



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.