Cisco Secure Email Threat Defense Release Notes

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

September 04 2024

Fixed Issues

- Minor bug fixes.

August 23 2024

Enhancements

- Public API Client credentials will expire after one year. This will be enforced beginning in July 2025. A banner will show when credentials are within 90 days of expiring. New credentials can be created from **Administration** > **API Clients** in the Secure Email Threat Defense UI.

Fixed Issues

- Minor bug fixes.

August 12 2024

Fixed Issues

- Minor bug fixes.

July 29 2024

Fixed Issues

- Minor bug fixes.

June 27 2024

Fixed Issues

- Minor bug fixes.

June 12 2024

Fixed Issues

- QR code analysis is restored for .doc and .docx files. URLs are extracted and sent to engines for analysis.

May 29 2024

Fixed Issues

- Customers may have encountered some unexpected problems with how sender information is handled in our Phish Test Bypass Rules due to recent updates. To resolve these issues, we are undoing these updates and returning to the way things worked before March 19. Existing Phish Test Bypass Rules will be regenerated and may take a few days to take effect. For additional guidance on using Bypass Rules, see Advisory Summary on Bypass Rules, page 13.
- Minor bug fixes.

May 14 2024

Fixed Issues

- Minor bug fixes.

April 30 2024

Enhancements

- User accounts are now listed alphabetically under the Accounts drop-down-list.
- Public API rate limiting is now being enforced for businesses in the North American and European regions.
  - API keys can be generated from **Administration** > **API Clients**.
  - Including the API key in requests in the header x-api-key is required. Otherwise, your requests will fail.
  - The current rate limit per tenant is 5 requests/second, the burst limit is 10 requests/second, and the daily quota is 5000 requests. Should you exhaust your limit, contact support to request an increase.

- W3C URLs are no longer extracted from emails and shown on the Secure Email Threat Defense UI.

Fixed Issues

- Minor bug fixes.

April 16 2024

Enhancements

- Recent updates to the Message Search API allow you to filter messages based on Verdict Indicators, Action Indicators, Attachments and Links, and Last Action.
- Public API rate limiting is now being enforced for businesses in the Indian and Australian regions.
  - API keys can be generated from **Administration** > **API Clients**.
  - Including the API key in requests in the header x-api-key is required. Otherwise, your requests will fail.
  - The current rate limit per tenant is 5 requests/second, the burst limit is 10 requests/second, and the daily quota is 5000 requests. Should you exhaust your limit, contact support to request an increase.

Fixed Issues

- Minor bug fixes.

April 3 2024

Fixed Issues

- Minor bug fixes.

March 19 2024

Enhancements

- A new Message Report page is introduced in this release. This page combines the expanded message view and the timeline view and introduces additional features. New features include:
  - Email Preview that allows super-admin and admin users to see the message as it appears to the end-user.

    Note: An audit log record is created when a user previews an email. The audit log is available for download from **Administration** > **Business** > **Preferences**.
  - Sender Messages graph that shows total messages sent and total threat messages sent by the sender of the message over the last 30 days.
  - Mailbox List showing a list of end-user mailboxes that received the message. The list shows if the message was read prior to the last remediation action and any remediation errors on the message.

  For more details, see the Cisco Secure Email Threat Defense User Guide.
- Phish Test bypass message rules now match only sender email addresses or domains criteria against the Envelope From email address.

- Recent updates to the public reporting API include:
  - Top 10 threat senders report and retrospective verdict count report.
  - Date range increased to up to 90 days.
- We have removed QR code detections for .doc files due to an issue causing intermittent crashing with large files. We will return this functionality as soon as possible.

Fixed Issues

- Minor bug fixes.

March 04 2024

Enhancements

- Remediation improvement: For outgoing and internal messages, the Move to Inbox action moves the message to the Sent folder of the initial sender of the message, instead of to their Inbox.

Fixed Issues

- Minor bug fixes.

February 21 2024

Enhancements

- QR code detections are available for more file types. In addition to the previously announced graphics files, URLs are extracted from QR codes present in pdf, word, xls, and ppt files and sent to the engines for analysis.

