Support for Azure Platform	From AsyncOS 15.0 release onwards, Secure Email and Web Manager supports Generation 2 deployments for Azure. **Note** The supported model for Azure Generation 2 deployment is **M600V** only. **Note** The Generation 2 image does not boot after the deployment on Azure platform. You must reboot the virtual machine after the Generation 2 image is deployed. For more information on Generation 2 deployment on Azure platform, see Cisco Secure Email Virtual Gateway and Cisco Secure Email and Web Manager Virtual on Microsoft on Azure Deployment Guide available at https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html.
[On-premises only] Microsoft Hyper-V Server 2019 Support	Secure Email and Web Manager 15.0 supports the Microsoft Hyper-V Server 2019.
[On-premises only] Generation 2 Deployment Support for Hyper-V	From AsyncOS 15.0 release onwards, Secure Email and Web Manager supports only Generation 2 deployment for Hyper-V. **Note** The supported model for Hyper-V Generation 2 deployment is **M600V** only. For more information on Generation 2 deployment support for Hyper-V, see the Cisco Content Security Virtual Appliance Installation Guide, available at https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html
[On-premises only] Supported Model for AWS Deployment	From AsyncOS 15.0 release onwards, the supported model for AWS deployment is **M600V** only. For more information, see Deploying Cisco Secure Email Gateway, Secure Web, and Secure Email and Web Manager Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services Guide available at https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html.

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.