



# Cisco Secure Email Threat Defense FAQ

**First Published:** 2021-04-26

**Last Updated:** 2024-06-15





# Contents

- Introduction ..... 3
- Setup ..... 5
  - Why are Microsoft 365 Global Admin rights required to set up Secure Email Threat Defense? ..... 5
  - What access permissions does Secure Email Threat Defense request from Microsoft? ..... 5
  - Why did I receive a welcome email from Malware Analytics/Threat Grid? ..... 5
  - How can I find my journal address? ..... 5
  - Why do I receive a registration error when I try to register my Microsoft 365 tenant? ..... 5
  - How long does Cisco retain my journal data? ..... 6
  - Can a user be added to more than one Secure Email Threat Defense instance? .. 6
- Login Issues ..... 7
  - How can I find more information about problems logging in to Secure Email Threat Defense? ..... 7
  - Why can't I log in with my email address? ..... 7
  - How can I reset my password? ..... 7
  - Why do I see a 400 Bad Request error when trying to sign in to Security Cloud Sign On with my Microsoft account? ..... 7
  - How can I access Secure Email Threat Defense from the SecureX Application Portal? ..... 7
  - How can I switch between Secure Email Threat Defense instances? ..... 7
  - How can I find out the operational status of Secure Email Threat Defense? ..... 7
- Secure Email Threat Defense and Microsoft 365 ..... 9
  - Does Secure Email Threat Defense honor senders or domains from an allow list in Microsoft 365? ..... 9
  - Does Secure Email Threat Defense honor actions my users take on Junk mail in Outlook? ..... 9
  - What is the journaling size limit? ..... 9
  - Why aren't all of my domains showing in Secure Email Threat Defense? ..... 9
  - Where can I find more information about journaling in Microsoft 365? ..... 9
- Messages and Search ..... 11

---

How do I let Cisco know a message was misclassified?.....	11
Why am I still getting emails from a sender that I already reclassified?.....	11
Why do some messages appear twice on my Messages page?.....	11
What does undisclosed recipient mean? .....	11
Support .....	13
How can I access Secure Email Threat Defense documentation?.....	13
How can I get help setting up and using Secure Email Threat Defense?.....	13
How can I contact customer support? .....	13



# Introduction

This document includes Frequently Asked Questions (FAQ) about Cisco Secure Email Threat Defense. For further details on using Secure Email Threat Defense see [Cisco Secure Email Threat Defense User Guide](#).





# Setup

## Why are Microsoft 365 Global Admin rights required to set up Secure Email Threat Defense?

Cisco does not physically accept your Microsoft 365 credentials, nor do we cache or store the Global Admin's credentials. Secure Email Threat Defense redirects you to Microsoft's Azure application registration process so it can issue an authentication token for Microsoft's APIs. Only a Global Admin can authorize this token.

For more information, refer to the Microsoft documentation for a discussion of admin rights for applications:  
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/>

## What access permissions does Secure Email Threat Defense request from Microsoft?

For Microsoft 365 Authentication mode, Secure Email Threat Defense requests access permissions from Microsoft. These permissions depend on whether you choose Read/Write or Read mode. Details about the permissions can be found in the linked Microsoft documentation.

Both Microsoft Authentication modes request: **Organization.Read.All** and **User.Read**

- <https://learn.microsoft.com/en-us/graph/permissions-reference#organizationreadall>
- <https://learn.microsoft.com/en-us/graph/permissions-reference#userread>

Read/Write mode requests: **Mail.ReadWrite**

- <https://learn.microsoft.com/en-us/graph/permissions-reference#mailreadwrite>

Read mode requests: **Mail.Read**

- <https://learn.microsoft.com/en-us/graph/permissions-reference#mailread>

## Why did I receive a welcome email from Malware Analytics/Threat Grid?

A minimal Cisco Secure Malware Analytics (formerly Threat Grid) account is created as part of the Secure Email Threat Defense account creation process. The new Malware Analytics account is not linked to any existing Malware Analytics account you may have. You do not need to take any action on the Malware Analytics account to set up Secure Email Threat Defense.

## How can I find my journal address?

Your journal address is shown on the Secure Email Threat Defense setup page. If you need to find it after your initial setup, you can locate it on the **Administration > Business** page in the Account section.

## Why do I receive a registration error when I try to register my Microsoft 365 tenant?

If you try to register a tenant that has previously been registered to a different Secure Email Threat Defense account, your authorization will fail. Secure Email Threat Defense does not allow multiple accounts with the same Microsoft tenant ID.

## How long does Cisco retain my journal data?

Data is kept according to the [Cisco Secure Email Threat Defense Privacy Data Sheet](#).

## Can a user be added to more than one Secure Email Threat Defense instance?

A user can access multiple Secure Email Threat Defense instances using the same Security Cloud Sign On account. This makes it easier to keep track of each instance without having to log out and log back in with a separate account.

Add the user to additional instances by creating a new user from **Administration > Users** page. Secure Email Threat Defense accounts using the same Security Cloud Sign On will be available from their User menu. Note that this access is limited to Secure Email Threat Defense accounts in the same region.





# Login Issues

## How can I find more information about problems logging in to Secure Email Threat Defense?

Secure Email Threat Defense uses Cisco Security Cloud Sign On for user authentication management. For information on Security Cloud Sign On, including FAQ, see the [Cisco Security Cloud Sign On Quick Start Guide](#).