Fixed Issues

Minor bug fixes.

February 06 2024

Enhancements

- The Mixed direction has been removed from the UI and APIs. This value is no longer populated by Microsoft.
- Recent updates to the public API include:
  - New Reporting APIs: Total messages scanned by direction, total traffic by verdicts, and top 10 targets that received threat messages.
  - Message Search API update: you can now filter messages by techniques.

Fixed Issues

- Minor bug fixes.

February 01 2024

Enhancements

- QR Code detections
  - URLs are extracted from QR codes found in the message body and in .jpg, .jpeg, and .png attachments. These URLs are then analyzed along with other URLs included in a message.
  - QR code URLs are shown in the expanded message view in the Links section.
  - If a URL is deemed malicious, a Malicious URL technique is shown.
  - A QR Code Detected technique is shown for some messages with QR codes. This technique will be available for all QR codes in a future release.

January 30 2024

Enhancements

- Style changes throughout the Secure Email Threat Defense UI for better consistency across Cisco Security products. Changes include:
  - Downloads, Help, Notifications, and User Settings are accessible from the page header.
  - Menu items that were previously across the top of the screen are accessible from the left side menu.

Fixed Issues

- Minor bug fixes.

January 18 2024

Fixed Issues

- Minor bug fixes.

December 13 2023

Enhancements

- You can now delete Message Rules. Previously, rules could only be disabled.
- The High Impact Personnel List is now generally available for use. Use this list to help protect your organization from User Impersonation attacks.
  - Build your list of up to 100 important people in your organization. The list is sent to our engines for higher scrutiny on Display Name and Sender Email Address.
  - Deviations from the configured information are identified as User Impersonation in the Verdict Details panel of convicted messages.
- Recent updates to the public API include:

  - Ability to filter messages based on retro verdicts by adding **“isRetroVerdict”: true** in the request body of the message search API.
  - Rate limiting has been implemented on Public APIs. API keys can be generated from **Settings** > **Administration** > **API Clients**.

    Note: Rate limiting will be enforced beginning in February 2024; including the API key in requests in the header x-api-key will be required. Otherwise, your requests will fail.

- In the Messages Download report, the Auto Remediated column is renamed Remediation Method and indicates if a message was remediated automatically, manually, or by API.

Fixed Issues

- Minor bug fixes.

December 4 2023

Fixed Issues

- Minor bug fixes.

November 16 2023

Enhancements

- Additions to the public API allow you to programmatically remediate and reclassify messages. For details, see the API guide. This guide is accessible from the Secure Email Threat Defense Help menu, or at https://developer.cisco.com/docs/message-search-api.

Fixed Issues

- Minor bug fixes.

October 31 2023

Enhancements

- Email Threat Defense now scans attachments and extracts URLs for engine analysis.
  - Over 250 file types are supported and sent to engines.
  - File analysis supports 5 levels of archived files (e.g. .zip files).
- Allow List and Verdict Override message rules allow the selection of threat verdicts in addition to spam and graymail.

Fixed Issues

- Minor bug fixes.

October 18 2023

Fixed Issues

- Minor bug fixes.

October 03 2023

Enhancements

- Icons for Threats and Unwanted Messages on the Home page and Impact Report are now clickable.

Fixed Issues

- Minor bug fixes.

September 20 2023

Enhancements

- The Timeline view now shows:
  - A list of mailboxes that have read a message at the time of remediation.
  - Information about any remediation errors on the message and which mailboxes had the errors. You can also download the error log from the timeline.

Fixed Issues

- Minor bug fixes.

September 08 2023

Fixed Issues

- Minor bug fixes.

August 28 2023

Enhancements

- Small EML files are now downloaded immediately. Larger files continue to be accessible from the Downloads page.
- The Recipient Search field now includes the Envelope To and Delivered To fields.

Deprecation Notice

- Organizational-Bcc in the user interface, and bccAddresses in the public message search API response are deprecated and will be removed in a future release. BCC addresses are now captured in the To/Cc field.

