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 13.6

Feature	Description
Ability to view Cisco Domain Protection reports	Cisco Domain Protection cloud service interface helps you protect the ownership of your domain from phishing, spam, and forged attacks. You can use the **Monitoring > Domain Protection** report page of the new web interface of your appliance to view: • Summary of messages that are classified as legitimate or threat in a graphical format. • Summary of the destination domains details based on the senders in a tabular format. You must have Administrator or Cloud Administrator privileges on the Cisco Domain Protection cloud service interface to authenticate and view the Domain Protection reports on the appliance. To view the Domain Protection report page, make sure that `trailblazerconfig` is enabled on your appliance. For more information, see Domain Protection Page.

Feature	Description
Ability to view Cisco Advanced Phishing Protection reports	You can use the Advanced Phishing Protection report page to view: • Total number of messages attempted to be forwarded to the Cisco Advanced Phishing Protection cloud service, in a graphical format. • Summary of messages forwarded to the Cisco Advanced Phishing Protection cloud service in a graphical format. For more information, see the Advanced Phishing Protection Reports Page.
Ability to view service status of the managed appliances and manage centralized services on the new web interface	You can use the Service Status section on the new web interface of the Security Management appliance to: • View the status of the managed appliances. • Enabled and disable centralized services. For more information, see Monitoring System Status.
Enabling proxy server to connect to Cisco Threat Response	You can enable a proxy server to connect to the Cisco Threat Repsonse using the `threatresponseconfig > enable_proxy` command in the CLI. For more information, see Integrating with Cisco Threat Response.

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.