# Cisco Secure Email Threat Defense Release Notes

# Table of Contents

# Introduction

This document includes information on product updates, usage caveats, and known problems for Cisco Secure Email Threat Defense.

Archived release notes for Cisco Secure Email Cloud Mailbox from July 12, 2021 through September 29, 2022 are located here: https://www.cisco.com/c/en/us/td/docs/security/cloud-mailbox/release-notes/cloud-mailbox-release-notes-archive.html

# Product Updates

## January 27 2026

## Enhancements

- Message Report error messaging is improved. When downloading a failed EML file, the UI now shows accurate and meaningful error information, improving clarity and troubleshooting.
- Per-Mailbox Delivery Details: The Message Report now displays Delivery Status and Delivery Error details per mailbox, improving visibility into message delivery issues. (Applicable for SMTP/Inline Mode Only)

## Fixed Issues

- Minor bug fixes.

## December 16 2025

## Enhancements

- Policy exceptions by sender are available for Journal message sources. These rules allow you to create exceptions to your base policy for specific senders. Policy exceptions can be created under **Configuration** > **Policy settings.**
- Deprecation of Message Rules: Allow List and Verdict Override

  The rules under **Administration** > **Message Rules** are deprecated and will be removed in a future release. Your rules are still available and functioning. You should recreate any Message Rule functionality using the new Policy exceptions rules under **Configuration** > **Policy settings**. Once new rules are created, they will take precedent over any existing Message Rules.
- Policy exception rules can now be ranked. Drag and drop the items in the list to reorder them.
- The Message Report is redesigned as part of Cisco's ongoing efforts to provide a more consistent experience across Security products. The refreshed look and feel now matches the rest of the Secure Email Threat Defense UI.
- In the Message Report, links that are contained in a QR code are now indicated with a QR code icon.

## Fixed Issues

- XDR Ribbon Issue: You may have encountered an error while accessing certain response actions for observables. This issue arose due to changes in the XDR authentication requirements, which have now been addressed. If you continue to experience issues, re-authenticate the XDR ribbon to fix the problem.
- Minor bug fixes.

# December 04 2025

## Enhancements

- High Impact Personnel list improvements:
  - Click the number of impersonations in the last 30 days to pivot to a filtered list of the messages that were flagged as impersonations
  - Filter by Impersonated Users using the Messages page filter panel
- SMTP/Inline message sources:
  - The Quick message filter on the Dashboard has new items for Policy exceptions and Security mailbox
  - Status and Action are added to the SPF/DKIM/DMARC tooltips when applicable

## Fixed Issues

- Minor bug fixes.

# November 18 2025

## Enhancements

- SMTP/Inline message sources: Sender Authentication information (SPF, DKIM, DMARC) including pass/fail, reason, and action is now included in the Messages page export.

## Fixed Issues

- Minor bug fixes.

## November 04 2025

# Enhancements

- Cisco Secure Email Threat Defense Inline mode is introduced with this release. Secure Email Threat Defense Inline offers real-time inline scanning and remediation. Inline mode improves detection speed and remediation capabilities by processing messages as they flow through the mail system, detecting threats and stopping them before reaching the end-user.

  New customers onboarding with an Advantage license can set up their businesses with SMTP/Inline message sources. Options include receiving traffic via SMTP or SMTP Relay.
- URL bypass rules are new in this release. These rules can be configured to prevent specific URLs from being scanned. You can create these rules at **Configuration** > **Global settings** > **URL rules**.
- Bypass Analysis Rules for Phish Test & Security Mailbox are relocated from **Administration** > **Message Rules** to **Configuration** > **Global settings** > **Message bypass rules**. Any existing rules are migrated to the new location and will behave in the same manner as before.
- Spam and Graymail analysis defaults to On/Checked for newly created businesses.
- Message view improvements:
  - Improved column resizing for Verdict, Action, and Date columns.
  - User column resizing is maintained in-browser, preventing resets after browser refreshes.
  - Introduced a more compact date/time format to optimize screen space usage.
  - Improved adjustments for table density and column show/hide options from the gear icon on the messages table
- Documentation improvements:
  - User documentation is updated with new formatting and is now integrated with the UI.
  - Access the new documentation from the (?) menu in the top right corner of the UI.

# Fixed Issues

- Minor bug fixes.

