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. 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 11.5

Feature	Description
Message Tracking Support for new features in AsyncOS 11.1 for Cisco Email Security Appliances	Message tracking support for the following new features in AsyncOS 11.1 for Cisco Email Security Appliances: • **Handling Unscannable Messages for URL Filtering, AMP Engine and Content Scanner** – You can use message tracking to view the log entries of messages not scanned by URL filtering, AMP engine and Content Scanner, and the appropriate actions taken on such messages. • **URL Filtering Support for Shortened URLs** - You can use message tracking to view the log entries of messages that are scanned for shortened URLs, and the appropriate actions taken on such messages. • **Support for URL Scanning in Attachments** - You can use message tracking to view the log entries of messages that are scanned for URLs in attachments, and the appropriate actions taken on such messages.

Feature	Description
Message Tracking Details for Low Risk verdict in Messages	You can use Message Tracking to search for messages that contain files categorized as Low Risk due to no dynamic content found in a file after file analysis. Use **Low Risk** for the Message Event option in the Advanced section of Message Tracking. For more information, see Tracking Email Messages.
Restarting and Viewing the status of services enabled on the appliance.	You can use the `diagnostic > services` sub command in the CLI to: • Restart the services enabled on your appliance without having to reboot your appliance. • View the status of the services enabled on your appliance. For more information, see Common Administrative Tasks.
Support for new features in AsyncOS 11.5 for Cisco Web Security Appliances.	Reporting support for the following feature which is new in AsyncOS 11.5 for Cisco Web Security Appliances: User Count. Use this report to view details about: • The total number of authenticated and unauthenticated users of Web Security appliances. • The unique user count for the last 30 days, 90 days, and 180 days. See User Count Report (Web).
Support for Scheduled Policy Expiration	Cisco Content Security Management appliance now supports Policy Expiration feature. You can now set the expiry time for Access and Decryption policies.The policies are automatically disabled once they exceed the set expiry time. You will receive alerts on 3 days prior to expiry and also upon expiry. Policy Expiration feature is applicable only for Access and Decryption policies.

Feature	Description
Advanced Malware Protection Report Enhancements	The Advanced Malware Protection report page has the following enhancements: • A new section- **Malware Files by Category** to view the percentage of blacklisted file SHAs received from the AMP for Endpoints console. • The threat name of a blacklisted file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Malware Threat Files section of the report. • You can click on the link in the More Details section of the report to view the file trajectory details of a blacklisted file SHA in the AMP for Endpoints console. • A new verdict – **Low Risk** is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the Incoming Files Handed by AMP section of the report. See Advanced Malware Protection (File Reputation and File Analysis) Report Pages.

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.