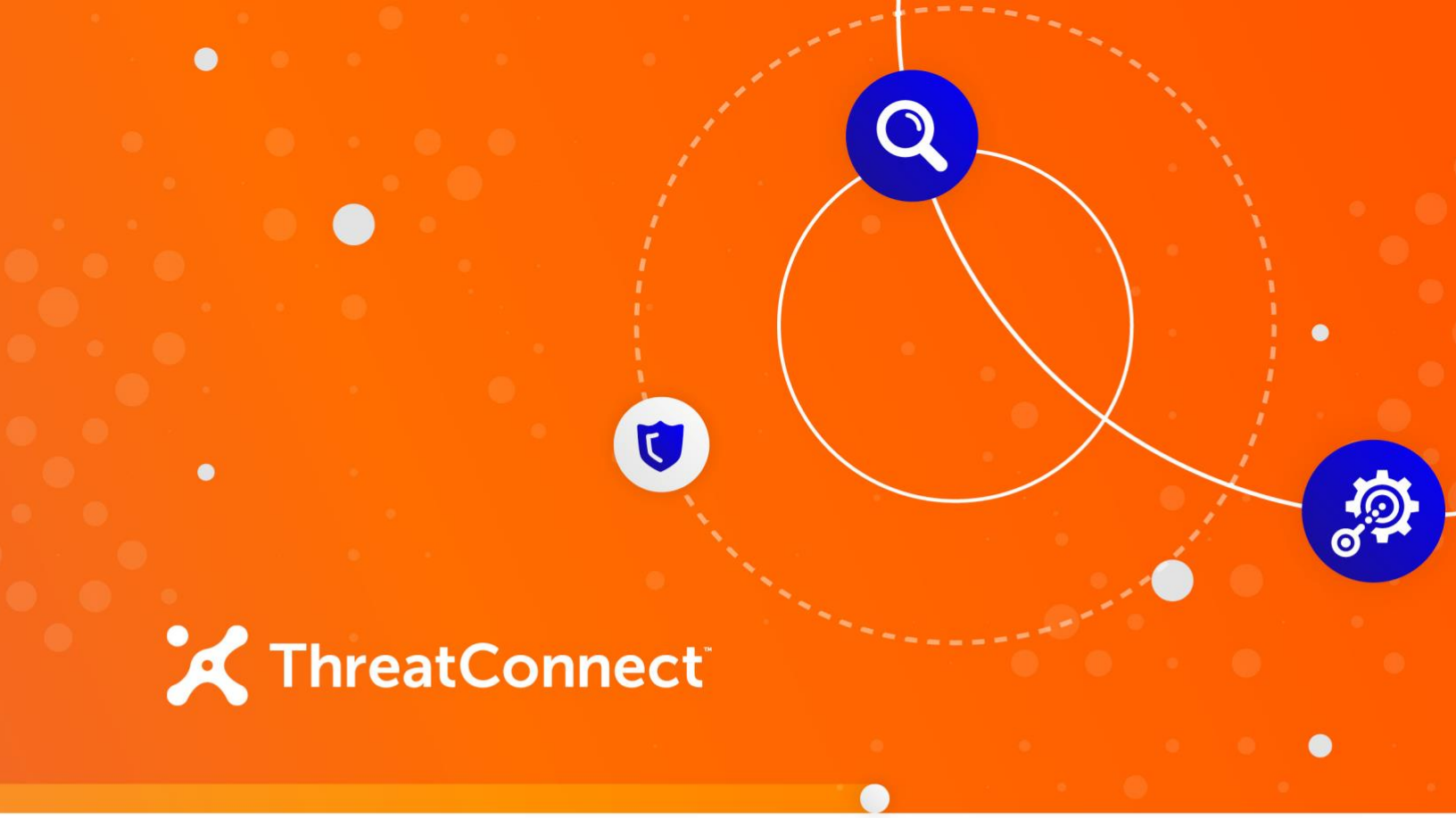

Organization Administration

User Guide

Software Version 6.1

February 24, 2021

10012-09 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: 1.703.229.4489
www.ThreatConnect.com

Table of Contents

Organization Administration

Getting Started

Organization Administration is carried out in ThreatConnect® by the Org Administrator for each Organization account. Org Administrators have full administrative control for their Organization, allowing them to assign or delete user accounts, set permissions, set pseudonyms for individual users or for the Organization, and join Communities.

At least one Org Administrator must exist per Organization account, and one is created at the same time as the Organization. However, there can be more than one Org Administrator in an Organization.

Account Roles

Table 1 provides an overview of account roles.

Table 1

Account Role	Description
Read Only User	This role offers viewing or reading capability only.
Standard User	This role has full accesses to create, delete, or modify any information in the Organization.
Sharing User	This role has the same privileges as a User, but can also share or contribute Groups to other Communities of which the Organization is already a part. It can also export data in bulk from the Organization.
Organization Administrator	This role has full control for administration of the Organization account. It has the same privileges as the Sharing Administrator, but it can also create and delete Organization users, configure Community privileges for users, send invites, view Organization logs, and join Communities.
App Developer	This role is for anyone with an Organization Administration account or higher, and it allows the individual to build and release apps.
Playbook API User	This role allows API-level user functionality.

Managing Org Users

Creating User Accounts

Follow these steps to create additional Organization user accounts:

1. Log in with an Org Administrator Account.

2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2).

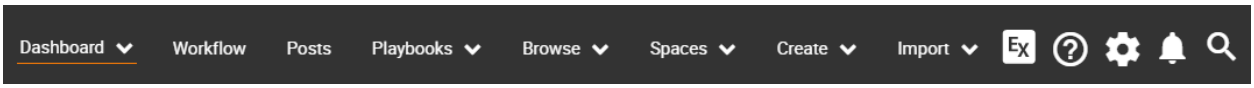

Figure 1

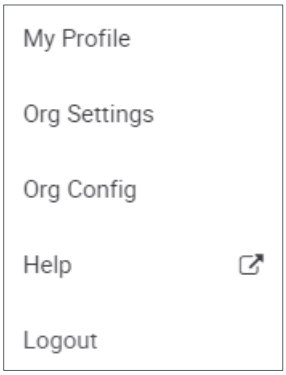

Figure 2

3. Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).

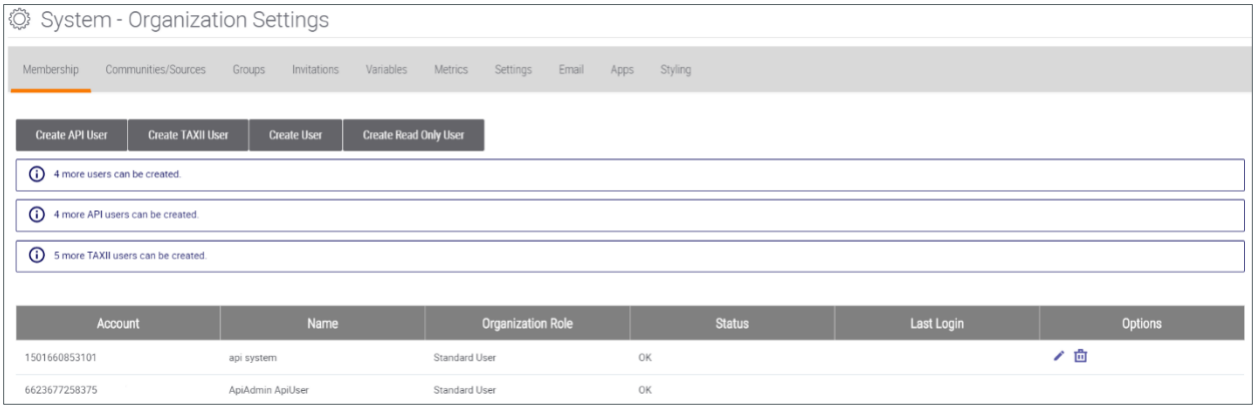

Figure 3

4. Click the **Create User** button, and the **User Administration** pop-up screen will appear (Figure 4).

   NOTE: Above the Account table, the Organization Settings screen displays how many more users can be added by the Organization account.

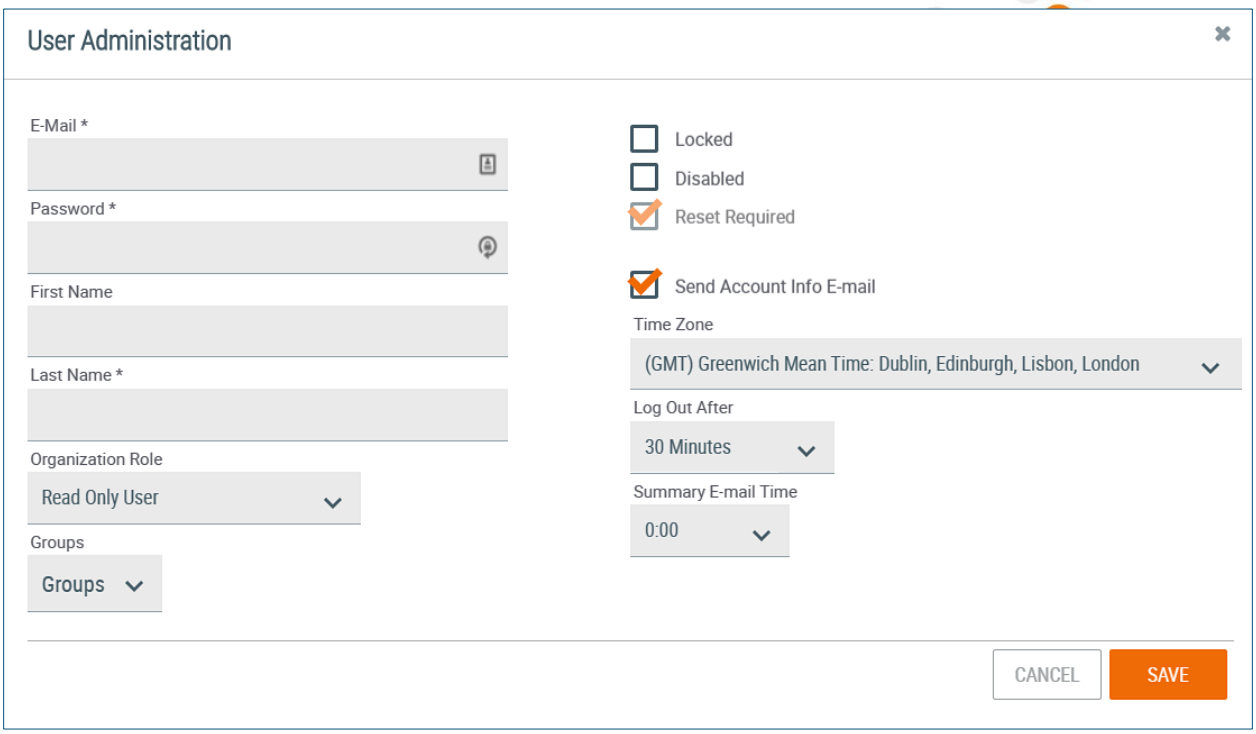

Figure 4

5. Fill in the required fields in order to create and configure the user account.
   a. **E-Mail**: Click in the box to enter an email address that will also be the name of the user account.
   b. **Password**: Click in the box to set the initial user password in this field, which is subject to the ThreatConnect password policy defined within the system settings.
   c. **First Name**: Click in the box to enter the user's first name, which, along with the last name, is what other user accounts see when the user posts within the Organization or in a full-profile Community.
   d. **Last Name**: Click in the box to enter the user's last name, which, along with the first name, is what other user accounts see when the user posts within the Organization or in a full-profile Community.
   e. **Organization Role**: Click on the drop-down menu to select one of the following roles— Read Only User, Standard User, Sharing User, Organization Administrator, App Developer, or Playbook API User.
   f. **Groups**: Click the drop-down menu to enter a Group for which to search.
   g. **Locked**: Click on the box if it is checked in order to unlock a user account that has been locked by ThreatConnect.
   h. **Disabled**: Click the checkbox to disable a user account, which is typically done when a user no longer requires ThreatConnect access and the Administrator wishes to retain log integrity.

i. **Reset Required**: Click the checkbox to force a user to change the account password upon next login. This box is checked by default upon account creation, and it is unchecked once the password has been changed.

NOTE: When initially creating the account, the Reset Required box cannot be unchecked. To uncheck the box, first create the account, edit it, and uncheck the setting, which enforces tighter security.

j. **Send Account Info E-mail**: Click the checkbox to receive an email with the information corresponding to this account.

NOTE: This setting must be set to "true" in the System Settings screen in order for the checkbox to appear.

k. **Time Zone**: Click on the drop-down menu to select the appropriate time zone.

l. **Log Out After**: Click on the drop-down menu to select a time interval upon which a user will be logged out after a corresponding period of inactivity.

m. **Summary E-mail Time**: Click on the drop-down menu to set the time at which a user account will receive daily summary emails of followed items, or other notifications, from ThreatConnect.

6. Click the **SAVE** button to create the User account.
7. Log out and log back in with the new User account's credentials.
8. The **Password Reset Required** screen will appear (Figure 5).

Figure 5

9. Enter a new password and click **Sign In**. The **Profile Settings** screen will appear (Figure 6).

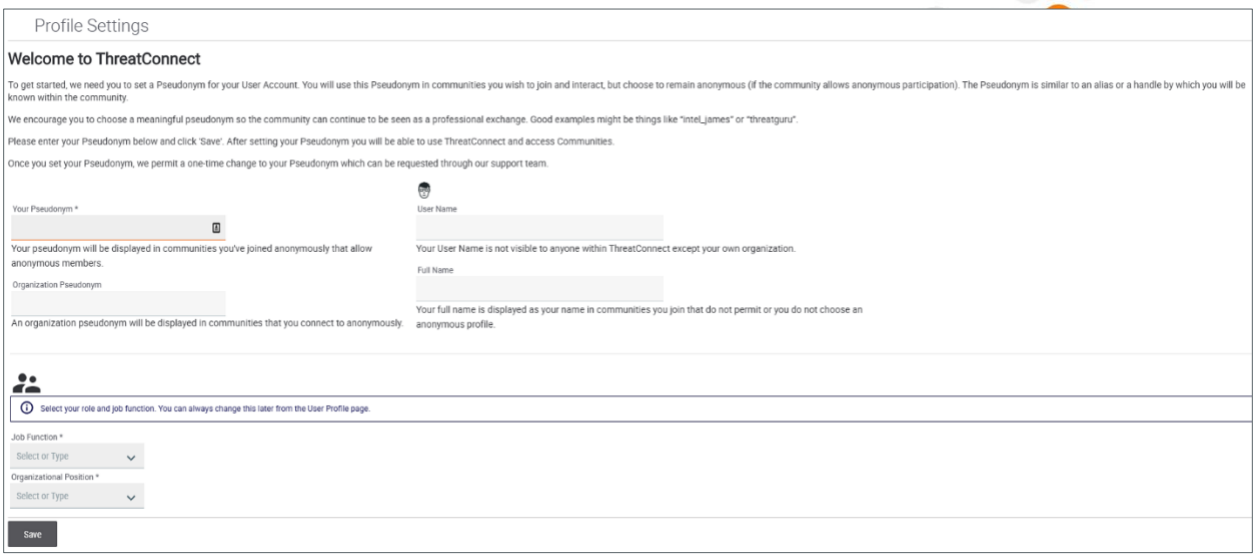

Figure 6

10. Enter a **Pseudonym**, **Job Function**, and **Organizational Position** and click **Save**.

To create Read-Only user accounts, follow the preceding steps, but click the **Create Read Only User** button in Step 4. Note that the Organization Role is locked, and such users that join a Community or Source will have read-only permissions. A benefit to creating Read-Only Users is that they do not count against Organization limits. Administering User Accounts

Follow these steps to administer or change settings of an existing Organization user account:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Modify** icon of the user account to be configured. The **User Administration** pop-up screen will appear (Figure 4). See Step 4 of the previous section, *Creating User Accounts*, for instructions and a description of all available fields.

Two-Step Verification

Some users will opt to enable two-step verification to increase the security of their ThreatConnect account. Google® Authenticator or any Time-based One-Time Password (TOTP)–compatible authentication service can be used. This procedure will enhance the security of an Organization's data within ThreatConnect by requiring a time-based key, in addition to a valid user name and password combination.

The Google Authenticator logo will appear in the **Status** column (under the **Membership** tab of the **Organization Settings** screen) of those user accounts for which 2-Step Verification has been enabled.

Creating API User Accounts

NOTE: In order to create an API user account, Administrators must have this feature enabled in their license. If they do not, they must contact their account manager or the sales team at sales@threatconnect.com to request a license upgrade. Also, creating an API user account will decrease the total number of user accounts that are available, as will creating a new user account.

Follow these steps to create an API user account:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. From the **Organization** drop-down menu on the upper right of the screen, select the Organization for which the new API user will be created
4. Click the **Create API User** button, and the **API User Administration** screen will appear (Figure 7).

