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 this Release

Feature	Description
Support for TLS v1.2	Cisco Content Security Management appliance now supports an additional SSL method - TLS v1.2. If you were not using TLS v1 prior to the upgrade, the SSL methods are not automatically set to TLS v1.2 after the upgrade. You can use the `sslconfig` command in the CLI to view or modify the existing SSL configuration. **Note** The highest supported TLS or SSL method in the client advertisement is always selected during the negotiation.

Feature	Description

Support for new features in AsyncOS 11.0 for Cisco Email Security Appliances	Reporting support for the following features that are new in AsyncOS 11.0 for Cisco Email Security Appliances:
	• Geo Distribution. Use this report page to view details such as:
	  • Top incoming mail connections based on country of origin in graphical format.
	  • Total incoming mail connections based on country of origin in tabular format.
	
	You can use Message Tracking to search for incoming messages from specific geolocations detected by the content or message filter. Use the **Geolocation** filter for the Message Event option in the Advanced section of Message Tracking.
	For details, search for the relevant terms in the email reporting chapter of the online help or user guide.
	The following reports have been enhanced to show details of outgoing messages scanned by the AMP engine:
	• Advanced Malware Protection
	• AMP File Analysis
	• AMP Verdict Updates
	• Overview Page
	• Outgoing Destinations
	• Outgoing Senders
	• Internal Users
	For details, search for the relevant terms in the email reporting chapter of the user guide.

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. In addition, there are several extended reports for web security that are uniquely available on the Security Management appliance.

- **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.

- **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.