Manage Users

Manage your user accounts from the **Administration** > **Users** page.

Secure Email Threat Defense uses Cisco Security Cloud Sign On (formerly SecureX sign-on) for user authentication management. For information on Security Cloud Sign On, see https://cisco.com/go/securesignon.

Note: If you are an existing Cisco XDR, Cisco Secure Malware Analytics (formerly Threat Grid), or Cisco Secure Endpoint (formerly AMP) customer, be sure to sign in with your existing Security Cloud Sign On credentials. If you are not an existing user, you must create a new Security Cloud Sign On account

Although Security Cloud Sign On allows you to sign on with other types of accounts, we recommend using a Security Cloud Sign On account to keep your Cisco security product accounts connected.

Multi-Account Access

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 using a separate Security Cloud Sign On account.

Add a user to additional Secure Email Threat Defense instances by following the steps in Create a New User, page 48. Accounts using the same Security Cloud Sign On account will be available from their User menu. Note that this access is limited to Secure Email Threat Defense instances in the same region (North America, Europe, Australia, or India).

User Roles

Role-based access control (RBAC) allows you to have users with different levels of control or access within the application. Secure Email Threat Defense users can be created in the roles described in the following table.

Table 1 User Roles

Role	Description
super-admin	These users have access to all features in Secure Email Threat Defense. They can alter settings and policies, reclassify and remediate messages, download EML files, and view email message previews.
admin	These users have all the capabilities of super-admins, except they cannot create, edit, or delete super-admin or admin users.
analyst	These users can use the search and insight capabilities. They can reclassify and remediate messages, but cannot delete messages from user mailboxes. They cannot make changes to the account setup or policies or create, edit, or delete new users. They also cannot download EML files or view email message previews.
read-only	These users can use the search and insight capabilities. They cannot reclassify or remediate messages, make changes to the account setup or policies, or create new users. They also cannot download EML files or view email message previews.

Table 2 Access to Features by Role

Feature Group	Feature	Role
Administration	Add/Edit Users	■ super-admin ■ admin
	Create/Edit/Delete Admins	■ super-admin
Business	Toggle Google Analytics	■ super-admin ■ admin
	View Notification Email	■ super-admin ■ admin
	Edit Retro Notification Email	■ super-admin ■ admin
	Download Audit Logs	■ super-admin ■ admin ■ analyst ■ read-only
	View Quarantine Folder	■ super-admin ■ admin
	View Notifications	■ super-admin ■ admin ■ analyst ■ read-only
Policy	Edit Policy	■ super-admin ■ admin
	Import Domains	■ super-admin ■ admin
	Modify Message Rules	■ super-admin ■ admin ■ analyst
Search	Search from Home Page	■ super-admin ■ admin ■ analyst ■ read-only

Table 2 Access to Features by Role

Feature Group	Feature	Role
Messages	View Expansion	■ super-admin ■ admin ■ analyst ■ read-only
	View Reports	■ super-admin ■ admin ■ analyst ■ read-only
	Download EML	■ super-admin ■ admin
	View Email Preview	■ super-admin ■ admin
Reclassify and Remediate	Reclassify	■ super-admin ■ admin ■ analyst
	Move Message	■ super-admin ■ admin ■ analyst
	Quarantine Message	■ super-admin ■ admin ■ analyst
	Delete Message	■ super-admin ■ admin
	View Remediation Error Log	■ super-admin ■ admin ■ analyst ■ read-only

Table 2 Access to Features by Role

Feature Group	Feature	Role
Cisco XDR	Authorize Dashboard	■ super-admin ■ admin
	Authorize Ribbon	■ super-admin ■ admin ■ analyst ■ read-only
API	Access API Tab	■ super-admin ■ admin
	Access API Key	■ super-admin ■ admin
	Generate API Credentials	■ super-admin ■ admin

Create a New User

Complete the following steps to create a new user:

1. Select **Administration** > **Users**.
2. Click **Add New User**.
3. Enter the user's credentials, select a role, then click **Create**.

   Note: The user's email address *must* match the one they use for their Security Cloud Sign On account.

The user receives an email with the subject **Welcome to Cisco Secure Email Threat Defense**. They must follow the directions in the email to set up a Security Cloud Sign On account (if they do not already have one) and log in.

Edit a User

You can update a user's role. You cannot edit a user's email address. If a user changes their name, they must update it in their Security Cloud Sign On account.

To edit a user's role:

1. Select **Administration** > **Users**.
2. Click the pencil under the Action column.
3. In the Edit User dialog, select a new role for the user, then click **Save changes**.

Delete a User

Complete the following steps to delete a user:

1. Select **Administration** > **Users**.

2. Click the X icon under the Action column.
3. Click **Delete** in the Confirm Deletion dialog to complete the action.

A status message shows the deletion is complete. This deletes the user’s account from Secure Email Threat Defense, but does not delete their Security Cloud Sign On account. If you want to delete a user from multiple Secure Email Threat Defense instances, you must complete these steps for each instance.