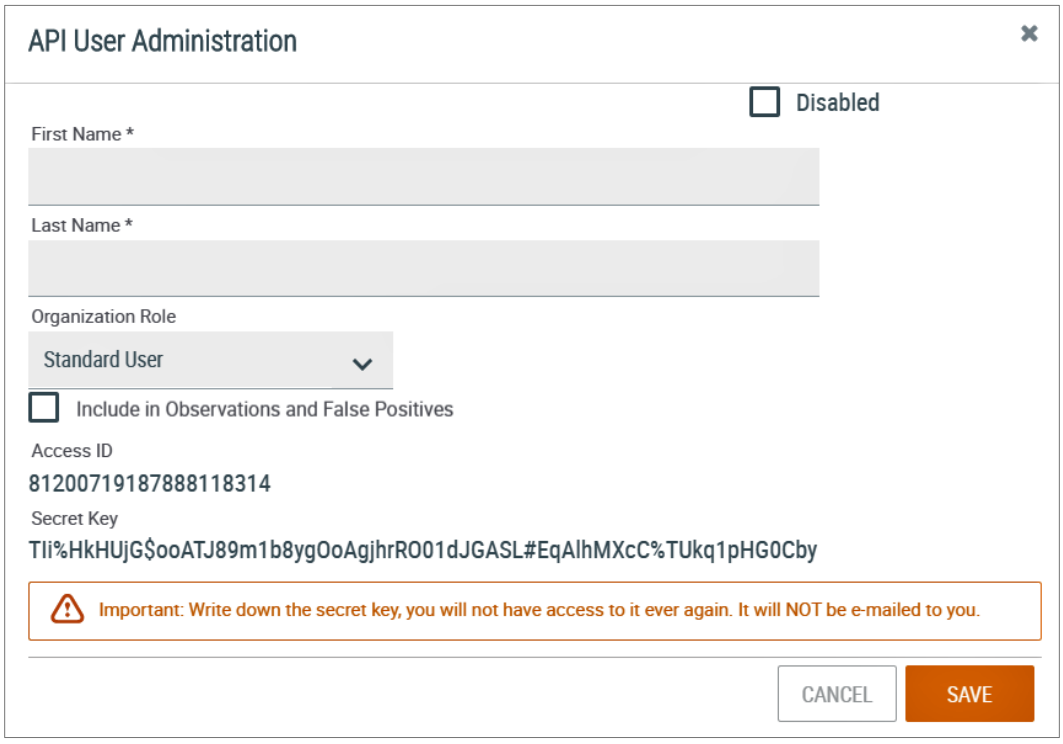

Figure 7

a. **Disabled**: Check this box to disable individual API users.

b. **First Name**: Click in the box to enter the API user's first name.

c. **Last Name:** Click in the box to enter the API user's last name.

NOTE: If the API account will be used with specific application integration, it may be helpful to set the user's first and last name as something indicative.

d. **Organization Role**: Click on the drop-down menu to select one of the following roles—Standard User, Sharing User, Organization Administrator, App Developer, or Playbook API User.

e. **Include in Observations and False Positives**: Check this box to display the API account on an Indicator's **Details** screen. If used with an integration that supports it, Observations and False Positives will be tied to this API account and tracked.

f. **Access ID**: The Access ID populated in this field acts as the identification for the account when used to access the API and is associated with the Secret Key, which is provided in the next field.

g. **Secret Key**: The Secret Key is generated uniquely for each account. It is used for authentication to the API. Without it, access will be denied.

NOTE: Record the Secret Key! Once the account is created, the system will not display the key again, and it cannot be sent to the user.

5. Click the **SAVE** button to create the API user account.

Creating TAXII User Accounts

Creating a Trusted Automated eXchange of Indicator Information (TAXII™) user account sets up login credentials (username and password) that may be used in a TAXII client to access the ThreatConnect TAXII server and retrieve data from the user's Organization and any Communities or Sources to which the user has access. The TAXII Client will require a Discovery URL of the form https://api.threatconnect.com/taxii/discovery. The POLL URL is of the form https://api.threatconnect.com/taxii/poll. The exact URL will differ if the user has a private instance of ThreatConnect.

Collection Information requests can be made to both the Discovery and Collection-Management endpoints. The ThreatConnect TAXII Server supports Discovery, Collection-Management, and POLL requests, including multi-part POLL exchanges. TAXII 1.1 documentation may be found at: https://taxiiproject.github.io/releases/1.1/TAXII_Services_Specification.pdf.

Follow these steps to create a TAXII user account:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. From the **Organization** drop-down menu on the upper right of the screen, select the Organization for which the new TAXII user will be created
4. Click the **Create TAXII User** button, and the **TAXII User Administration** screen will appear (Figure 8).

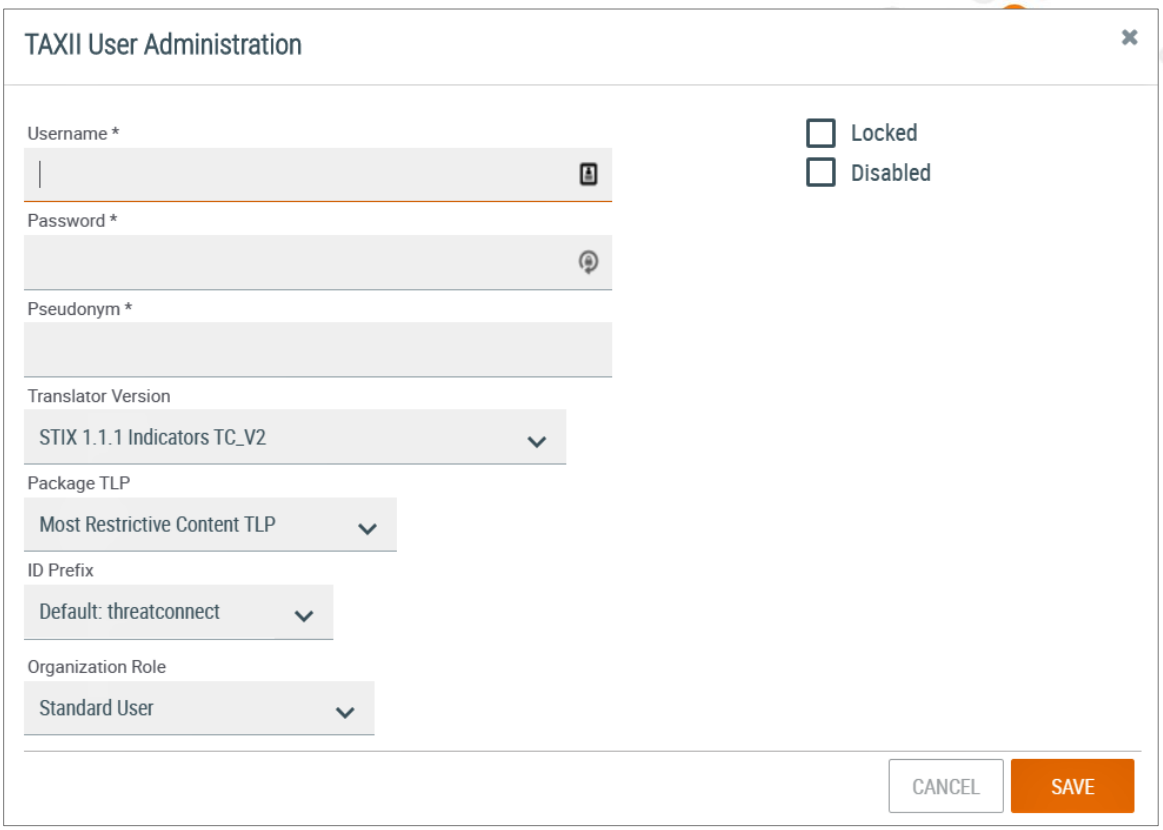

Figure 8

a. **Username**: Click in the box to enter the TAXII account's username.

b. **Password:** Click in the box to enter the TAXII account's password.

c. **Pseudonym**: Click in the box to enter the TAXII account's pseudonym.

d. **Translator Version**: Click the drop-down menu to select the type of STIX™ data that can be delivered via the TAXII server.

e. **Package TLP**: Click the drop-down menu to select the desired security-label level.

f. **ID Prefix:** Click the drop-down menu to assign a namespace prefix for generated STIX IDs. The default prefix is **threatconnect**, but the user can also choose the **Collection Name** or a **Custom** name as a prefix.

a. **Organization Role**: Click on the drop-down menu to select one of the following roles— Read Only User, Standard User, Sharing User, Organization Administrator, App Developer, or Playbook API User.

b. **Locked**: Click on the box if it is checked in order to unlock a user account that has been locked by ThreatConnect.

c. **Disabled**: Click the checkbox to disable a user account, which is typically done when a user no longer requires ThreatConnect access and the Administrator wishes to retain log integrity

5. Click the **SAVE** button to create the TAXII user account.

Creating Read Only User Accounts

A user with a Read Only account does not have write or update access. Follow the steps in the Creating User Accounts section. The screen for creating a Read Only account is identical to the **User Administration** screen (Figure 4), except that the **Organization Role** option is grayed out.

Deleting a User Account

Follow these steps to delete a user account:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click on the **Delete** icon under the **Options** column of the account to be deleted.

Managing Community Membership

Org Administrators have the ability to manage their Organizations' membership in Communities. They can accept invitations to join a Community sent by a Community Director, change their Organizations' anonymity settings for each Community where they are members, and remove their Organizations from a Community.

Viewing Current Community Membership and Settings

Follow these steps to view an Organization's current Community membership and settings:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will appear (Figure 9), which displays current Community memberships and configuration settings for all Communities.

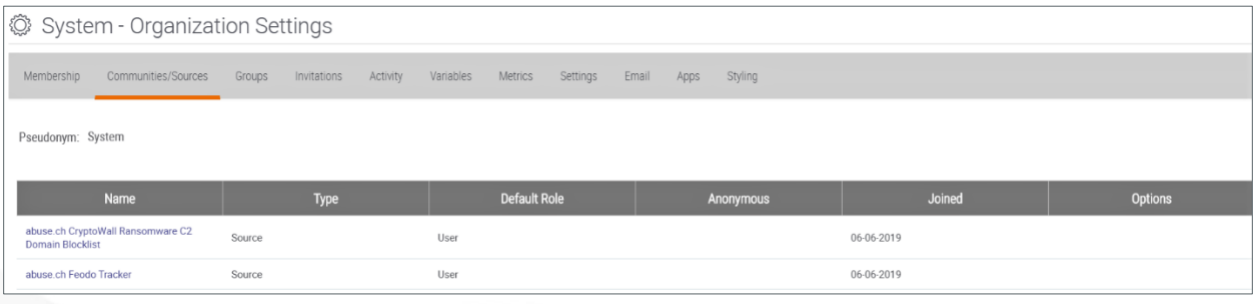

Figure 9

a. **Name**: This column displays the Community Name, which is hyperlinked; click on it to navigate to the **Community Profile** screen.

b. **Type**: This column indicates whether the object is a Community or a Source.

c. **Default Role**: This column displays the default role of Organization members in the Community. See the *ThreatConnect Community and Source Administration Guide* for more details on Community roles.

NOTE: A Community Director account may change the role of Organization members within a Community.

d. **Anonymous**: This column indicates an Organization's anonymity within a Community. For Communities where anonymity is allowed, an Org Administrator may configure this setting as on or off. If anonymity is not allowed in a Community, the Org Administrator will not be able to configure this setting. Anonymity can also be configured on a Community's **Profile** screen.

NOTE: Changing this setting will affect ALL Organization user accounts in a Community.

e. **Joined**: This column indicates the date on which a Community was joined.

f. **Options**: Currently, the only option available in this column is to exit the Community. This is accomplished by clicking the **Delete**  icon in the field.

Changing an Organization's Pseudonym

Typically, an Organization's pseudonym is set when the account is created, and it cannot be changed. However, a System Administrator account may enable a one-time change of an Organization or user account's pseudonym.

Follow these steps to change an Organization's pseudonym:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the Communities/Sources tab, and the Communities/Sources screen will appear (Figure 9).
4. Click on the text of the current Organization's pseudonym (the text will have become editable if a System Administrator account has enabled a one-time change of the pseudonym), and change the pseudonym.
5. Click the checkmark inside the circle.

NOTE: Once the checkbox is clicked, it is not possible to modify the pseudonym again without having a System Administrator enable another change.

Leaving a Community

Follow these steps to leave a Community:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will appear (Figure 9).
4. Click on the **Delete** icon in the **Options** column of the Community to leave.

   NOTE: This action does not delete a Community. That is accomplished in Account Settings.

Creating Groups

Follow these steps to create a group within a Community:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Groups** tab, and the **Groups** screen will appear (Figure 12).

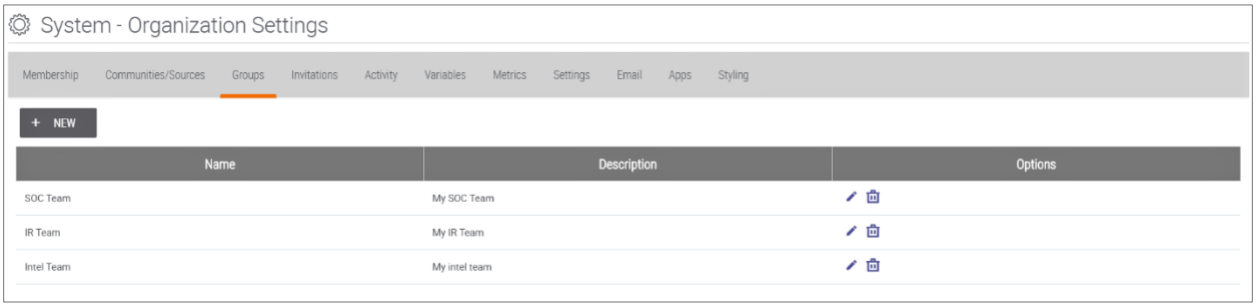

Figure 10

4. Click the **+ NEW** button, and the **Create Group** screen will appear (Figure 11).

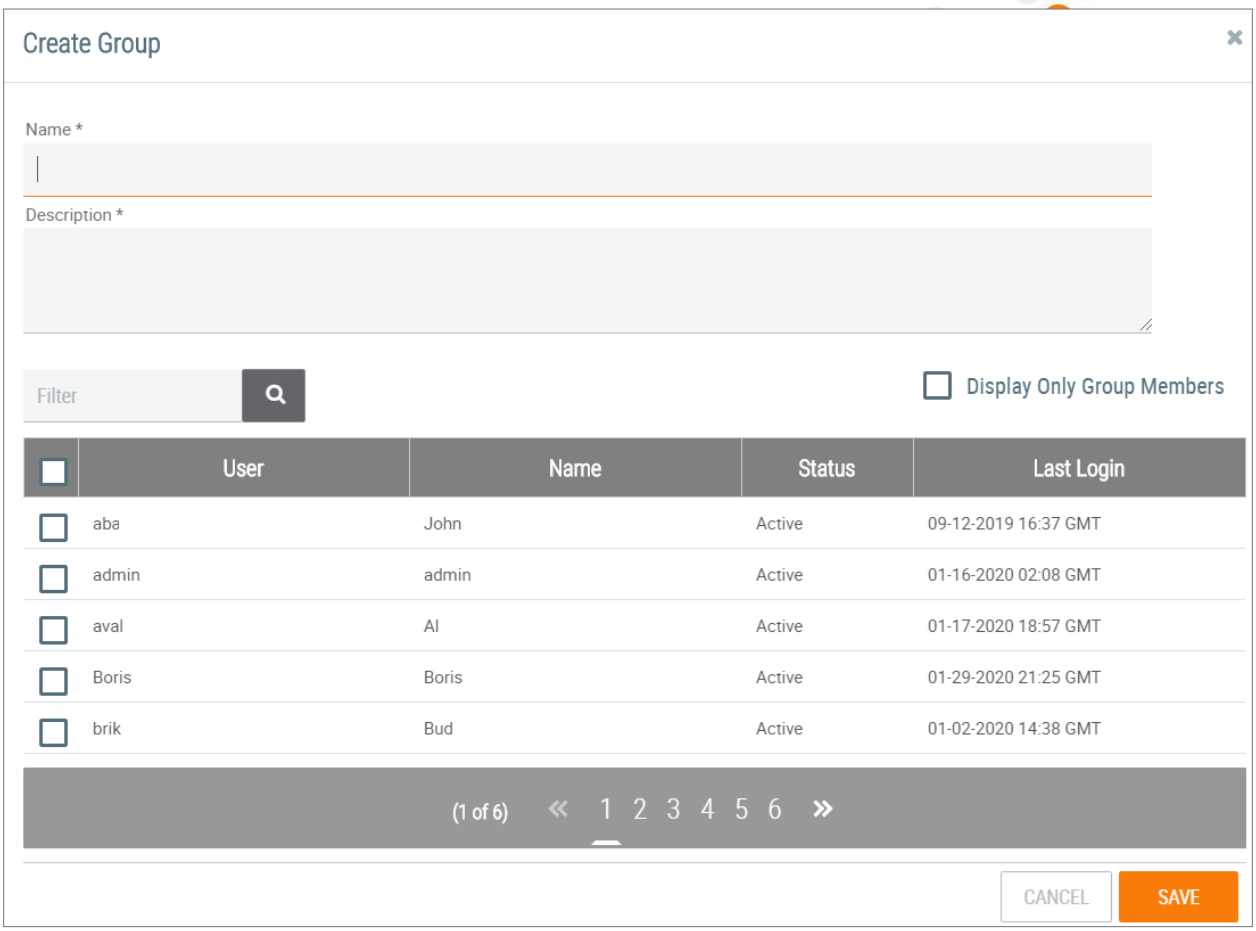

Figure 11

5. Enter a **Name** and a **Description** for the group, and check the boxes next to the names of the **Users** that will make up the group.
6. Click the **SAVE** button.

Invitations

Follow these steps to accept an invitation to join a Community:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Invitations** tab, and the **Invitations** screen will appear (Figure 12).

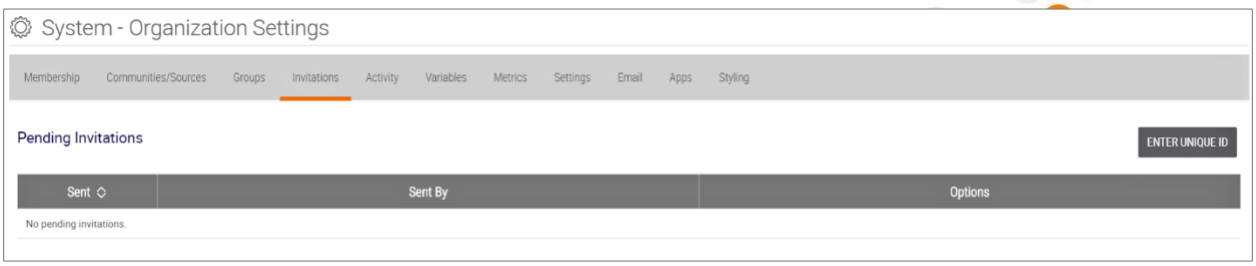

Figure 12

4. Any invitations sent to an Administrator's account will be visible in the **Pending Invitations** table. In the **Options** column, an Administrator can accept or reject an invitation.
5. Click **Accept** to join a Community, and the **Accept Invite** pop-up screen will appear (Figure 13), explaining the Community's anonymity policy.

