# 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 13.8.0***

| Feature | Description |
|---|---|
| Message Tracking Enhancements | The new web interface includes the following user experience enhancements:<br>• The **Message Tracking Search Results** page is now enhanced to display more search results per page view.<br>• The **Message Tracking Search Details** page layout is now enhanced to display the **Envelope Header and Summary** and **Sending Host Summary** panes alongside the **Processing Details** pane. This new layout allows you to view all the important information in the same page view without scrolling. |
| Reporting Enhancements | You can now schedule and archive My Favorite Reports. You can also export My Favorite Reports data in CSV or PDF format. |

| Feature | Description |
|---|---|
| Spam Notification Enhancements | • You can now set an expiration period for the links in the Spam notification. These links will expire automatically after the specified period.<br>• You can now show or hide the links to view all the quarantined messages in a Spam notification. Also, if you are showing the links in the spam notification, you can now force the end-user to authenticate before accessing the Spam quarantine.<br><br>For more information, see the **Notifying End Users About Quarantined Messages** topic in the User Guide. |
| Security Enhancements | AsyncOS 13.8.0 includes the following security enhancements:<br>• The appliance will no longer support SSLv2 and SSLv3 methods. When you upgrade from a lower AsyncOS version, the appliance will automatically use TLS 1.1 and TLS 1.2. For more information, see **SSL Configuration Changes** topic in the Release Notes.<br>• The appliance will now send the Cisco Technical Support requests over TLS. If your SMTP server is not using TLS, the requests are sent as plaintext.<br>• You can now configure your appliance to send alerts over TLS. Use the following subcommand in the CLI to configure this functionality: **alertconfig > SETUP > Do you want to enable TLS support to send alert messages?**. |
| Cisco SecureX and Cisco Threat Response Enhancement | You can now configure your appliance to connect to Cisco SecureX and Cisco Threat Response via a proxy. Check the **Use Proxy** check box in the **Network** > **Cloud Service Settings** page to connect via a proxy. |

| Feature | Description |
| --- | --- |
| YouTube Report (Web) | In the new web interface (**URL Categories** report page), you can now view the following information related to the YouTube categorization feature:<br>• Top Youtube Categories: Total Transactions<br>You can view the top Youtube Categories that are being visited on the site in a graphical format.<br>• Top Youtube Categories: Blocked and Warned Transactions<br>You can view the top Youtube URL that triggered a block or warning action to occur per transaction in a graphical format. For example, a user went to a certain Youtube URL and because of a specific policy that is in place, this triggered a block action or a warning. This Youtube URL then gets listed in this graph as a transaction blocked or warning.<br>To view the **URL Categories** report page, select **Web** from the **Product** drop-down and choose **Monitoring** > **URL Categories** from the **Reports** drop-down.<br>• Youtube Categories Matched<br>The Youtube Categories Matched interactive table shows the disposition of transactions by Youtube category during the specified time range, plus bandwidth used and time spent in each category.<br>To view the Youtube Categories Matched interactive table, choose **Web** > **Reporting** > **URL Categories**.<br>• Youtube (YT) Category<br>A new filter YT Category has been added under **Web** > **Tracking**. To filter by a specific Youtube category, expand the Youtube Category section and select the Youtube categories that you want to view. |

| Feature | Description |
|---|---|
| IP Spoofing Profiles | You can now configure Web Proxy IP Spoofing by creating an IP spoofing profile and adding it to the routing policies. When IP spoofing profile is used in a routing policy, the web proxy changes the source IP address to custom IP address defined in the IP spoofing profile.<br><br>To create a new IP spoofing profile or modify and existing IP spoofing profile, choose **Web** > **IP Spoofing Profiles**.<br><br>To add IP spoofing profile in a routing policy, choose **Web** > **Routing Policies**.<br><br>**Note** If you do not want to publish the Security Management Appliance IP Spoofing profiles to Web Security Appliance and overwrite the existing IP Spoofing profiles in the Web Security Appliance, follow the below steps:<br><br>1. Log into Security Management Appliance.<br>2. Go to **Configuration Master** > **IP Spoofing Profile**.<br>3. Click **Edit Settings**.<br>4. Set **Publish IP Spoofing Profiles to WSA** as **No**.<br><br>The default option selected is **Yes**.<br><br>For more information, see *User Guide for AsyncOS 12.5 for Cisco Web Security Appliances*. |

# 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.