Cisco Secure Email Threat Defense FAQ

First Published: 2021-04-26

Last Updated: 2025-12-03

Table of Contents

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

In this chapter:

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 and Write or Read mode. Details about the permissions can be found in the linked Microsoft documentation.

MS Graph API Permission	ETD Mode	ETD Usage
Mail.Read	Read	■ EML download ■ Reclassification feedback
Mail.ReadWrite	Read and Write	■ All Mail.Read usages ■ Remediation ○ Create quarantine folders

MS Graph API Permission	ETD Mode	ETD Usage
		◦ Move messages ◦ Delete messages
User.Read	All	Default requesting user permission
Domain.Read.All	All	Import mail servers
Organization.Read.All	All	Import domains
User.Read.All	All	■ Recipient validation ■ Group based policy exceptions
Group.Read.All	All	■ Recipient validation ■ Group based policy exceptions
GroupMember.Read.All	All	Group based policy exceptions

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

In this chapter:

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

In this chapter:

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

Yes, for businesses using journalled traffic sources. 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 Threat verdicts (BEC, Scam, Malicious, Phishing); these items will be remediated according to your policy settings.

In the Microsoft Defender, you can access this setting here: https://security.microsoft.com/antispam

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 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

In this chapter:

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. This feedback may be used to influence future classifications.

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.

Further Support

In this chapter:

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 https://docs.cmd.cisco.com/en/Content/homeGlobal.htm

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.

How can I contact customer support?

To contact Cisco support:

- Open an online support case: https://www.cisco.com/c/en/us/support/index.html
- Email 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.

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.