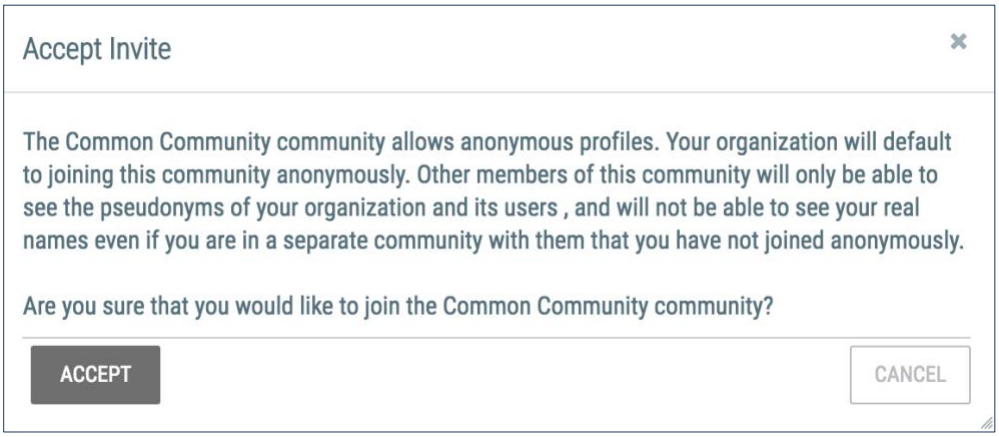

Figure 13

6. Click the **ACCEPT** button to join the new Community.
7. If the email address is not currently associated with an account, the recipient will be able to use the invite code contained in the email to establish the connection after establishing an account by clicking the **ENTER UNIQUE ID** button (Figure 12).

Activity Logs

Viewing Activity Logs

The Activity Logs display activity within the system, including logins, creations, and deletions.

Follow these steps to view the Activity Logs:

1. Log in with a **System Administrator** account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Activity** tab, and the **Activity** screen will appear (Figure 14).

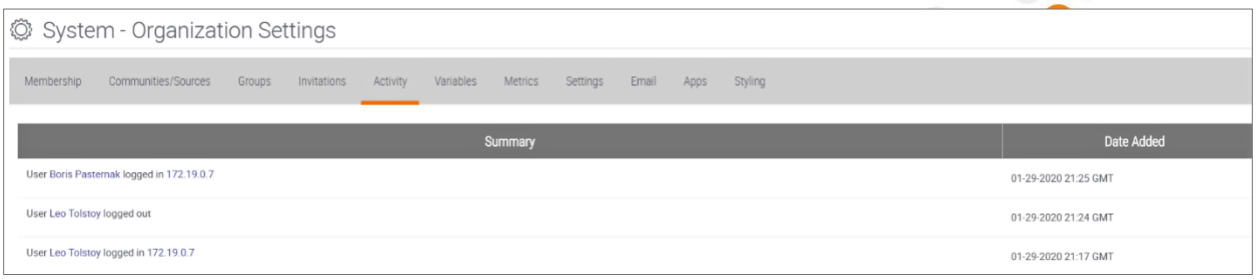

Figure 14

4. Click on the drop-down menu in the upper right-hand corner to view the activity of a specific Organization.

Variables

Variables can be preconfigured and used to populate certain fields, such as the ThreatConnect API Access ID or Secret Key.

Adding New Variables

Follow these steps to add a new variable:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Variables** tab, and the **Variables** screen will appear (Figure 15).

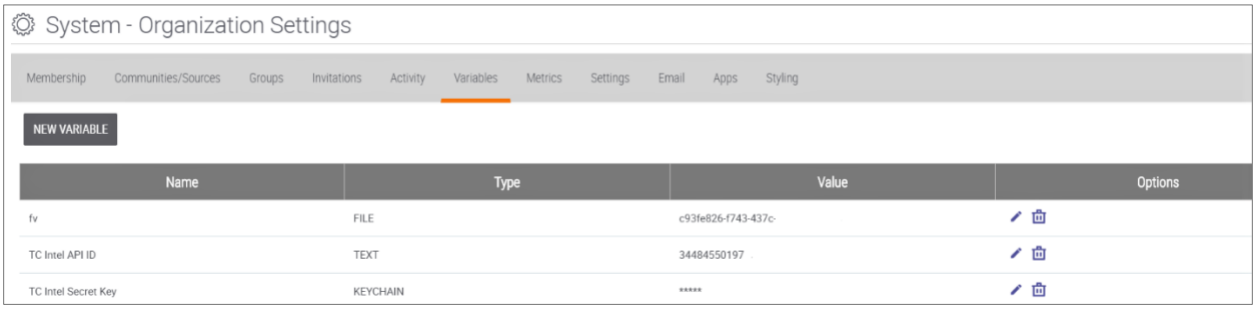

Figure 15

4. Click the **NEW VARIABLE** button, and the **Property** pop-up screen will appear (Figure 16).

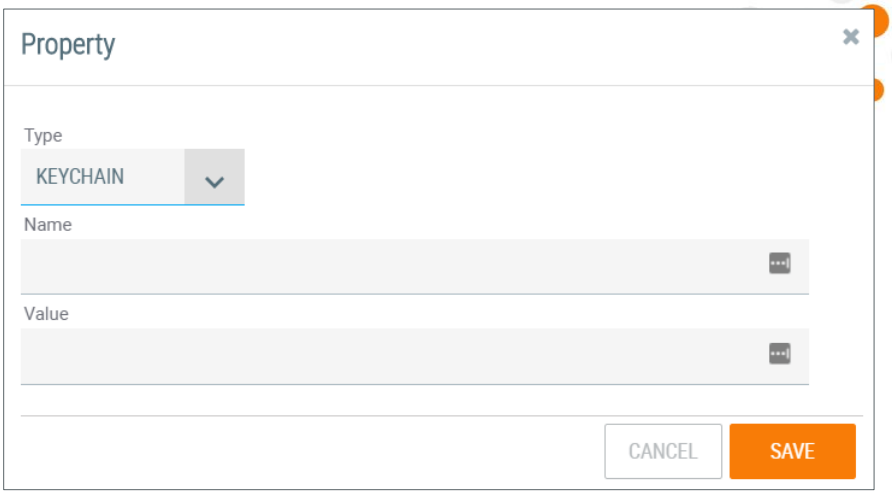

Figure 16

5. Enter the required information in the fields, and click the **SAVE** button.

Custom Metrics

Custom metrics allow users to track data not available through other functionality. For example, a user may want to know the number of times a particular Playbook was run. This task can readily be carried out through the **Metrics** feature at the organizational level.

Creating a Custom Metric

Follow these steps to create a custom metric:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Metrics** tab, and the **Metrics** screen will appear (Figure 17).

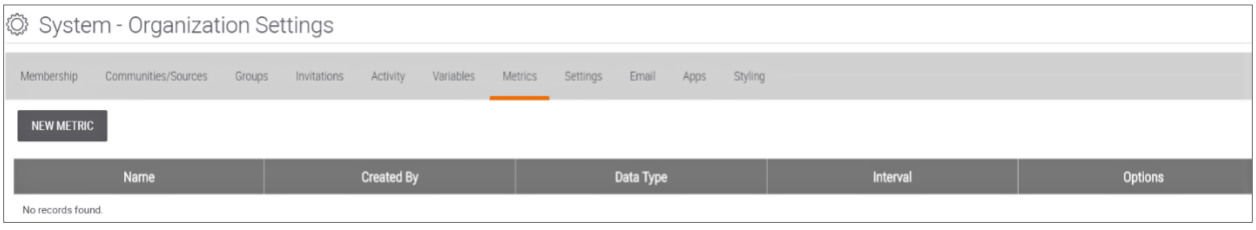

Figure 17

4. Click the **NEW METRIC** button, and the **Configure Metric** pop-up screen will appear (Figure 18).

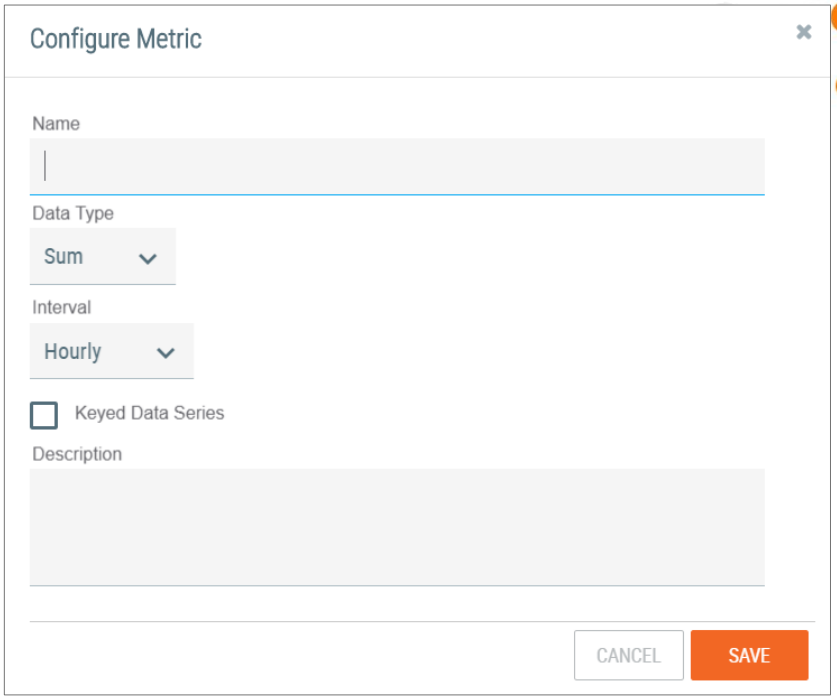

Figure 18

a. **Name**: Enter a name for the new metric.

b. **Data Type**: Click the drop-down arrow to select the type of data to be run. For example, to determine the number of times an app was executed, **Sum** would be selected.

c. **Interval**: Click the drop-down arrow to choose a time interval from which to obtain the data type. This is the time interval before the metric is reset, which starts on midnight of the day created for daily, midnight of the first of the month for monthly, etc.

d. **Keyed Data Series**: Click the checkbox to store the metric as an arbitrary number of key:value pairs. This is useful when tracking categorical information in which the categories are not known in advance. For example, this feature would be used when recording a metric of Incidents by status from an integrated ticketing system, where the key is status and the value is number of Incidents. Note that for Playbooks this requires the use of a key metrics app.

e. **Description**: Click in this field to enter descriptive words for the metric.

f. Click the **SAVE** button and the new metric will be created.

The Login IP Address Access Filter

The Login IP Address Access Filter provides a multifactor authentication capability, giving Org Administrators the option of limiting IP Address space from which their Org users are permitted to log into the ThreatConnect Instance.

Configuring the Login IP Address Access Filter

Follow these steps to configure the Login IP Address Access Filter for an Organization account:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Settings** tab, and the **Settings** screen will appear (Figure 19).

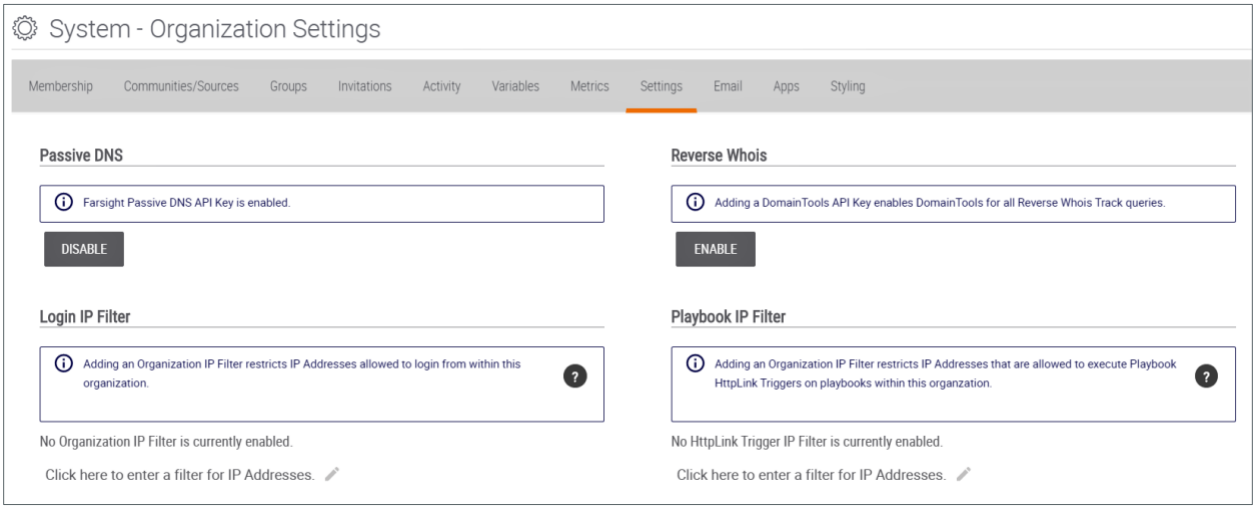

Figure 19

4. At the bottom left of the screen, under the **Login IP Filter** box, click on the **Click here to enter a filter for IP Addresses** text.
5. In the text box that appear, enter any IP addresses or IP address ranges that will be allowed to log into Org user accounts within the Organization. Separate multiple values with commas.
6. Click the checkmark inside the circle to save additions or changes to the Login IP Address Filter.

The Playbook IP Address Access Filter

For Playbooks containing an HttpLink Trigger, the Playbook IP Address Access Filter can specify the IP addresses that can send a request to that Trigger.

Configuring the Playbook IP Address Access Filter

Follow these steps to configure the Playbook IP Address Access Filter for an Organization account:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Settings** tab, and the **Settings** screen will appear (Figure 19).
4. At the bottom right of the screen, under the **Playbook IP Filter** box, click on the **Click here to enter a filter for IP Addresses** text.
5. In the text box that appear, enter any IP addresses or IP address ranges that will be allowed to send a request to the HttpLink Trigger. Separate multiple values with commas.
6. Click the checkmark inside the circle to save additions or changes to the Playbook IP Address Filter.

NOTE: Users trying to trigger a Playbook from IP addresses not on the filter list will receive an error message.

Passive DNS

Users with their own Passive DNS data-service provider may be able to utilize that provider's data, as opposed to ThreatConnect's current provider's data, for Passive DNS lookups.

Adding a Private Passive DNS API Key

Follow these steps to add a passive DNS API key:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Settings** tab, and the **Settings screen** will appear (Figure 19).
4. Click the **ENABLE** button under the **Passive DNS** box, and the **Setup Farsight Passive DNS** pop-up screen will appear (Figure 20).

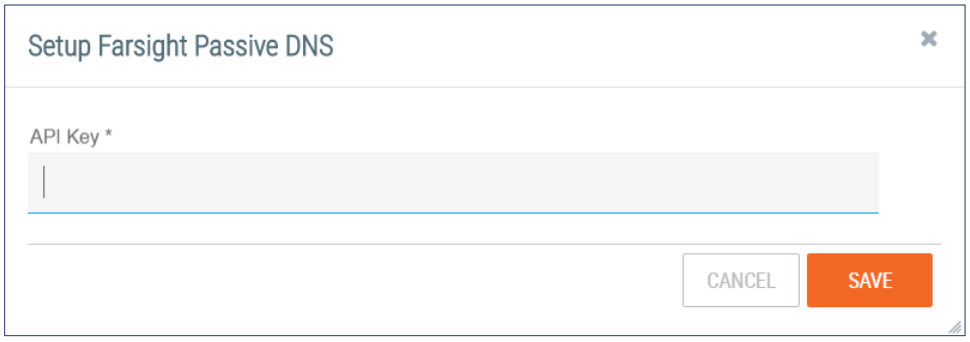

Figure 20

5. Enter a Passive **DNS API Key**.
6. Click the **SAVE** button.

Reverse Whois

Users can access and create Tracks by entering a DomainTools API key in the Reverse Whois field. Depending on the API key entered, users will not be limited as to the number of Tracks they can create and run.

Adding a DomainTools API Key

Follow these steps to add a DomainTools API key:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Settings** tab, and the **Settings screen** will appear (Figure 19).
4. Click the **ENABLE** button under the **Reverse Whois** box, and the Setup **DomainTools** pop-up screen will appear (Figure 21).

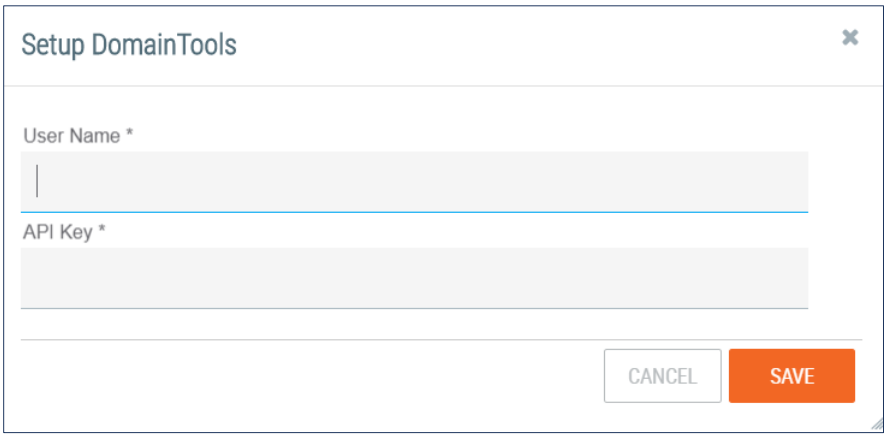

Figure 21

5. Enter a DomainTools API Key.
6. Click the **SAVE** button.

Setting Up Email Ingestion

Email ingestion allows users to send cyberthreat-related emails to ThreatConnect, where they will be parsed and imported for further analysis.

Creating a Feed Mailbox

Feed Mailboxes receive mail from cyber-intel sources, which release information periodically as an RSS feed in an email-type format. Emails sent to the Feed Mailbox have only their bodies parsed for Indicators. When the parsing is complete, ThreatConnect will do the following:

- Create a "document" object out of the email's body.
- Create any Indicators that matched the pre-defined Feed Mailbox regular expressions.
- Link the Indicators to the document.

