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 13.0

Feature	Description
Support for new hardware models	The AsyncOS 13.0.0 release for Cisco Content Security Management appliance supports the following hardware models: • M195 • M395 • M695 For details, see https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html

Feature	Description
Performing Threat Analysis using Casebooks	The Cisco Content Security Management appliance now includes the casebook and pivot menu widgets. **Note** If you are using the Microsoft Internet Explorer browser to access your appliance, you will not be able to use the casebook widget. You can perform the following actions in your appliance using the casebook and pivot menu widgets: • Add an observable to a casebook to investigate for threat analysis. • Pivot an observable to a new case, an existing case, or other devices registered in the Cisco Threat Response portal (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis. For more information, see Integrating with Cisco Threat Response.
Ability to choose Cisco Threat Response server when registering appliance with Cisco Threat Response portal	When registering your appliance with the Cisco Threat Response portal, you can now choose a Cisco Threat Response server to connect your appliance to the Cisco Threat Response portal. The following are the Cisco Threat Response servers that are supported for this release: • `AMERICAS (api-sse.cisco.com)` • `EUROPE (api.eu.sse.itd.cisco.com)` For more information, see Integrating with Cisco Threat Response.
Managing favorite reports	You can now create a custom report page by assembling charts (graphs) and tables from all your existing email security reports on the new web interface of your appliance. For more information, see Working With Reports on the New Web Interface.
Creating a New CA Certificate for Policy, Virus, and Quarantines	You can create a CA certificate of 2048 bits for Policy, Virus, and Quarantines using the `updatepvocert` CLI command. For more information, see The updatepvocert Command.

Feature	Description

Support for new features in AsyncOS 13.0 for Cisco Email Security Appliances	• **Scheduling and Archiving Reports** - You can now schedule email reports and view the archived reports on the new web interface of your appliance.
	For more information, see Using Centralized Email Security Reporting.
	• **Safe Print Action report page** - You can use this report page to view:
	  • Number of safe-printed attachments based on the file type in graphical format.
	  • Summary of safe-printed attachments based on the file type in tabular format.
	For more information, see Using Centralized Email Security Reporting.
	• **Reporting Data Availability report page** - You can now view the reporting data availability report page on the new web interface of your appliance.
	For more information, see Using Centralized Email Security Reporting.
	• **Policy, Virus and Outbreak Quarantine** - You can now configure Policy, Virus and Outbreak Quarantine on the new interface of your appliance.
	For more information, see Centralized Policy, Virus, and Outbreak Quarantines.
	• **Swagger UI support** - Swagger UI helps you to design and manage AsyncOS API resources on a web interface.
	For more information, see Setup, Installation, and Basic Configuration
	• **Export Reports** - You can now export email reporting pages in a .PDF (Portable Document File) format on the new web interface of your appliance.
	For more information, see Working With Reports on the New Web Interface.

Improving User Experience by Collecting Feature Usage Statistics	The Cisco Content Security Management appliance now collects feature/interface usage statistics on the new web interface of the appliance that helps Cisco improve overall user experience. All data collected is anonymized. If you want to opt-out of this feature, navigate to **Management Appliance > System Administration > General Settings > Usage Analytics** page of the web interface to disable it. For more information, see Monitoring Web Usage Analytics.

Feature	Description
Improving user experience by collecting web interface usage statistics of the appliance	The Cisco Content Security Management appliance can now collect the web interface usage statistics of the appliance using the Usage Analytics feature. This feature is used to collect and analyze the web interface usage data and provide insight to improve user experience of the appliance. For more information, see Monitoring Web Usage Analytics.
Single Sign-On using SAML 2.0	The Cisco Content Security Management appliance now supports SAML 2.0 SSO so that the users can log in to the web interface of the appliance using the same credentials that are used to access other SAML 2.0 SSO enabled services within their organization. For more information, see SSO Using SAML 2.0.
Managing Multiple Subset of 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.

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.

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