Fixed Issues

- Minor bug fixes.

August 10 2023

Enhancements

- Administrators can now change the role of a user on the **Settings** > **Administration** > **Users** page.
- The expanded message view shows additional recipient data extracted from the journal headers. There can be up to 3 separate, scrollable sections: To/Cc, Envelope To, and Delivered To.
- The Message Rules Status column filter is saved in your browser to default to the last setting selected.

Fixed Issues

- Minor bug fixes.

July 31 2023

Fixed Issues

- Minor bug fixes.

July 18 2023

Enhancements

- The High Impact Personnel page shows how many times a user has been impersonated in the last 30 days.
- Recent updates to the public message search API include:
  - Expanded search capabilities: recipient email address, sender email address, and Internet message ID.
  - The API response can now indicate if a message was manually reclassified.
  - A link to the Public API Guide is accessible from the Secure Email Threat Defense Help menu. The guide is located at https://developer.cisco.com/docs/message-search-api/

Fixed Issues

- Minor bug fixes.

June 29 2023

Fixed Issues

- Minor bug fixes.

June 19 2023

Enhancements

- You can filter Message Rules by status to show or hide active or disabled rules.

Fixed Issues

- Minor bug fixes.

June 09 2023

Enhancements

- The Messages Graph and Quick Filter is updated:
  - The start of each day is now clearly highlighted in the week view, allowing you to drill into a specific day
  - The threat and direction metrics are shown in blue to indicate that they are links that can be used to filter the messages

Fixed Issues

- Minor bug fixes.

May 19 2023

Enhancements

- The Cisco Secure Email Threat Defense public API is introduced with this release. The API allows you to programmatically access and consume data in a secure and scalable manner. For API Documentation, see https://doc.api.etd.cisco.com/.

Fixed Issues

- Minor bug fixes.

May 11 2023

Enhancements

- For businesses created after May 11, 2023, Spam and Graymail analysis defaults to Off. This setting can be adjusted on the Policy page.
- Messages Graph and Quick Filter
  - A graphical representation of threats and messages is shown at the top of the Messages page.
  - Threat and category breakout allows you to view totals and easily filter for threats.
  - A Quarantine total is shown and is filterable.

  - Message Direction totals are shown and are filterable.
- The Home page Messages Scanned graph now pivots to the Messages page with a custom time frame for an hour (Daily View), 3 hour (Weekly graph point), and day (Weekly X-axis label).

Fixed Issues

- Minor bug fixes.

April 20 2023

Enhancements

- Secure Malware Analytics detections are shown as the Malicious Behavioral Indicators technique in the Verdict Details panel.
- Secure Endpoint detections are shown as the Low File Reputation technique in the Verdict Details panel.
- Message recipients are sorted so High Impact Personnel are listed first.

Fixed Issues

- Minor bug fixes.

April 13 2023

Enhancements

- Secure Email Threat Defense is further integrated with SecureX. You can now quarantine messages with a specific observable directly from the SecureX pivot menus in integrated products. Additionally, you can use the pivots to initiate a search in Secure Email Threat Defense. Observables you can pivot from include:
  - Email Address
  - Email Message ID
  - Email Subject
  - File Name
  - Sender IP
  - SHA 256
  - URL

March 22 2023

Enhancements

- A new No Authentication mode for businesses that use Cisco Secure Email Cloud Gateway as a message source is introduced. This visibility-only mode allows you to send traffic to Secure Email Threat Defense without authenticating to Microsoft. You will not be able to remediate messages in this mode. The initial setup flow for new businesses and the Policy page settings are updated to support this configuration.

Fixed Issues

- An issue with how graphs were displaying that was introduced with the Daylight Saving Time adjustment on March 12, 2023 is now resolved.

March 15 2023

Enhancements

- A link to the Secure Email Threat Defense system status page is available from the User Profile menu.

Fixed Issues

- Minor bug fixes.