Follow these steps to create a Feed Mailbox:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Email** tab, and the **Email** screen will appear (Figure 22).

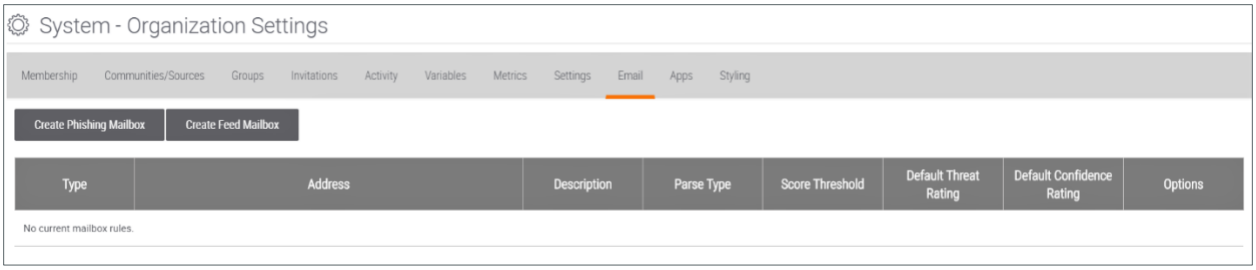

Figure 22

4. Click the **Create Feed Mailbox** button, and the **Feed Mailbox Administration** pop-up screen will appear, with the **Mailbox** tab highlighted (Figure 23).

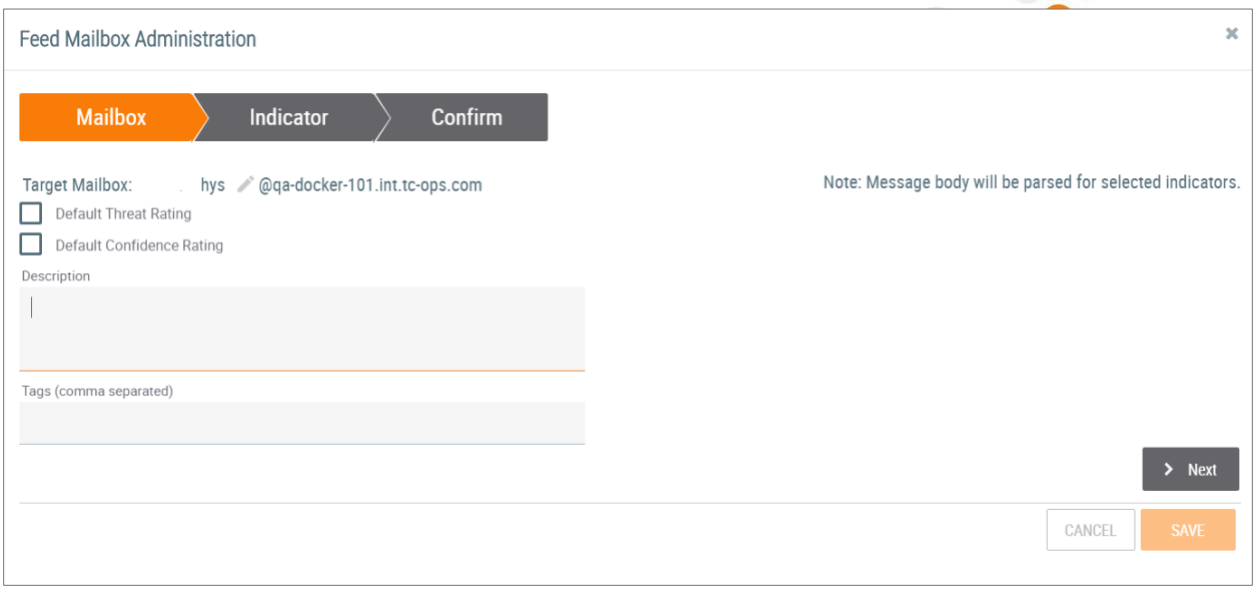

Figure 23

NOTE: A System Administrator can modify the Target Mailbox name at this step.

5. Click the checkboxes to assign a **Default Threat Rating** and **Default Confidence Rating** to found Indicators, and click in the **Description** and **Tags** text boxes to enter the appropriate information.
6. Click the **Next** button to proceed to the **Indicator** tab (Figure 24). Use the drop-down menu to select an Indicator Type (**Host**, **Address**, **E-mail Address**, **File**, **URL**, and any custom Indicators that have been added, including ThreatConnect's five built-in custom Indicators).

   Enabling an Indicator allows regex entries. The **Question Mark** icon on the top right of the screen offers explanations and examples to help define the criteria for each Indicator Type.

   NOTE: Indicators that were sanitized within a document can be de-sanitized after the main regex finds them.

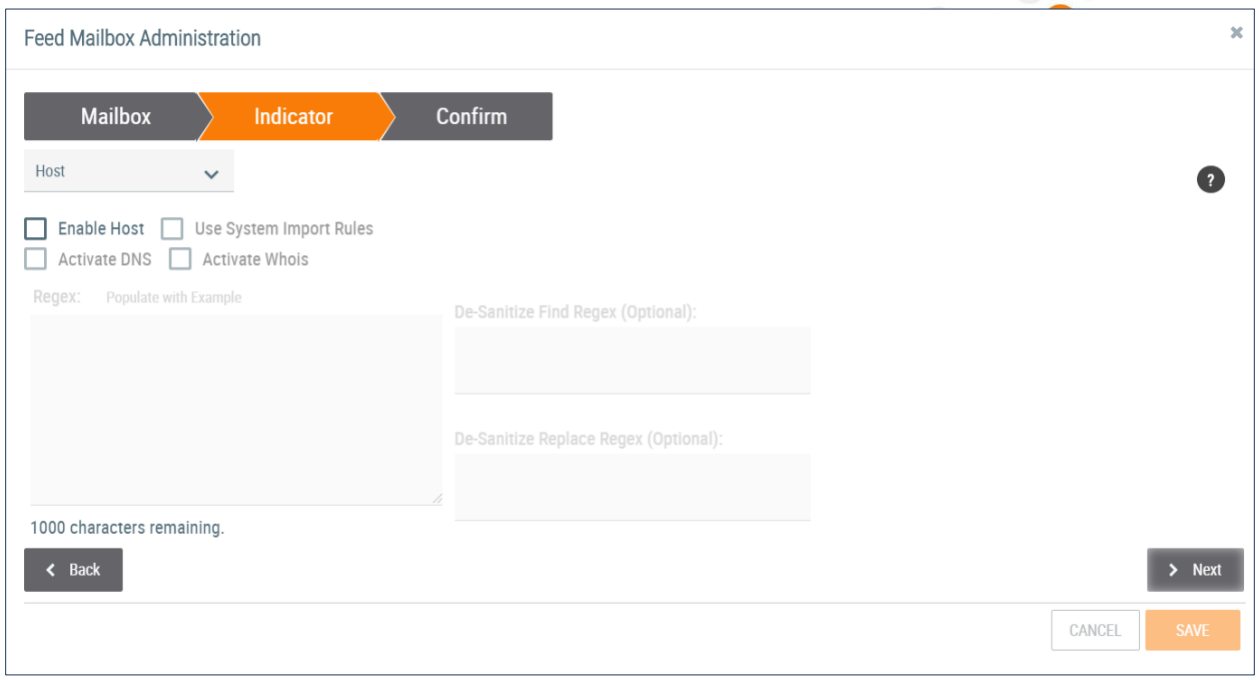

Figure 24

7. After all Indicator parameters have been specified, click the **Next** button, and the **CONFIRM** tab screen will appear (Figure 25), offering a summary of the entries.

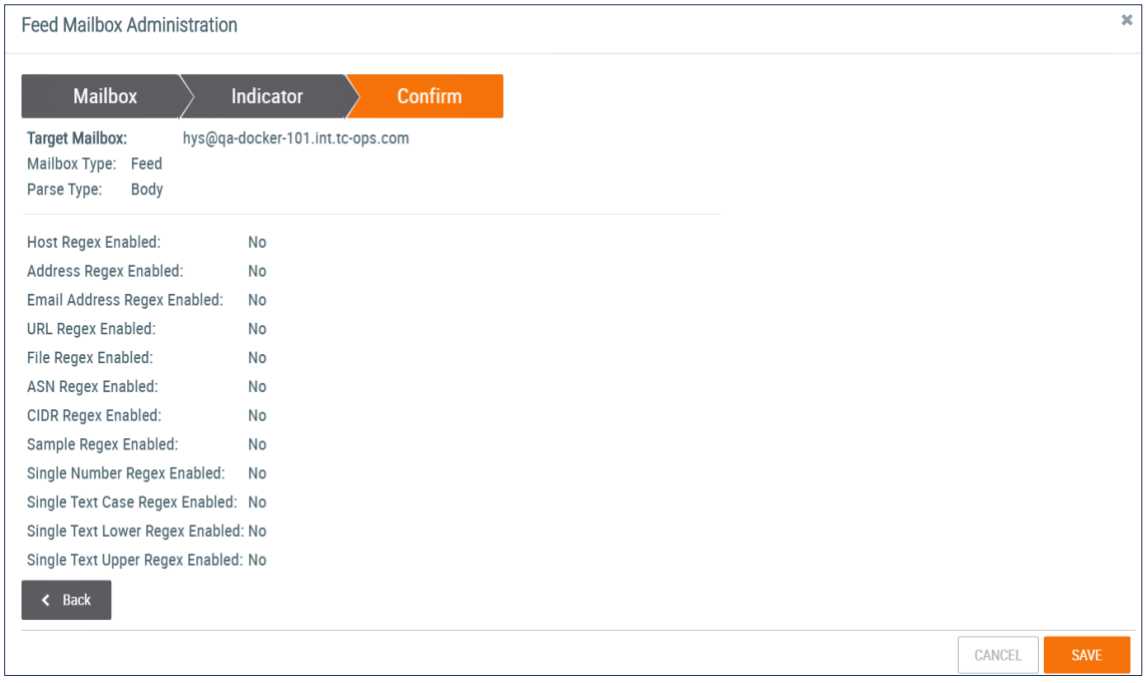

Figure 25

8. Click the **SAVE** button.

Creating a Phishing Mailbox

Phishing Mailboxes receive malicious or suspicious emails that are flagged by the Email Security Gateway, or emails in **.msg** or **.eml** format that have been flagged by a security analyst. When creating a Phishing Mailbox, the Administrator must specify if the mailbox is meant to receive emails directly from network devices or if it is meant to receive email headers in the form of attachments. ThreatConnect will parse these emails, and when the parsing is complete, if an email meets the minimum email scoring threshold, then ThreatConnect will do the following:

- Create an Email Object containing the email's header and body.
- Create a Task Object signaling that the email is ready for additional processing.
- Link previously existing Indicators to the Email Object, if they are found in the header or body.
- Link previously existing Victim email addresses to the Email Object, if they are found in the header.

Follow these steps to create a Phishing Mailbox:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).

   NOTE: For Communities and Sources, the Email tab is accessed through the Community or Source Config option, respectively.
3. Click the **Email** tab, and the **Email** screen will appear (Figure 22).
4. Click the **Create Phishing Mailbox** button, and the **Phishing Mailbox Administration** pop-up screen will appear (Figure 26).

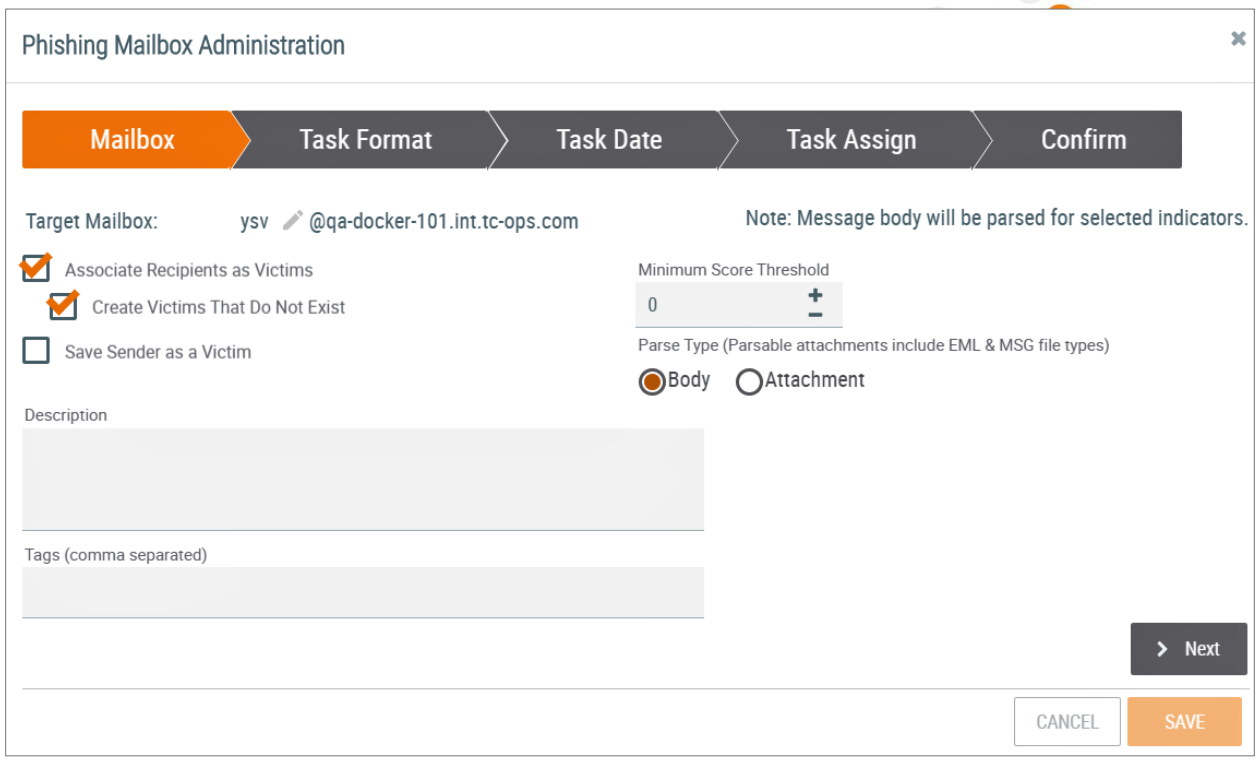

Figure 26

NOTE: A System Administrator can modify the Target Mailbox name at this step.

5. Click one of the radio buttons to **Associate Recipients as Victims** or **Create Victims That Do Not Exist** to create an association between the email and Victim asset.

   NOTE: The association is created only if the Victim asset already exists in ThreatConnect.

6. Click the **Save Sender as Victim** checkbox to create an association between the sender and the Victim Asset.
7. Click inside the **Description** and **Tags** text boxes to enter the appropriate information.
8. Click the **Next** button to proceed through the steps required for ThreatConnect to assign a task to an analyst when new emails arrive.
9. Click in the **Minimum Score Threshold** box (or use the plus and minus signs) to indicate the minimum score that an email must meet in order to be processed.
10. Click one of the **Parse Type** radio buttons to select if the Phishing Mailbox will receive emails directly or in the form of an **.eml** or an **.msg** attachment.
11. Click the **SAVE** button.

Apps and Jobs

Creating a Job

ThreatConnect is integrated with many third-party applications and services, which allows ThreatConnect users to employ these product integrations as apps via TC Exchange™ to further augment their analytic capabilities. Apps with feeds take advantage of the feed-deployment mechanism to create Sources, which then run associated jobs.

Follow these steps to create a new job:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Apps** tab, and the **Apps** screen will appear with the **Jobs** option displayed (Figure 27).

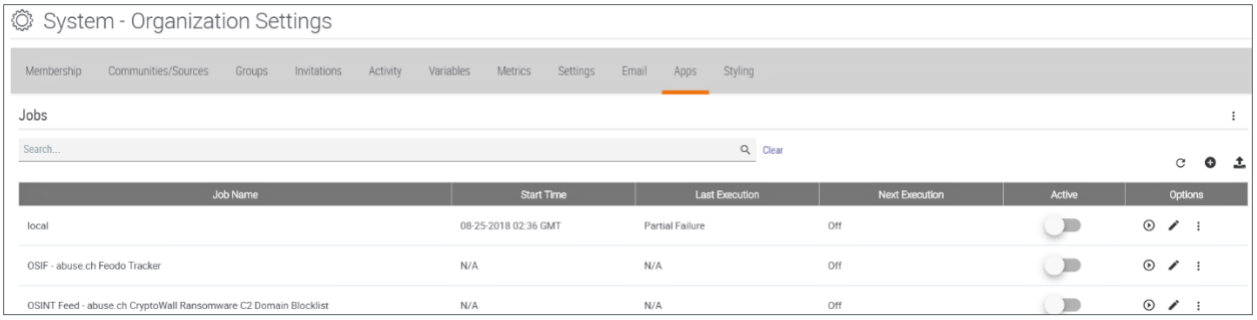

Figure 27

4. Click the **Add Job** icon, and the **Add Job** pop-up screen will appear (Figure 28).

NOTE: Click the Refresh icon to reload the list of jobs.
NOTE: Enter text in the box above the results table to search for Jobs.