## Why can't I log in with my email address?

Make sure the email address you are using for Security Cloud Sign On matches the email associated with your Secure Email Threat Defense account. Some customers may have Security Cloud Sign On accounts using multiple email addresses. Secure Email Threat Defense does not support multiple email addresses for a single user. You must log in using the email address that was used to create your Secure Email Threat Defense account. If you don't know which email address was used, check with your Secure Email Threat Defense administrator.

## How can I reset my password?

During the Security Cloud Sign On login process you will be prompted to enter your password; click **Forgot password** to get to the **Reset Password** page.

## Why do I see a 400 Bad Request error when trying to sign in to Security Cloud Sign On with my Microsoft account?

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 work around this issue, make sure both first name and last name are defined in your Microsoft 365 account.

## How can I access Secure Email Threat Defense from the SecureX Application Portal?

To access Secure Email Threat Defense from the [SecureX Application Portal](#), locate your region (North America, Europe, or APJC) and find the Secure Email Threat Defense icon.

## How can I switch between Secure Email Threat Defense instances?

You can access multiple Secure Email Threat Defense instances using the same Security Cloud Sign On account. This makes it easier to keep track of each instance without having to log out and log back in with a separate account. Secure Email Threat Defense accounts using the same Security Cloud Sign On are available from your User menu. Note that this is limited to accounts in the same region.

## How can I find out the operational status of Secure Email Threat Defense?

If you suspect Secure Email Threat Defense may be down or having an issue, check our system status page. You can access the page from the User Profile menu, or directly at <https://ciscosecureemailthreatdefense.statuspage.io>.





# Secure Email Threat Defense and Microsoft 365

## Does Secure Email Threat Defense honor senders or domains from an allow list in Microsoft 365?

Yes. Secure Email Threat Defense honors senders and domains added to your spam filter allow lists in Microsoft 365 for Spam and Graymail messages. MS Allow lists are not honored for Malicious or Phishing verdicts.

In the classic Exchange admin center, this is accessible from **Exchange admin center** > **protection** > **spam filter**.

In the new Microsoft 365 security center, you can access this setting here: <https://security.microsoft.com/antispam>

Because of some recent changes to Microsoft's MSAllowList header, 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 Threat verdicts. That is, Safe Sender messages with Spam or Graymail verdicts will not be remediated.

## Does Secure Email Threat Defense honor actions my users take on Junk mail in Outlook?

Users may mark email using the Outlook Junk options, such as **Never Block Sender** or **Add to Safe Senders**. 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 Threat verdicts. That is, Safe Sender messages with Spam or Graymail verdicts will not be remediated.

## What is the journaling size limit?

Any message over 150 MB will not be journaled by Microsoft 365.

## Why aren't all of my domains showing in Secure Email Threat Defense?

Secure Email Threat Defense imports domains with email capabilities associated with your tenant. If a domain does not have email capabilities, it is not shown in Secure Email Threat Defense.

## Where can I find more information about journaling in Microsoft 365?

Refer to the Microsoft documentation: <https://docs.microsoft.com/en-us/exchange/security-and-compliance/journaling/journaling>





# Messages and Search

## How do I let Cisco know a message was misclassified?

If you believe a message was not classified correctly (false positive or false negative), you can [reclassify](#) the message. The message will be queued for review by Cisco Talos. Talos may use the feedback to influence future classifications.

## Why am I still getting emails from a sender that I already reclassified?

Reclassifying only affects the verdict on the selected message(s). It does not indicate any change to future messages from the selected sender or based on the message content. The message will be queued for review by Cisco Talos. Talos may use the feedback to influence future classifications.

If you have a Secure Email Gateway (SEG) in place, you should indicate this on the **Policy** page. This information will help decrease false positives.

For false positive messages, consider adding a [Verdict Override](#) message rule.

If you continue to have this issue, contact [Support, page 13](#).

## Why do some messages appear twice on my Messages page?

Duplicate entries are a result of Microsoft creating multiple journals for a single email. This can happen for several reasons. For example, mail rules set by the Exchange admin, or mail sent to groups with non-domain users.

## What does undisclosed recipient mean?

Undisclosed recipient indicates the email had no listed recipients. For example, when a BCC (blind carbon copy) is sent to a recipient. Secure Email Threat Defense does not track BCC recipients, but detection and remediation are not impacted.





# Support

## How can I access Secure Email Threat Defense documentation?

You can access Secure Email Threat Defense documentation directly from Secure Email Threat Defense using the Help menu, or at the following links.

- [Cisco Secure Email Threat Defense User Guide](#)
- [Cisco Secure Email Threat Defense Release Notes](#)

## How can I get help setting up and using Secure Email Threat Defense?

For help setting up and using Secure Email Threat Defense, contact the Email Security Customer Success team at [etd-acivations@cisco.com](mailto:etd-acivations@cisco.com).

## How can I contact customer support?

If you are a Secure Email Threat Defense PoV (Proof of Value) evaluation customer, email [cmd-support@cisco.com](mailto:cmd-support@cisco.com).

If you are a fully licensed Secure Email Threat Defense customer:

- Open an online support case: <https://www.cisco.com/c/en/us/support/index.html>
- Email [TAC@cisco.com](mailto:TAC@cisco.com)
- Call Cisco TAC at any of the worldwide phone numbers found here: <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

**Note:** To open a case, your Secure Email Threat Defense contract must be linked to your cisco.com account. If you do not already have a cisco.com account, go [here](#) to create one.

