



Introduction

This chapter contains the following sections:

- [What's New in this Release, on page 1](#)
- [Cisco Content Security Management Overview, on page 3](#)

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 12.x

Feature	Description
Support for hardware models	The AsyncOS 12.7.0 release for Cisco Content Security Management appliance supports only the x80 series hardware models. For details, see https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html
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 .

Feature	Description
Performing Threat Analysis using Casebooks	<p>The Cisco Content Security Management appliance now includes the casebook and pivot menu widgets.</p> <p>Note If you are using the Microsoft Internet Explorer browser to access your appliance, you will not be able to use the casebook widget.</p> <p>You can perform the following actions in your appliance using the casebook and pivot menu widgets:</p> <ul style="list-style-type: none"> • 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. <p>For more information, see Integrating with Cisco Threat Response.</p>
Ability to choose Cisco Threat Response server when registering appliance with Cisco Threat Response portal	<p>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.</p> <p>The following are the Cisco Threat Response servers that are supported for this release:</p> <ul style="list-style-type: none"> • AMERICAS (api-sse.cisco.com) • EUROPE (api.eu.sse.itd.cisco.com) <p>For more information, see Integrating with Cisco Threat Response.</p>
My Reports page on the New Web Interface	<p>You can 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.</p> <p>For more information, see Working With Reports on the New Web Interface.</p>
Configuring Policy, Virus and Outbreak Quarantine on the New Web Interface	<p>You can now configure Policy, Virus or Outbreak Quarantine from the new web interface of your appliance.</p> <p>For more information, see Centralized Policy, Virus, and Outbreak Quarantines.</p>
Managing APIs using Swagger UI	<p>Swagger is a set of open-source tools built around the OpenAPI Specification. Swagger UI helps you to design and manage AsyncOS API resources on a web interface.</p> <p>For more information, see Setup, Installation, and Basic Configuration</p>
Monitoring Web Usage Analytics	<p>You can enable or disable your website usage or activity from being sent for statistical analysis.</p> <p>For more information, see Common Administrative Tasks.</p>

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.