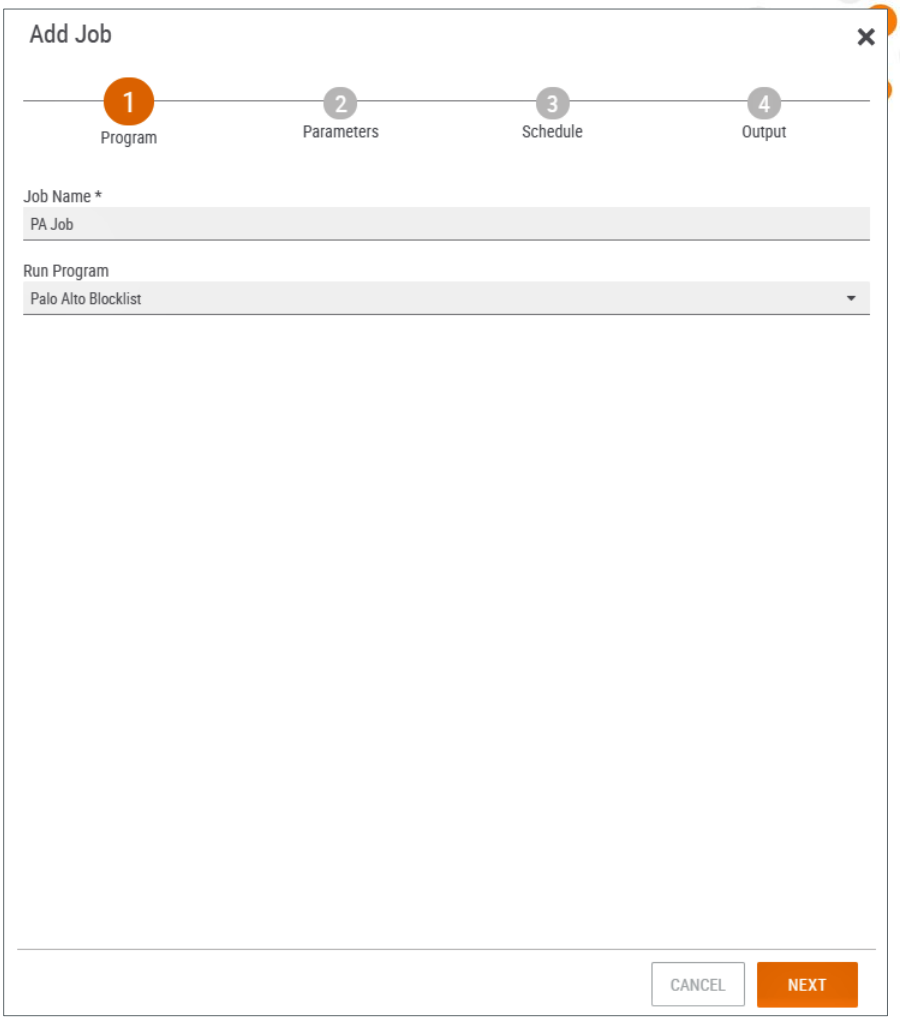

Figure 28

a. **Job Name**: Click in the text box to enter a name.

b. **Run Program**: Click on the drop-down menu and select a program. In this example, **Auto Enrich** was selected.

5. Click the **Next** button, and the **Parameters** screen will appear (Figure 29). Enter all pertinent parameters.

   NOTE: The parameters screen may be different for different apps.

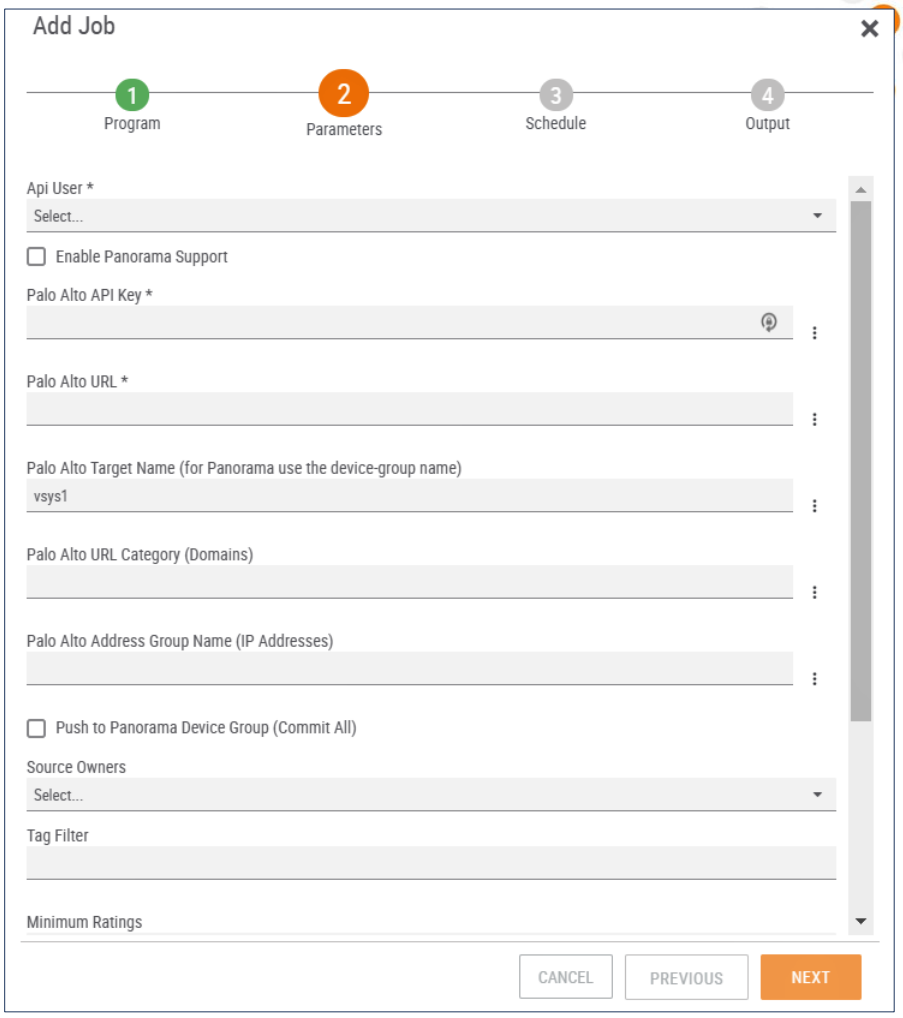
Add Job
1
Program
2
Parameters
3
Schedule
4
Output
Api User *
Select...
Enable Panorama Support
Palo Alto API Key *
Palo Alto URL *
Palo Alto Target Name (for Panorama use the device-group name)
vsys1
Palo Alto URL Category (Domains)
Palo Alto Address Group Name (IP Addresses)
Push to Panorama Device Group (Commit All)
Source Owners
Select...
Tag Filter
Minimum Ratings
CANCEL
PREVIOUS
NEXT

Figure 29

6. Click the **Next** button, and the **Schedule** screen will appear (Figure 30).

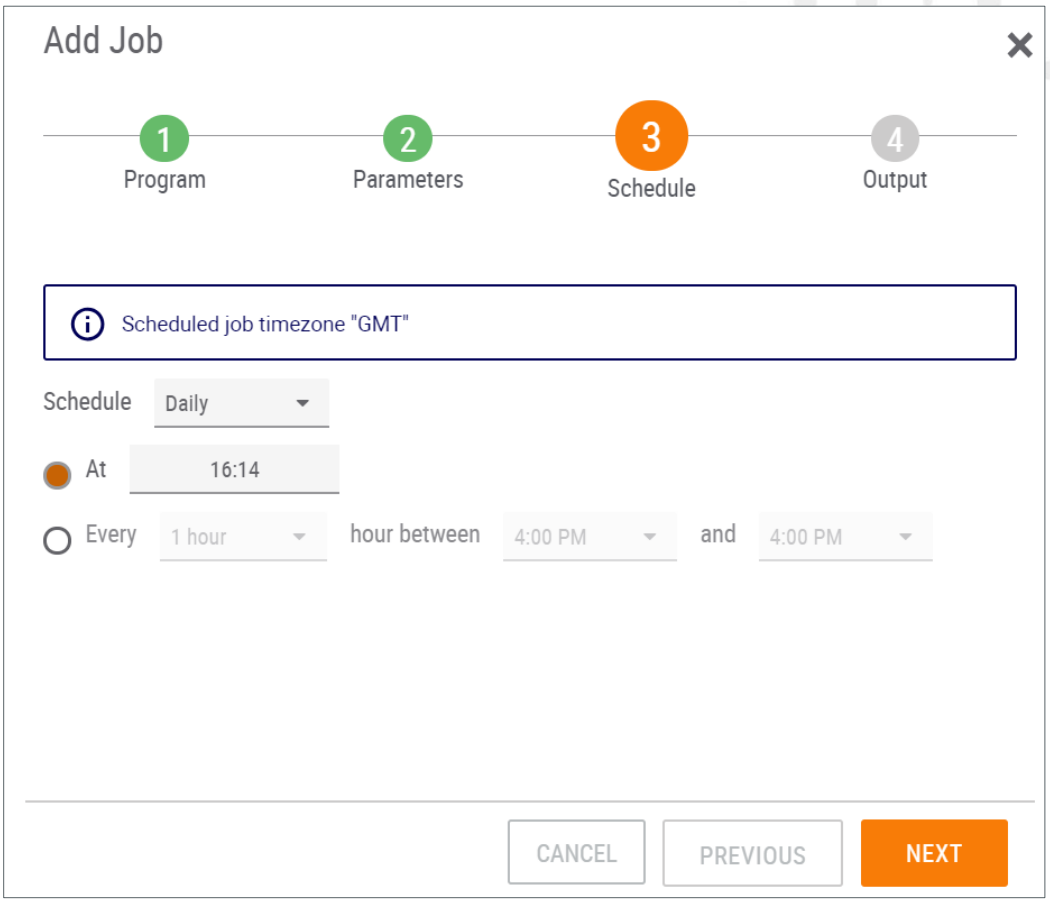

Figure 30

a. **Job Schedule**: Click on the drop-down menu to select whether the job should run daily, weekly, or monthly.

b. **Each Day at / Every**: Enter the desired time of day on which to run the job, or enter a time interval during which to repeat the job.

7. Click the **Next** button, and the **Output** screen will appear (Figure 31).

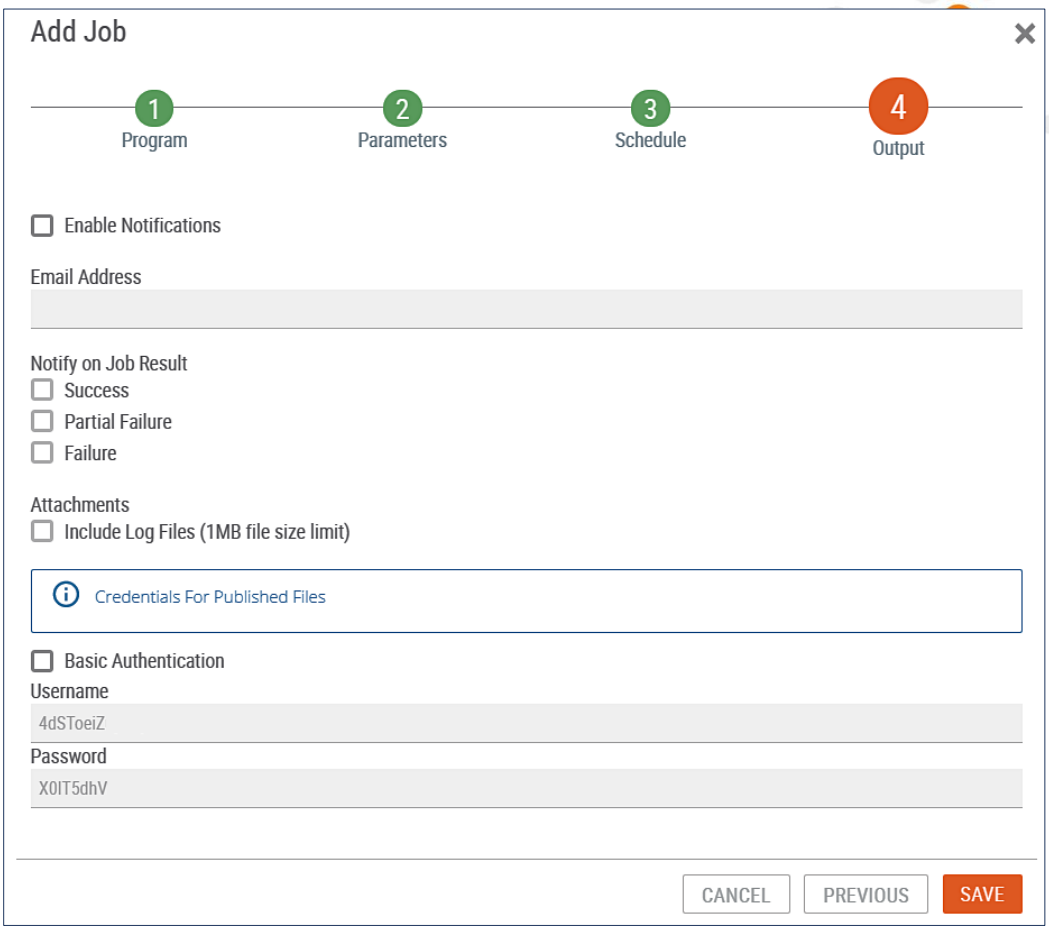

Figure 31

a. **Enable Notifications**: Click the checkbox to enable notifications.

b. **Email Address**: Enter the email address to which notifications should be sent.

c. **Notify on Job Result**: Click the box(es) for the job results for which notifications should be sent.

d. **Include Log Files**: Check the box to include log files of 1MB or less in the notification email.

e. **Basic Authentication**: Check the box to enter a user username and password associated with this job.

8. Click the **SAVE** button.

Importing a Job

Follow these steps to import a job that has already been created:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Apps** tab, and the **Apps** screen will appear with the **Jobs** option displayed (Figure 27).
4. Click the **Import Job** icon on the upper right of the screen, and the **Add Job** pop-up screen will appear (Figure 32).

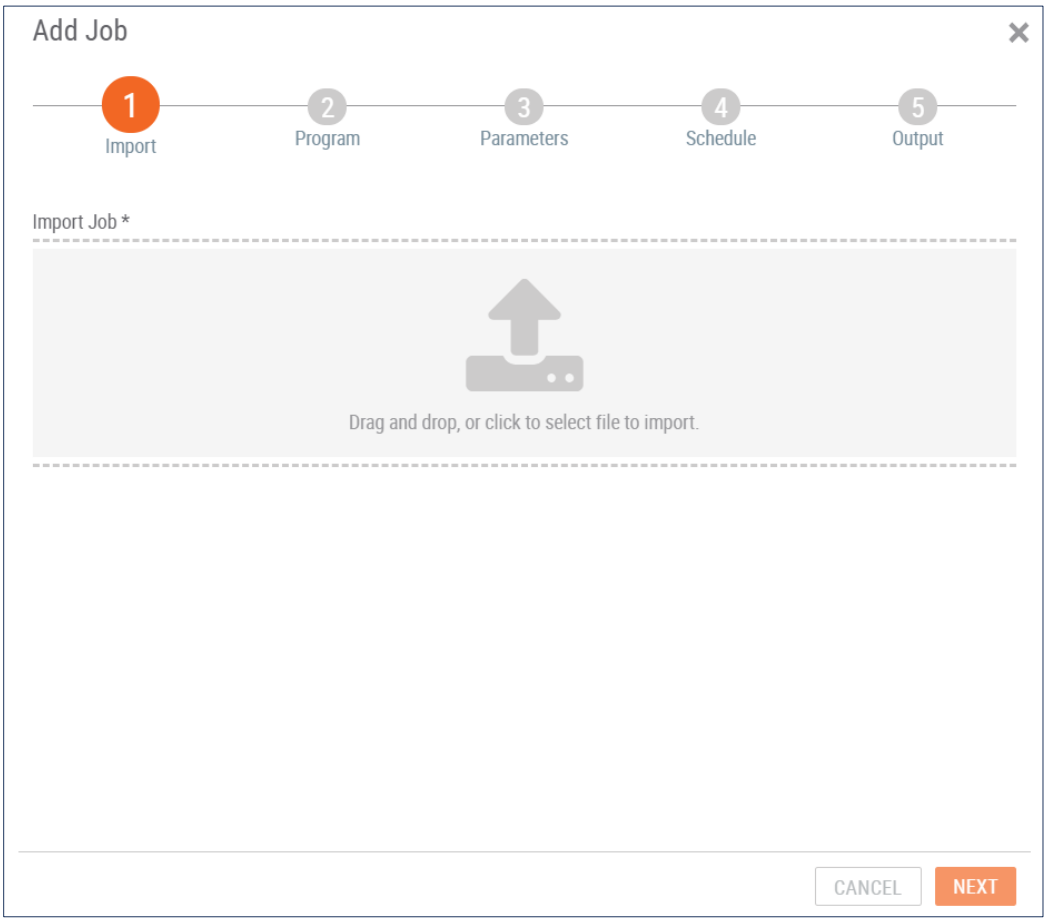

Figure 32

5. Drag and drop a Job into the gray rectangle, or click the gray **Import** symbol in the middle of the screen in order to navigate to a directory from which to select a file.
6. Click the **NEXT** button, and navigate through the remaining screens following the instructions in the Creating a Job section.

Editing or Running a Job

Follow these steps to edit or run a job:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Apps** tab, and the **Apps** screen will appear (Figure 27).
4. The following functions can be performed for an existing job displayed in the **System Jobs** table:
   - Click on the **Run Job** icon to start a job on demand.

     NOTE: A job can be run On Demand only if "on demand" is enabled in the job's configuration.
   - Click on the **Edit Job** icon to edit a job's setting.
   - Click on the **Ellipsis** icon to view a pop-up menu that provides the following options:

     Delete Job, **Environment** (allows jobs to be run remotely), **Export Job**, **Kill Job**, **Published Files**, **View Details** for a job (including the following parameters: **Program Name**, **Peak Memory** Usage, **Peak CPU** Usage, **Exit Message**, **Session Id**, **Server** Information, **Queued** Date, **Started** Date, **Completed** Date, and **Failed** Date), and **View Log**.

     NOTE: All the above options will not be available for every job. Also note that Environments allow Jobs to be run remotely. See the Playbook Environments Knowledge Base article for more information.

Data Store

Data Store is a feature that allows TC Exchange apps to persist data using Elasticsearch®. The app is intentionally decoupled from the data in order to offer a flexible data-sharing environment while still allowing a private database for apps that require it. As such, the information provided by Data Store is essentially "read only."

Data Store is available to any Job or Spaces apps requiring persistent storage. There is no initial setup required, and the Elasticsearch resources are available as an extension of the ThreatConnect API. The app will interact with Elasticsearch exclusively through the API in order to enforce proper security in a multi-tenant environment.