February 27 2023

Enhancements

- On the Policy page, there is a new option to turn analysis and remediation of Spam and Graymail On or Off. When Off is selected, Spam and Graymail and Unwanted Mail panels and options are removed.
  - Existing accounts default to Spam and Graymail analysis being On.
  - Future accounts with Cisco SEG configurations will default to Spam and Graymail analysis being Off. Spam and Graymail analysis is already performed by the SEG.
- Deviations from the configured information for individuals on the High Impact Personnel list are identified as a Technique in the Verdict Details panel of convicted messages.

Fixed Issues

- Some customers were experiencing login issues where HTTP headers were being stripped before they reached Secure Email Threat Defense. This issue has been resolved.

February 08 2023

Fixed Issues

- Minor bug fixes.

January 31 2023

Enhancements

- The Home page has the option to switch between showing data for a Day or a Week.
- On the Policy page, the Imported Domains section shows the total number of imported domains and the number of domains marked for auto-remediation. The list has a search feature that allows you to filter the list with a partial match search.

- The start date on the Impact Report is now editable. This allows you to select a 30 day range, or the first of the month for a calendar month view.
- The Messages page filter indicates when filters have been applied. A new Reset All link is added to the top of the page to simplify setting filters back to default. The Reset Filters button remains at the bottom of the filter panel for ease of use.
- The Timeline view now shows the seconds of events such as received, remediation, reclassification, etc.
- The Reclassified hover text now shows date and time.
- New Early Field Trial feature: High Impact Personnel List
  - Admins can create a list of up to 100 people that is sent to Talos for higher scrutiny on Display Name and Sender Email Address.
  - **Note**: Build your lists now, and you will see the User Impersonation technique in your Verdict Details in future releases.

Fixed Issues

- Minor bug fixes.

December 15 2022

Enhancements

- You can now use the Messages page filter to search by Sender IP address
- A Clear All button is added for Notifications
- On the **Settings** > **Downloads** > **Download EML** page, the message Subject is clickable for easy navigation back to the message

Fixed Issues

- Minor bug fixes.

November 17 2022

Enhancements

- The Sender column on the Messages page is renamed Sender (Display Name/Friendly From)

Fixed Issues

- Minor bug fixes.

November 09 2022

Enhancements

- The ability to use Cisco Secure Email Cloud Gateway as a message source is now available. For this initial release, support is limited to Microsoft O365 mailboxes. The initial setup flow for new businesses and the Policy page settings are updated to support this configuration.

- Brand Impersonation detections are now supported. No configuration change is needed. 1500 brands are currently indexed, and more will be added over time.
- The Home page dashboard includes new widgets and graphs that quickly show the state of your business in the last 24 hours, and allows you to quickly pivot to a filtered list of messages. It includes:
  - Threats: shows a count of BEC, Scam, Phishing, and Malicious detections
  - Unwanted Mail: shows a sparkline graph of Spam and Graymail detections
  - Messages Scanned: shows a graph of message traffic
  - Potentially Compromised Accounts: lists internal addresses that were seen sending threat messages from within the organization
  - Quick Message Filter: shows quick links to Retrospective Verdicts, Messages in Quarantine, and Messages with Message Rules applied
- A new Secure Email Threat Defense status page is available at https://ciscosecureemailthreatdefense.statuspage.io. Subscribe to receive updates when there is a change in status.

Fixed Issues

- Minor bug fixes.

October 25 2022

Enhancements

- Cisco Secure Email Cloud Mailbox is renamed Cisco Secure Email Threat Defense. You will see this name change over time throughout our interface, documentation, and marketing materials.

Fixed Issues

- Minor bug fixes.

Usage Caveats

Advisory Summary on Bypass Rules

Note the following important caveats when creating and using Bypass Rules:

- A 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 Bypass Rules. For all other scenarios only Verdict Override or Allow Rules are supported.
- IT IS STRONGLY ADVISED to use only the dedicated Sender IP Addresses/CIDR blocks provided by your Phish Test vendor as the basis of 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 Bypass Rule opens you up to bypassing potentially spoofed messages.

- DO NOT use Sender Domain or Email Address in a 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 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, select the **Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts** check box on the Policy page. 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