## October 17 2025

## Enhancements

- User Management Notifications. Notifications of user creation, changes, or user deletion by administrators are sent to a specified email address. To turn on these notifications, go to **Administration** > **Business** > **Preferences**.
- Messages page improvements
  - You can now show/hide the top graph charts.
  - You can now select **Copy message ID** from the **...** menu at the end of a message row.

## Fixed Issues

- Minor bug fixes.

## October 07 2025

## Fixed Issues

- Minor bug fixes.

## September 23 2025

## Enhancements

- The High Impact Personnel List can now contain up to 500 contacts. Additionally, the UI screens for the list are redesigned as part of Cisco's ongoing efforts to provide a more consistent experience across Cisco Security products.

## Fixed Issues

- Minor bug fixes.

## September 09 2025

## Enhancements

- Ability to detect URLs in QR codes within the Log Export API for message event logs.
- Admins can reclassify messages as Spam or Graymail, even if scanning for Spam and Graymail is disabled in the global policy.
- Enhanced Remediation and Reclassification for API performance: batch processing support and improved stability to prevent timeouts

## Fixed Issues

- Minor bug fixes.

## August 26 2025

## Enhancements

- Ability to resize columns on the Messages page.
- For users with multiple tenants, they are now listed in alphabetical order in the account selector.

## Fixed Issues

- Minor bug fixes.

# Usage Caveats

## Advisory Summary on Message Bypass Rules

Note the following important caveats when creating and using Message bypass rules:

- A Message bypass rule BYPASSES ALL SCANNING AND PROTECTIONS for messages that match the rule conditions. Do not use Bypass Rules for any use-cases other than customer employee security awareness training (Phish Test) or for end-mailbox-user reporting to an organization's Security Mailbox. These are the only supported scenarios for Message bypass rules. For all other scenarios, use other types of message rules, or adjust your configuration policy settings.
- IT IS STRONGLY ADVISED to use only the dedicated Sender IP Addresses/CIDR blocks provided by your Phish Test vendor as the basis of Message bypass rules.
- BE AWARE if your Phish Test vendor is unable to provide dedicated Sender IP Addresses/CIDR blocks; the usage of Sender Domain or Email Address in a Message bypass rule opens you up to bypassing potentially spoofed messages
- DO NOT use Sender Domain or Email Address in a Message bypass rule unless you have separately validated sender email authentication is tightly scoped by the vendor's SPF record, strongly enforced by your organization's upstream edge email controls, and the specified Sender Domain or Sender Email Address exactly matches the final Return-Path header on all messages intended to match the Bypass Rule
- Open a Support case to request assistance validating any existing Message bypass rules conform to the guidance above.

## Microsoft Excel cell size limit

Microsoft Excel has a limit of 32,767 characters per cell. If you export your data to CSV and then open it in Excel, any excess data beyond the character limit is moved to the next row.

## Cannot sign in to Security Cloud Sign On with Microsoft when Microsoft account does not have last name

Microsoft 365 does not require accounts to have a defined first name and last name. When trying to authenticate with a Microsoft account that does not have a last name, Security Cloud Sign On returns the following error:

*400 Bad Request. Unable to create the user. Required properties are missing*.

To workaround this issue, make sure both first name and last name are defined in the Microsoft 365 account.

## Trends delay when messages are manually reclassified

When messages are manually reclassified, there could be a delay of up to one hour before the changes are reflected on the Trends page.

# Known Issues

## Microsoft Allow lists and Safe Senders

Because of some recent changes to Microsoft's MSAllowList flag, Microsoft allow lists are not always honored by Secure Email Threat Defense if your organization allows individual users to configure allow lists in their mailbox and a message happens to fall in a user's allow list.

If you want Secure Email Threat Defense to honor these settings, deselect the **Apply policy to Microsoft Safe Sender messages** check box on the **Configuration** > **Global settings** > **Unwanted message analysis** panel. Safe Sender flags are respected for Spam and Graymail verdicts, but are not respected for Malicious and Phishing verdicts. That is, Safe Sender messages with Spam or Graymail verdicts will not be remediated.

## Conversation view

You may encounter the following issues when using Conversation view:

- The **+** symbols don't disappear until you click them, even if there are no additional messages
- There is a limit of 9 horizontal nodes

# Copyright Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.