NOTE: To enable ThreatConnect to use Data Store, the System Settings must have "elasticSearchEnabled" set to "true," and "elasticSearchUrl" must be defined. See the ThreatConnect System Administration Guide.

Follow these steps to use the Data Store feature:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Apps** tab, and the **Apps** screen will appear (Figure 27).
4. Click the **Ellipsis** icon above the **Import Job** icon and select **Data Store**. The **Data Store** screen will appear (Figure 33).

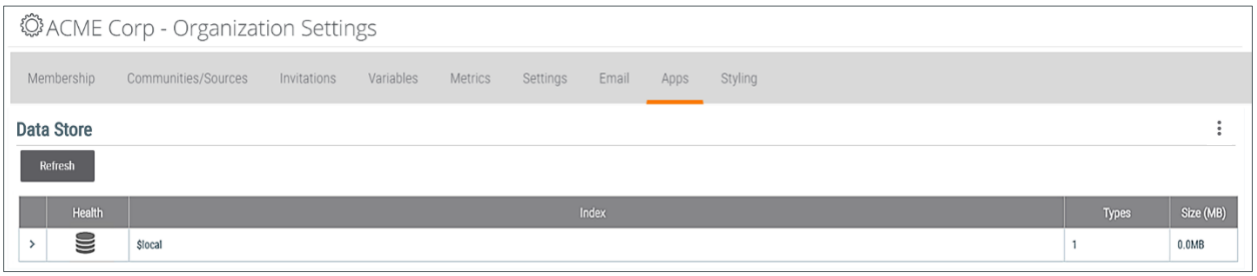

Figure 33

5. Click the right-arrow icon on the left of the index whose data are to be viewed. A table showing an expanded view of the types within that index will appear (Figure 34).

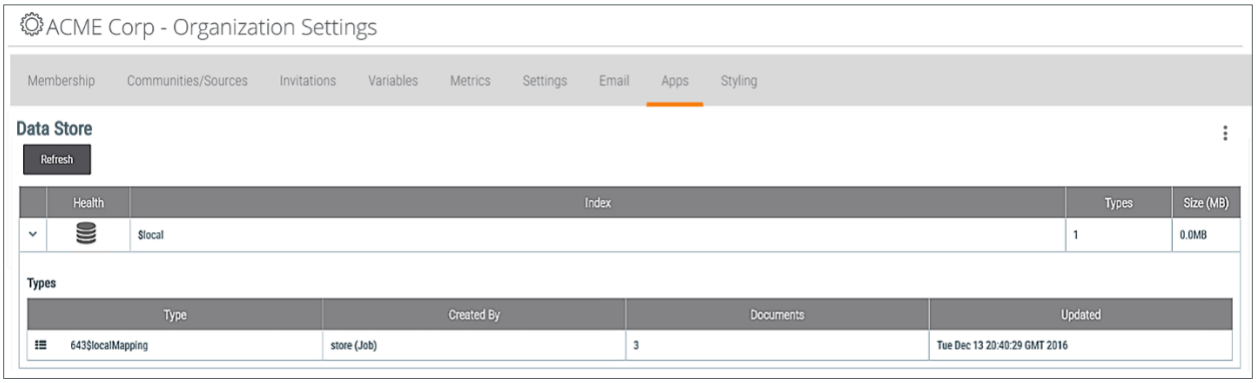

Figure 34

Viewing Existing App Profiles

A profile serves as a proxy for the app, and users interact directly with the profiled version of the installed app. Decoupling an app from a configuration profile allows the administrator to configure multiple profiles off an app and, subsequently, give permissions to different Organizations based on that profile. Moreover, this added level of abstraction allows the same app to be configured to work slightly differently at installation. App Profiles allow administrators to customize installed apps in the following ways:

- Set default parameter values for an app.
- Assign privileges to different profiles for the same app.
- Define setup parameters required by the app.

Follow these steps to view an app profile:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Apps** tab, and the **Apps** screen will appear (Figure 27).
4. Click the **Ellipsis** icon above the **Import Job** icon and select **Profiles**. The **Profiles** screen will appear (Figure 35), displaying previously created app profiles. (See the *ThreatConnect System Administration User Guide* for instruction on creating an app profile.)

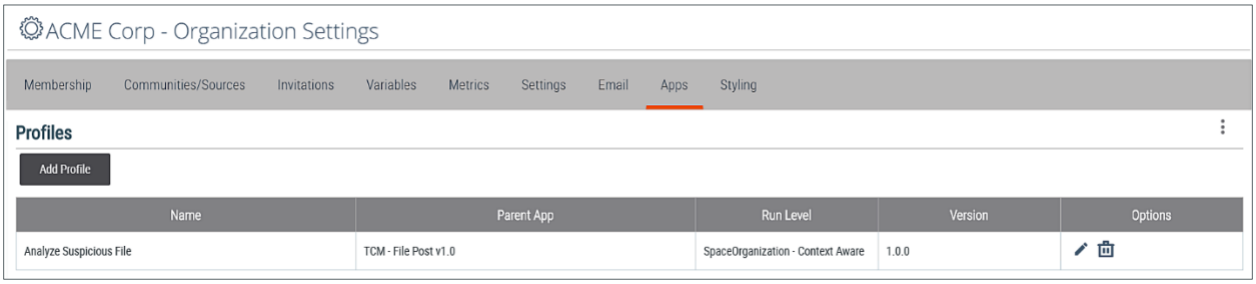

Figure 35

Adding App Profiles

The App Profile feature is a valuable tool for administrators who customize the installation of TC Exchange Spaces apps. A profile serves as a proxy for the app, and users interact directly with the profiled version of the installed app. Decoupling an app from a configuration profile allows the System Administrator to configure multiple profiles off an app and, subsequently, give permissions to different Organizations based on that profile. Moreover, this added level of abstraction allows the same app to be configured to work slightly differently at installation. App Profiles allow administrators to customize installed apps in the following ways:

- Set default parameter values for an app
- Assign privileges to different profiles for the same app
- Define setup parameters required by the app

Follow these steps to add an app profile:

1. Log in with a System Administrator Account.
2. On the top navigation bar (Figure 1), place the on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).

3. Click the **Apps** tab and the **Apps** screen will appear (Figure 17).
4. Click the **Ellipsis** icon above the **Import Job** icon and select **Profiles**. The **Profiles** screen will appear (Figure 35).
5. Click the **Add Profile** button, and **the App Profile** pop-up screen will appear (Figure 36). Enter the required information in the pertinent fields, and click the **Next** button. Continue entering information in the subsequent windows, and then click the **SAVE** button.

   NOTE: The Add Profile button will appear only if there is an app installed to which a profile can be applied.

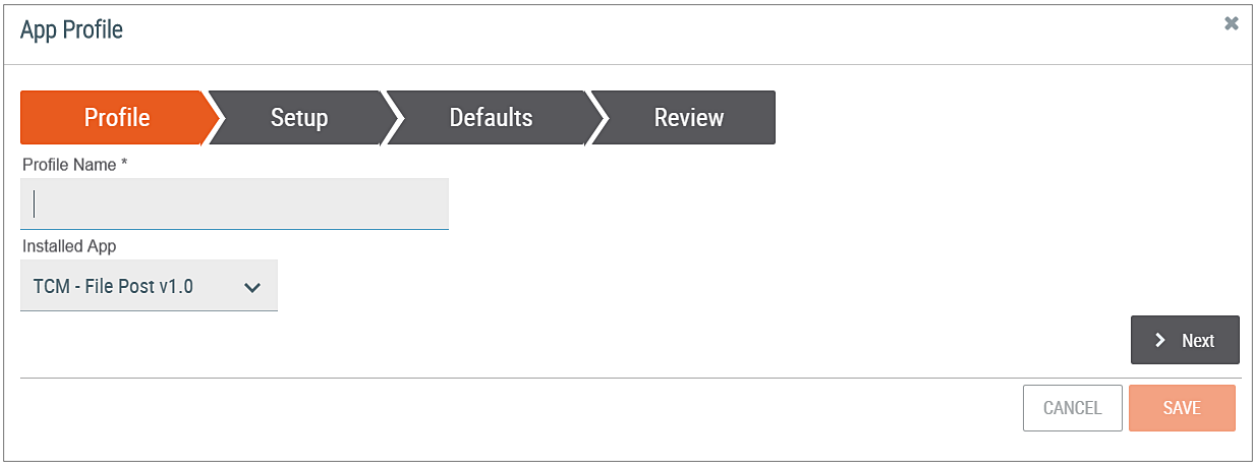

Figure 36

Styling a PDF Header

When downloading a PDF that describes an Adversary, Incident, or Threat, a user may want to include a custom header on the PDF.

NOTE: A PDF header image should not be larger than 250 x 70 pixels.

Follow these steps to style a PDF header:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
3. Click the **Styling** tab, and the **Styling** screen will appear (Figure 37), showing the default ThreatConnect header that will be used if no other image is uploaded.

   NOTE: Place the cursor on the question mark symbol to obtain information on image-size requirements.

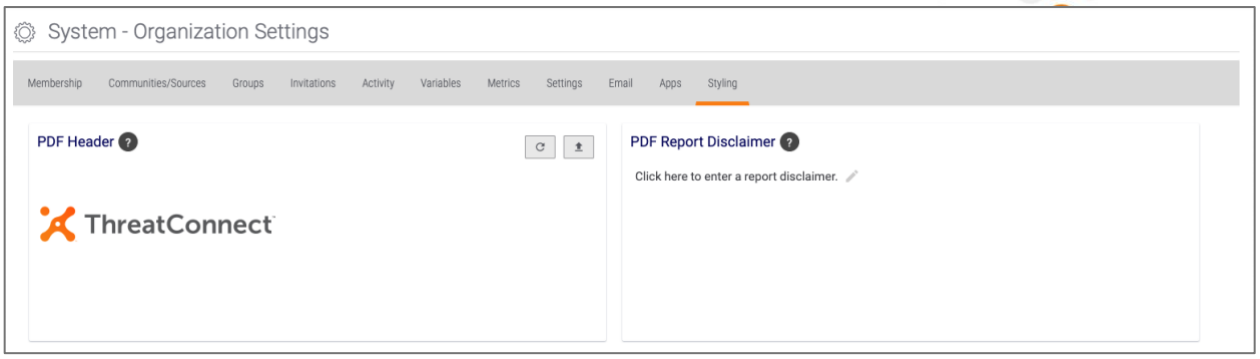

Figure 37

4. Click the **Upload**  icon to the left of **PDF Report Disclaimer**, navigate to a directory, and select a JPEG or PNG image file.

5. Click the **Pencil**  icon under **PDF Report Disclaimer** to add a disclaimer, such as "Demo," to a PDF.

6. The selected image will now appear in the appropriate header or footer box, and it will also appear as a header for downloaded PDFs or as a header or footer for the user's ThreatConnect site.

Customizing an Organization

One of the strengths of ThreatConnect as a threat-intelligence platform is that it allows an Administrator to customize how data are labeled and acted upon. The vehicles for such behavior, Attributes and Security Labels, can be customized for users within an Organization to enhance analysis and further action.

Creating Custom Attributes

Although ThreatConnect offers a variety of pre-configured Attributes for Groups and Indicators, Org Administrators may wish to create customized Attributes to reflect the needs of their mission space and workflow.

Follow these steps to customize an Organization's Attributes:

1. Log in with an Org Administrator account.

2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38). Select an Organization from the drop-down menu on the upper right. The existing Organization Attributes are displayed, as well as the included ThreatConnect System Attributes, if the **Include System Types** box is checked.

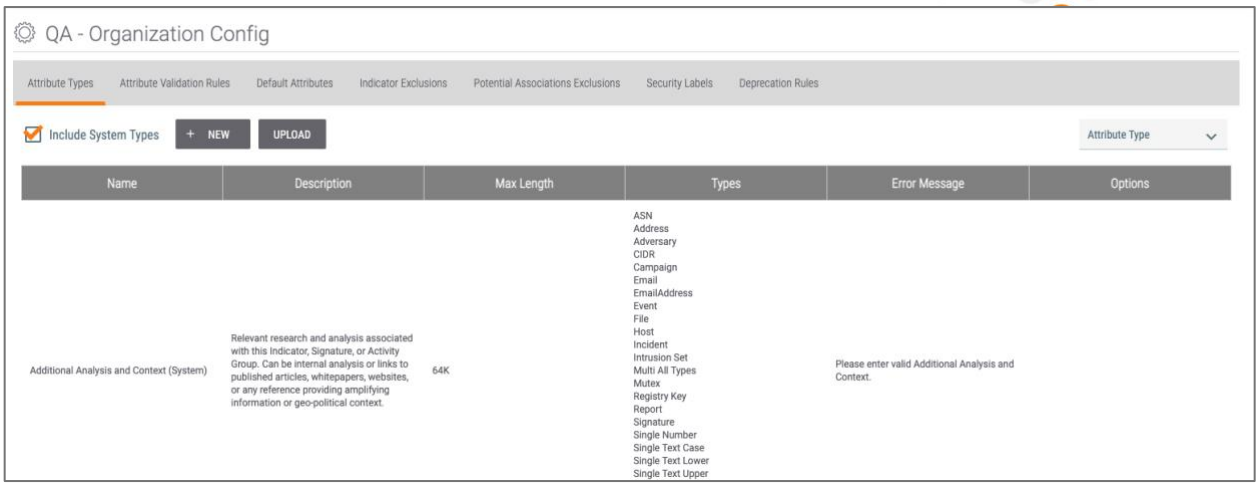

Figure 38

3. To create a new custom Org Attribute, click the **+ NEW** button, and the **Configure Attribute Type** pop-up screen will appear (Figure 39).

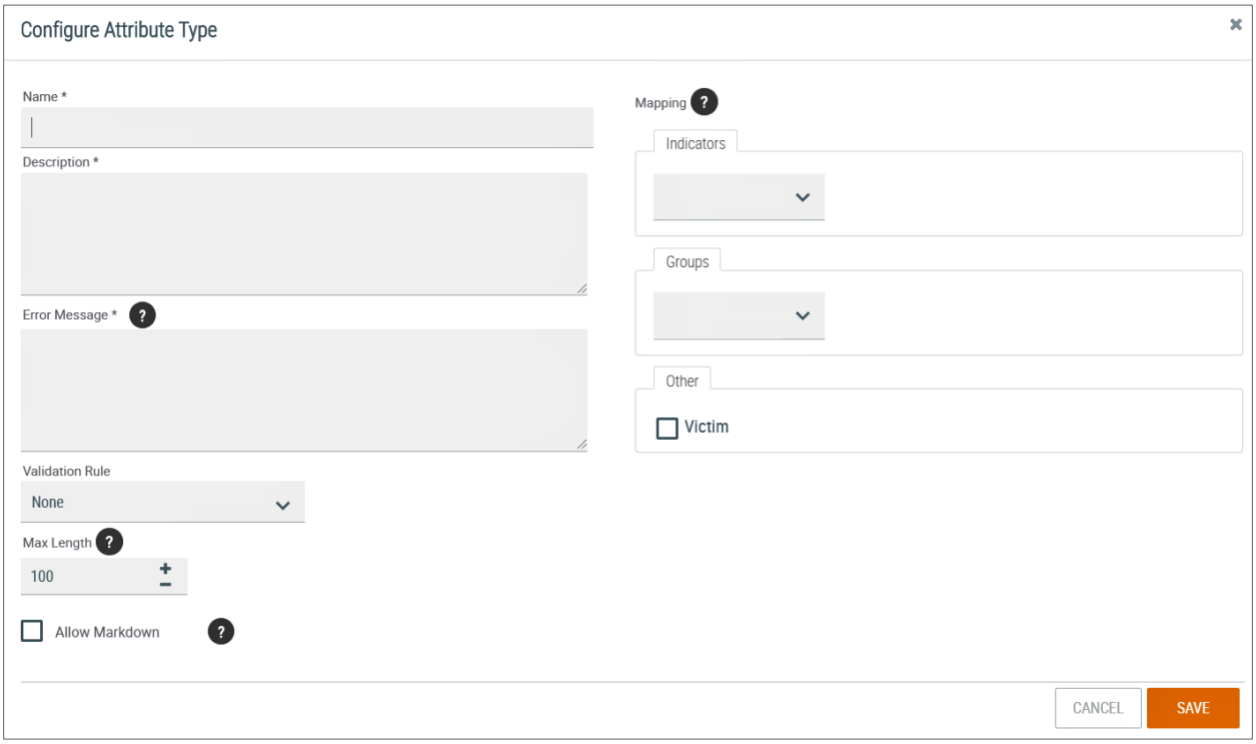

Figure 39

a. **Name**: Click in the box to enter the name of the Attribute as it will appear in menus and on the **Details** screen for Indicators and Groups.

b. **Description**: Click in the box to enter a description of the System Attribute as seen by users when inputting a value for the Attribute or when viewing it from the **Details** screen.

c. **Error Message**: Click in the box to enter the message presented when users try to input a value that does not meet the System Attribute's Validation Rules.

d. **Validation Rule**: Click on the drop-down menu to select the schema that determines whether a user's input is valid when logging an Attribute for an Indicator or Group. ThreatConnect is preloaded with a variety of Validation Rules, such as for IP Addresses, Dates, Country Codes, etc. System, Community, and Organization Administrators are able to define their own System Attribute Validation Rules as needed.

e. **Max Length**: Click in the box (or use the plus and minus signs) to manually enter the maximum size, in characters, of the System Attribute, if applicable, based on the Attribute's assigned Validation Rule.

f. **Allow Markdown**: Click this checkbox to allow the Markdown language to be used when configuring an Attribute.

g. ***NOTE: Markdown is a markup language used to transform text into HTML for the purpose of formatting. ThreatConnect supports the use of Markdown with several Attribute Types, including Description and Source.***

4. Click the **SAVE** button to create the custom Attribute.

Figure 40 shows an example of a custom System Attribute that uses the System Country Validation Rule to track the suspected nationalities of those responsible for the appropriate Groups and Indicators. If custom Indicators have been added, they will be displayed in the Indicators section as well.

