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. For more information about the release, see the product release notes, which are available at the following URL:

http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html.

If you are upgrading, you should also review release notes for other releases between your former release and this release, in order to see the features and enhancements that were added in those releases.

Table 1: What's New in AsyncOS 13.6.1

Feature	Description
Cisco Advanced Phishing Protection Reporting and Tracking	**Reporting:** You can use the Advanced Phishing Protection report page to view the following: • The total number of messages that your email security gateway attempted to forward to the Cisco Advanced Phishing Protection cloud service. • The summary of messages that your email security gateway forwarded to the Cisco Advanced Phishing Protection cloud service. **Message Tracking:** You can use the Message Tracking to view the message details based on whether your email security gateway was able to forward the messages to the Cisco Advanced Phishing Protection cloud service. Fore more information, see Advanced Phishing Protection (APP) Report Page.

Feature	Description
Monitoring Mailbox Remediation Results	You can now monitor the remediation results for Mailbox Auto Remediation and Mailbox Search and Remediate using the Remediation Report. This report provides a summary of: • Total number of messages attempted for remediation using Mailbox Auto Remediation and Mailbox Search and Remediate. • Number of messages successfully remediated for a configured remedial action. • Number of messages for which the remediation failed. Click the Mailbox Auto Remediation and Mailbox Search and Remediate tabs in the report to view details about the messages for which the remediation was attempted. For more information, see Remediation Reports Page.
Manual searching and remediating messages in the mailbox and filtering it in tracking	You can now configure your appliance to remediate the messages manually using the Search and Remediate feature. The Search and Remediate feature provides the capability to search for the messages using the Message Tracking filter and apply remedial action on the messages. You can view the report based on the search criteria that displays the filtered messages delivered to the user mailbox. For more information, see Remediating Messages in Mailboxes.
New web interface of the appliance in Dark Mode	Dark Mode is a reversed color scheme that utilizes light-colored typography, UI elements, and iconography on dark backgrounds. You can now use dark mode on the new web interface of your appliance. For more information, see Accessing the New Web Interface on Dark Mode.
Cisco Threat Response Enhancements	• You can now connect to the Cisco Threat Response Server through a proxy. Use the `threatresponseconfig > enable_proxy` command in the CLI. • You can now choose the "APJC data center - APJC (`api.apj.sse.itd.cisco.com`)" to connect your appliance to the Cisco Threat Response portal. For more information, see Integrating the Appliance with Cisco Threat Response , Integrating the Appliance with Cisco Threat Response using CLI.

Feature	Description

Monitoring Service Status on the New Web Interface of the Appliance	You can perform the following on the New Web Interface of the appliance:
	• Configure Centralized Email Reporting
	• Configure Centralized Email Tracking
	• Configure Spam Quarantine:
	  • Edit Spam Quarantine Settings
	  • Edit Safelist/Blocklist Settings
	
	For more information, see Enabling Centralized Email Reporting on the New Web Interface, Enabling Centralized Email Tracking on the New Web Interface, Enabling Safelists and Blocklists on the New Web Interface and Enabling and Configuring Spam Quarantine on the New Web Interface.

Enable or disable the next generation web interface banner	You can use the `adminaccessconfig > NGUIBANNER` command in the CLI to enable or disable the banner link that redirects to the new web interface of the appliance. For more information, see Enabling and Disabling Message Banners for Administrative Users

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.