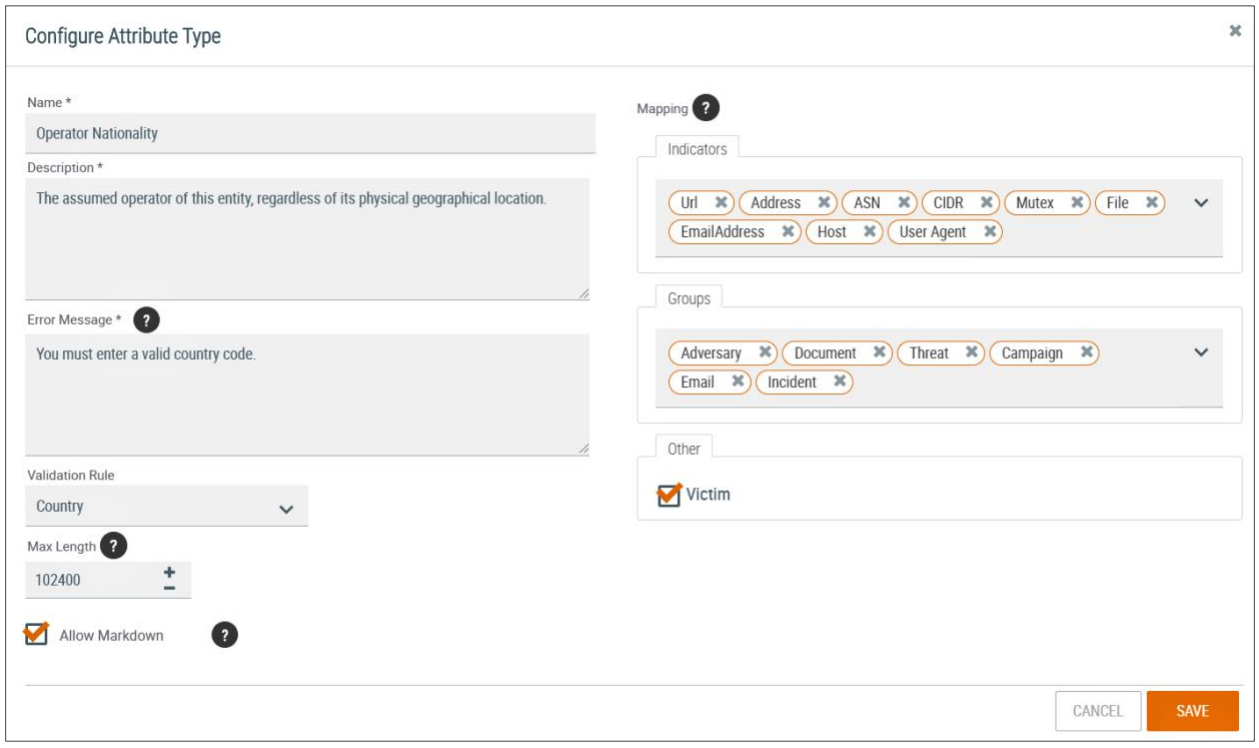

Figure 40

Uploading an Org Attribute

Follow these steps to upload one or many Org Attributes by using a comma-separated value file:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38).
3. Click the **UPLOAD** button, and the **Upload Attributes** pop-up screen will appear (Figure 41).

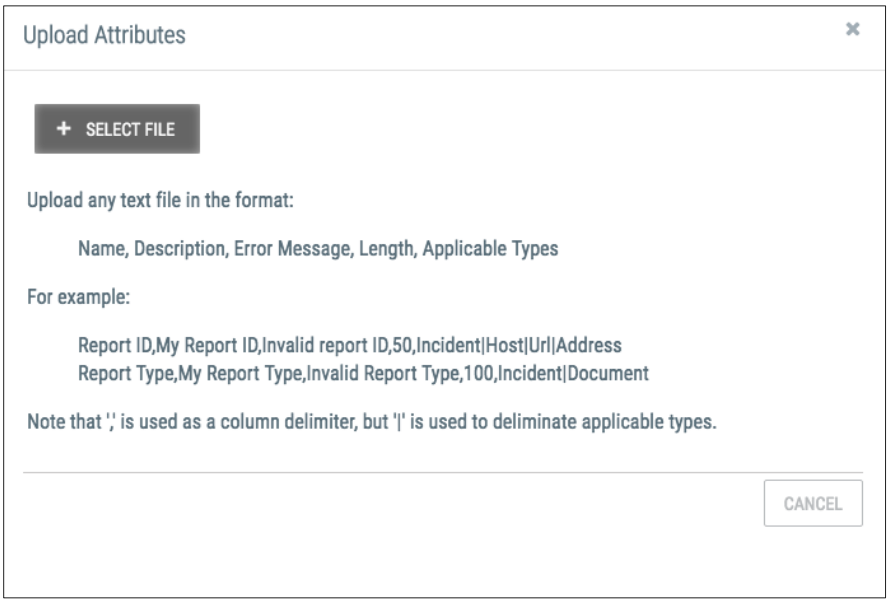

Figure 41

4. Click the **+ SELECT FILE** button, navigate to the desired directory, select a file, and click the **SAVE** button.

Creating Attribute Validation Rules

In addition to creating custom Attributes, Administrators may need to create custom Attribute Validation Rules for their Organizations.

Follow these steps to create custom Attribute Validation Rules:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38).
3. Click the **Attribute Validation Rules** tab, and the **Attribute Validation Rules** screen will appear, displaying existing Organization Attribute Validation Rules, as well as the included ThreatConnect System Attributes Validation Rules, if the **Include System Rules** box is checked (Figure 42).

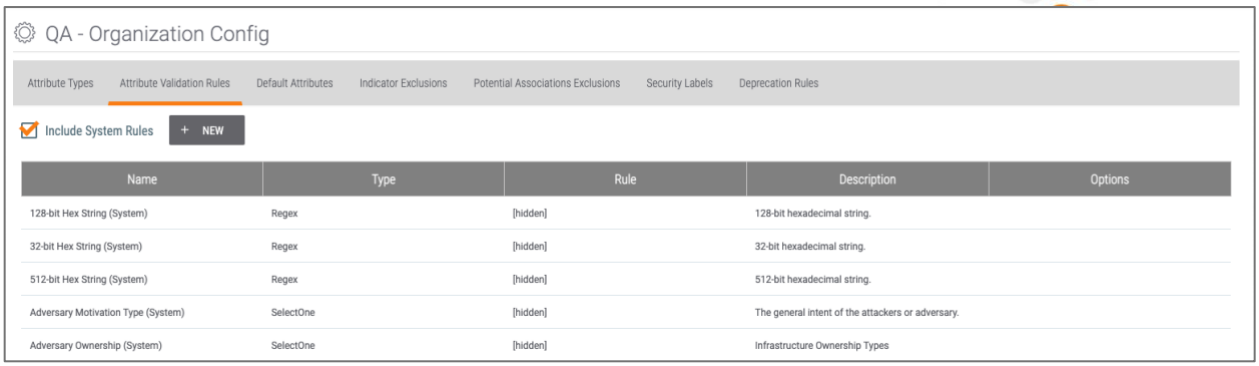

Figure 42

4. To create a new **Organization Attribute Validation Rule**, click the **+ NEW** button, and the **Create Attribute Validation Rule** pop-up screen will appear (Figure 43).

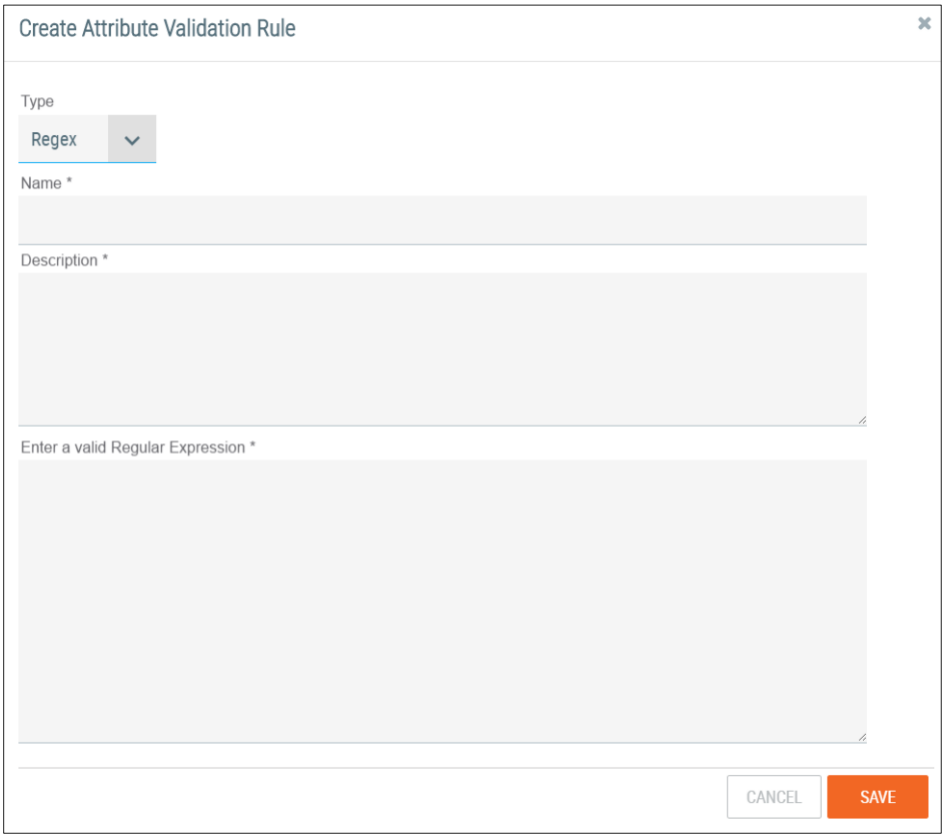

Figure 43

a. **Name**: Click in the box to enter the name of the Validation Rule as it will appear in the **Create Attribute** prompt described previously.

b. **Type**: Click on the drop-down menu to select the schema to use for the Validation Rule. Each option offers the flexibility to determine the valid domain for each Attribute type:

- **Regex**: a regular expression that will consider only matching inputs to be valid (e.g., an IP address or email address on a certain domain)

- **Xsd**: an XML Schema Definition used to validate input (useful for attaching logs from a vendor product)
- **Select One Picklist**: presented as a drop-down menu of options, defined in the box on the right, from which users may only select one value (e.g., high/medium/low priorities)
- **Select One Radio**: similar to the Select One Picklist, but presented as a series of radio buttons
- **Date**
- **Date/Time**
- **Integer**: A whole number, valid in the range specified in the box on the right (e.g., 0:1440 for "minutes worked")

c. **Description**: Click in this box to enter a description for the Attribute Validation Rule.

d. **Enter a valid Regular Expression**: If applicable, click in this box to specify the parameters for a Validation Rule, as defined previously.

5. Click the **SAVE** button to save the custom Validation Rule. Note that the Rule will have to be attached to an actual Attribute in order to validate user input.

Figure 44 is an example of a completed Attribute Validation Rule that defines acceptable inputs as emails from the ThreatConnect.com domain.

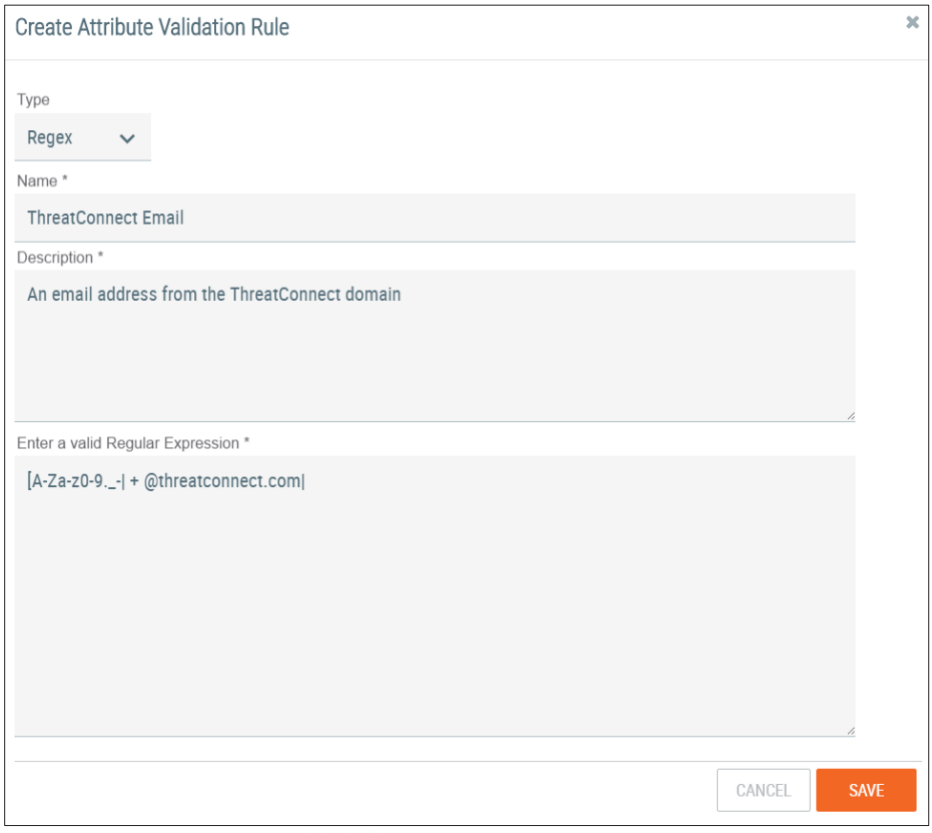

Figure 44

Setting Default Attributes

To keep the **Details** screens from becoming cluttered, only a few Attributes are pre-populated. However, an Administrator may choose to set placeholder Default Attributes for a Group or Indicator to remind users to populate them as soon as the Group or Attribute is created.

Follow these steps to set Default Attributes:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38).
3. Click the **Default Attributes** tab, and the **Default Attributes** screen will appear, displaying existing Organization Default Attributes (Figure 45).

Figure 45

4. To create a new Organization Default Attribute, click the **+ NEW** button, and the **Create Default Attribute Type** pop-up screen will appear (Figure 46).

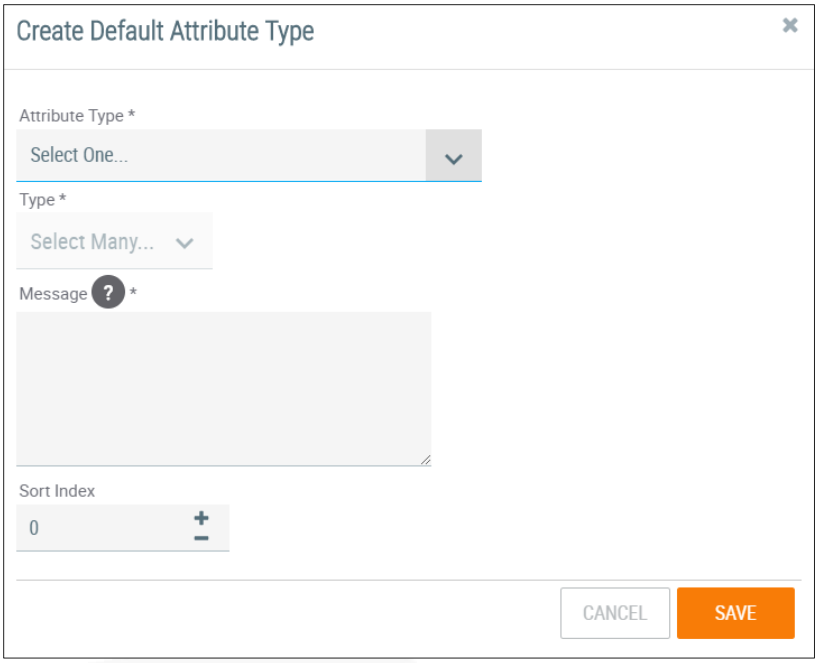

Figure 46

a. **Attribute Type**: Click on the drop-down menu to select one of the Attributes defined on the **Org Attribute Type** screen.

b. **Type**: Click on the drop-down menu to select any applicable Indicator or Group for which to assign the Default Attribute specified previously. Note that, as stated previously, only entities that were approved when the Attribute was created can be specified.

c. **Message**: Click in the box to enter a string presented to users to prompt them to populate this Default Attribute. The string is a link that takes users to a dialog box to edit the appropriate Attribute.

d. **Sort Index**: Click in the box (or use the plus and minus signs) to enter the index used to arrange Default Attributes. Indices are set in ascending order, meaning that the Attribute ranked 0 will be at the top of the Attributes list, and the highest number will be at the bottom.

5. Click the **SAVE** button to save the Organization Default Attribute settings.

Indicator Exclusion Lists: Organization Level

The purpose of creating an Indicator Exclusion list is to prevent the importation of Indicators that may be deemed illegitimate or non-hostile by an Administrator. ThreatConnect allows a user to create an Indicator Exclusion list at the System, Community, Source, or Organization level. The Organization-level list is configured through the **Org Config** screen by an Org Administrator.

Creating Organization-Level Indicator Exclusion Lists

Follow these steps to create an Organization-level Indicator Exclusion list:

1. Log in with an Organization Administrator account.

2. On the top navigation bar (Figure 1), place the cursor on the Settings  icon and the Settings menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38).

3. Click the **Indicator Exclusions** tab, and the **Indicator Exclusions** screen will appear (Figure 47).

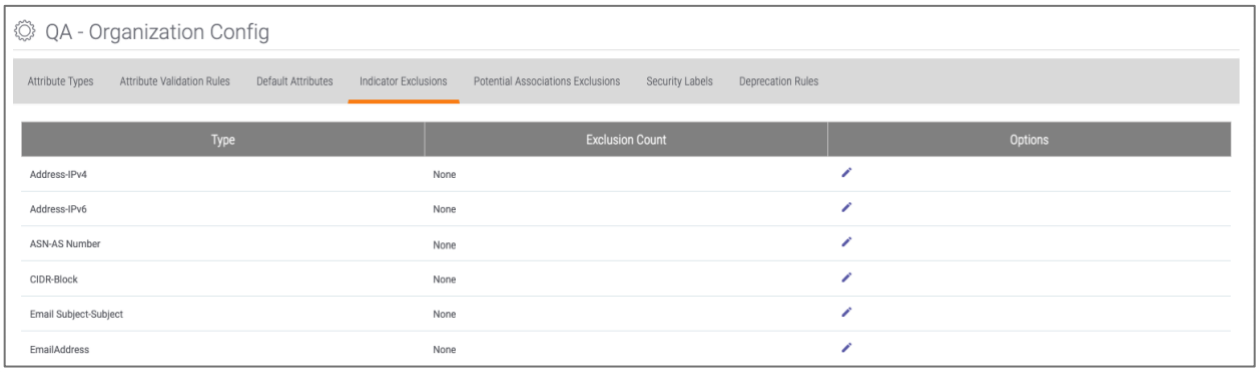

Figure 47

4. Click on the **Details** icon of an Indicator from the **Type** column (File-SHA1 in this example), and the **Exclusion Details** pop-up screen will appear (Figure 48).

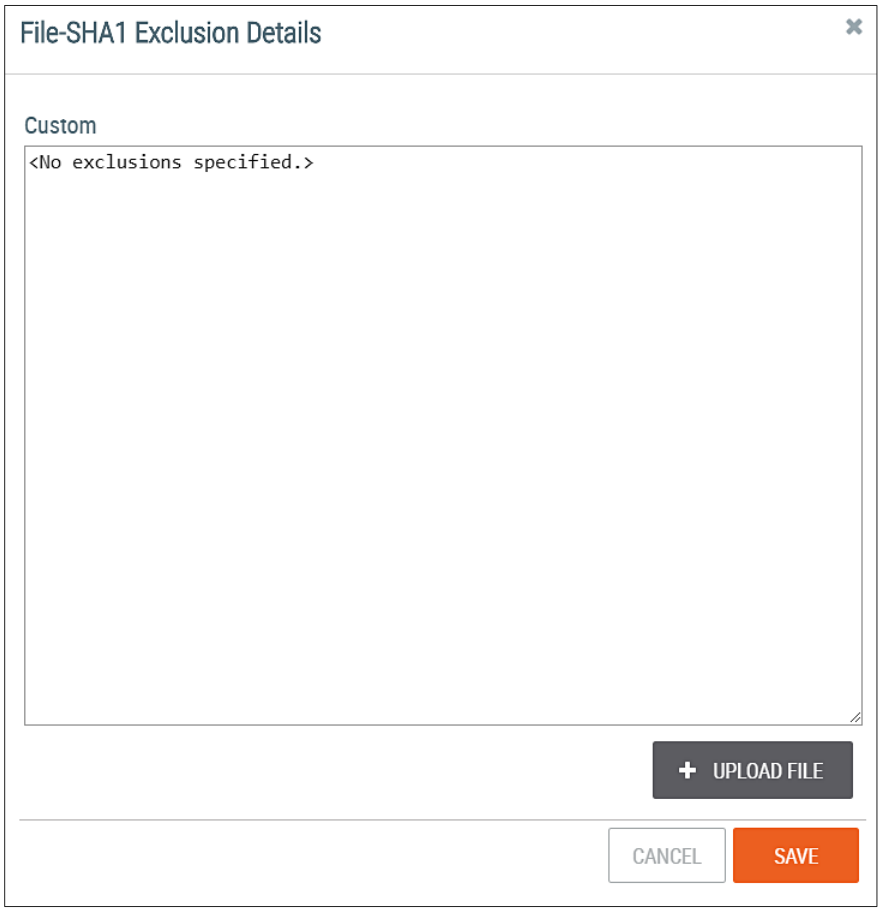

Figure 48

5. When creating a new Exclusion List, enter the information directly into the **Custom** text box, and click the **SAVE** button (Figure 49).

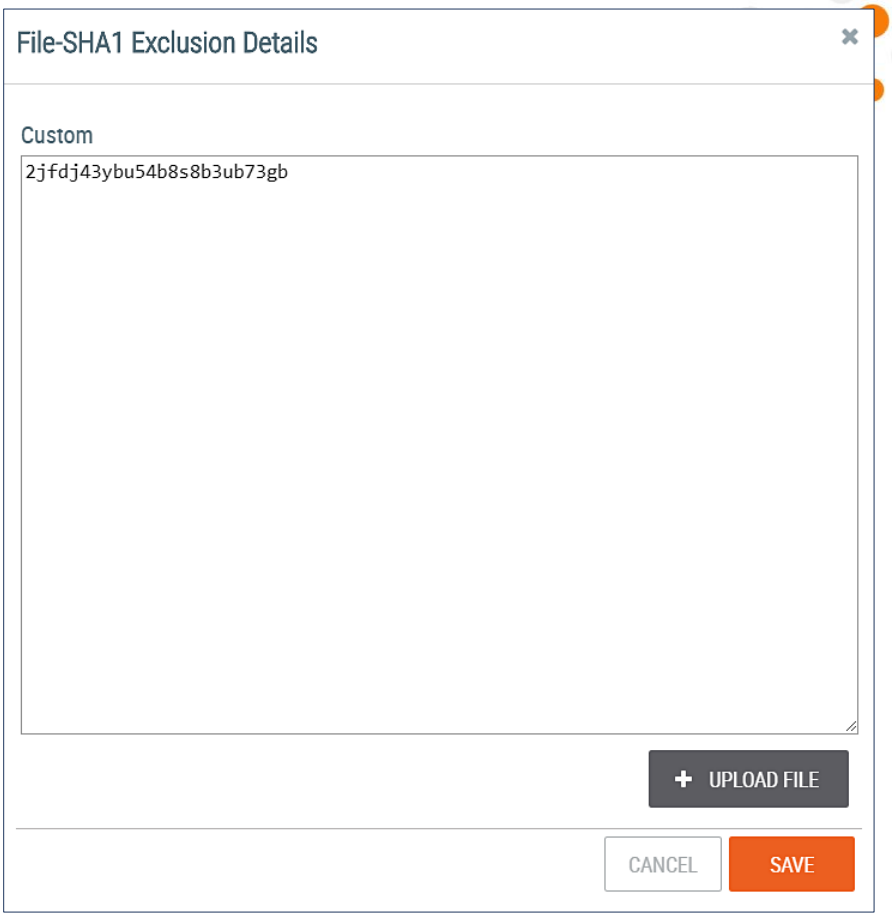

Figure 49

6. Otherwise, click the **+ UPLOAD FILE** button to navigate to the appropriate directory. The file must be in **.txt** format. Also, place an asterisk (*) at the beginning and end of the Indicator to exclude all results. For example, ***xyz.com*** in the URL Exclusion list would exclude any URL that contains the string **xyz.com**.
7. Select the desired file, and the Exclusion list will be uploaded (Figure 50).

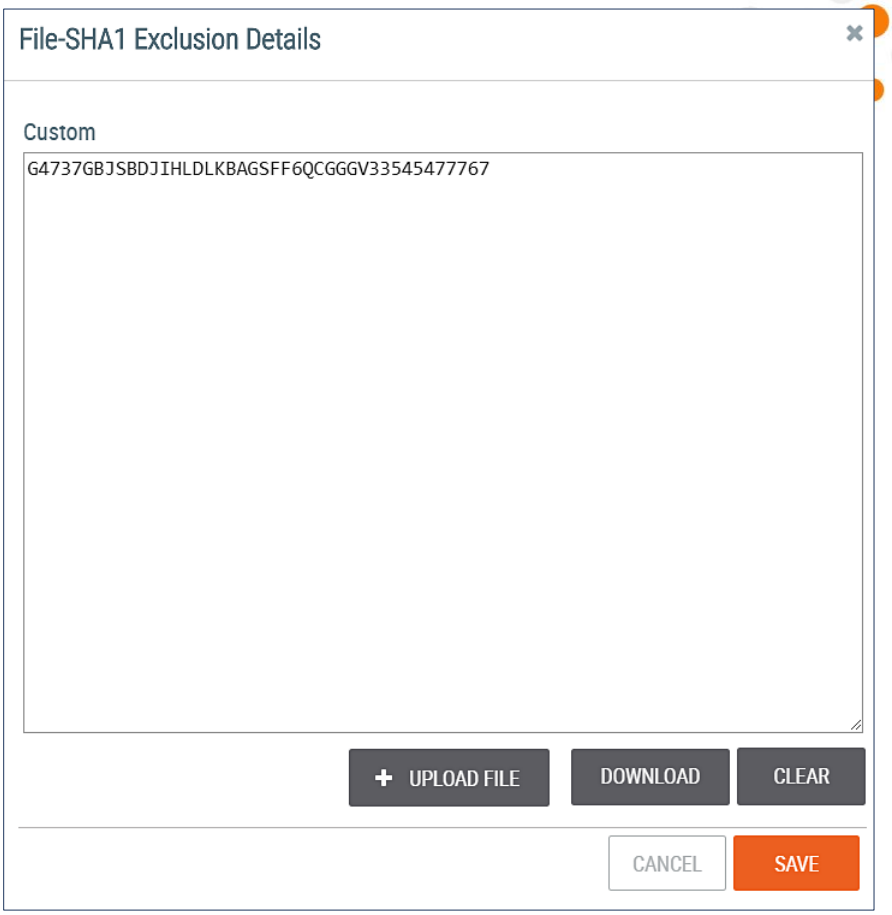

Figure 50

8. Click the **SAVE** button.
9. To modify an existing Exclusion list, edit it directly from the **Custom** text box. Otherwise, click the **DOWNLOAD** button to download and edit a file, and then click the **+ UPLOAD FILE** button to upload the edited file.
10. Click the **SAVE** button.

    NOTE: When trying to create an Indicator that has been placed on an Exclusion list, a message will appear in the Create pop-up screen warning that the Indicator is contained on an Organization-wide Exclusion list.

11. To remove an existing **Custom** Exclusion list, click the **CLEAR** button, and the **Remove Exclusions** pop-up screen will appear (Figure 51).

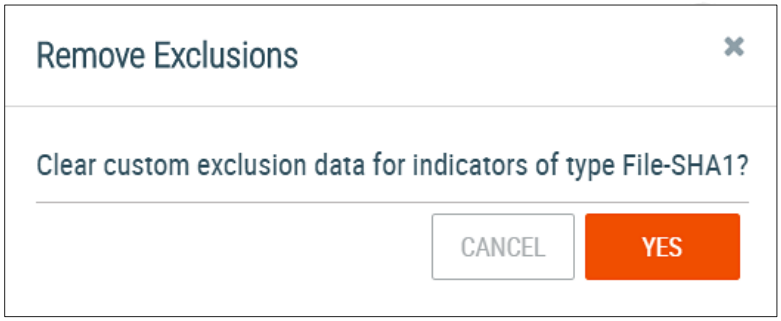

Figure 51

12. Click the **YES** button followed by the **SAVE** button.

Potential Associations Exclusions

Click the **Potential Associations Exclusions** tab to display the **Exclusion Rules** screen (Figure 54). These rules are not included by default, but users can add them. They prevent artifacts from creating potential associations between cases if the artifacts are on the Exclusion List. At the Organization level ThreatConnect supports exclusion lists for Indicators and for associations, which users can configure for individual Organizations.

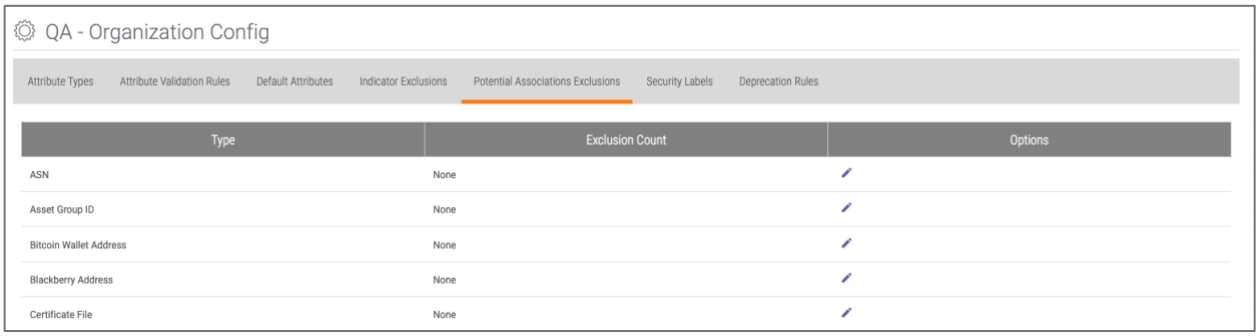

Figure 52

To edit or modify am Exclusion Rule, click the **Edit** icon to the right of an entry, and the **Exclusion Details** pop-up screen (Figure 54) will appear (ASN Type in this example). Enter the custom exclusion details manually, or click the **+ UPLOAD FILE** button to navigate to a directory. When done, click the **SAVE** button.

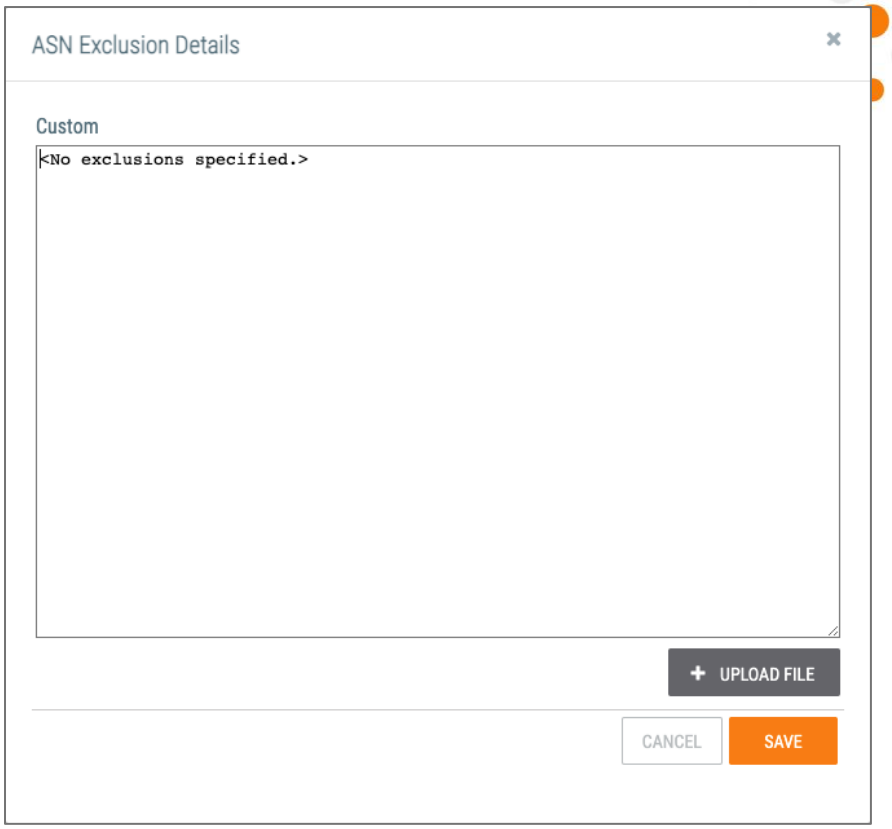

Figure 53

Security Labels

An Organization may use custom Security Labels to determine how to treat Groups and Indicators in bulk. Security Labels are a good way to designate how information should be treated. Within the Common Community, ThreatConnect uses the Traffic Light Protocol (TLP) system developed by the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). Administrators can define their own Security Labels based on their Organization's needs.

Security Labels are most effective when users share or contribute information within ThreatConnect—which allows them to withhold or divulge information, depending on their Organization's policies, based on the Security Label applied to each piece of data.

Security Labels are applied not just to Groups and Indicators, but also to their Attributes. For example, an IP Address Indicator may be considered TLP:Green (i.e., peers and partner Organizations may see it). However, its Source Attribute may be a sensitive system log that pinpoints a system vulnerability and, thus, may be considered TLP:Red (i.e., not to be shared). Administrators are encouraged to familiarize their users with their Organizations' sharing policies and the Security Labels used to enact them.

Creating Custom Security Labels

Follow these steps to create a custom Security Label:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38).
3. Click the **Security Labels** tab, and the **Security Labels** screen will appear (Figure 54). If the **Include System Labels** box is checked, the table will display ThreatConnect System Security Labels.

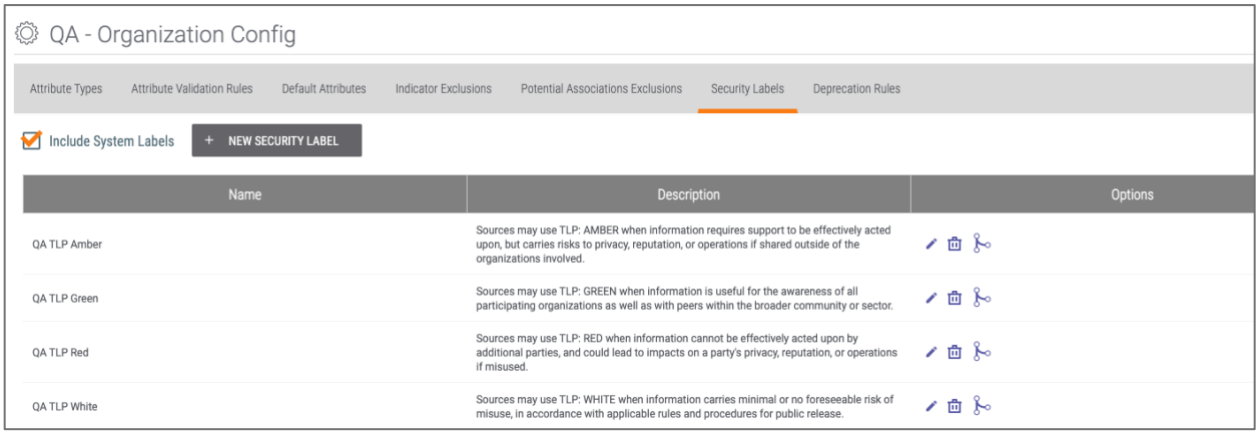

Figure 54

4. To create a new Organization Security Label, click the **+ NEW SECURITY LABEL** button, and the **Create Security Label** pop-up screen will appear (Figure 55).

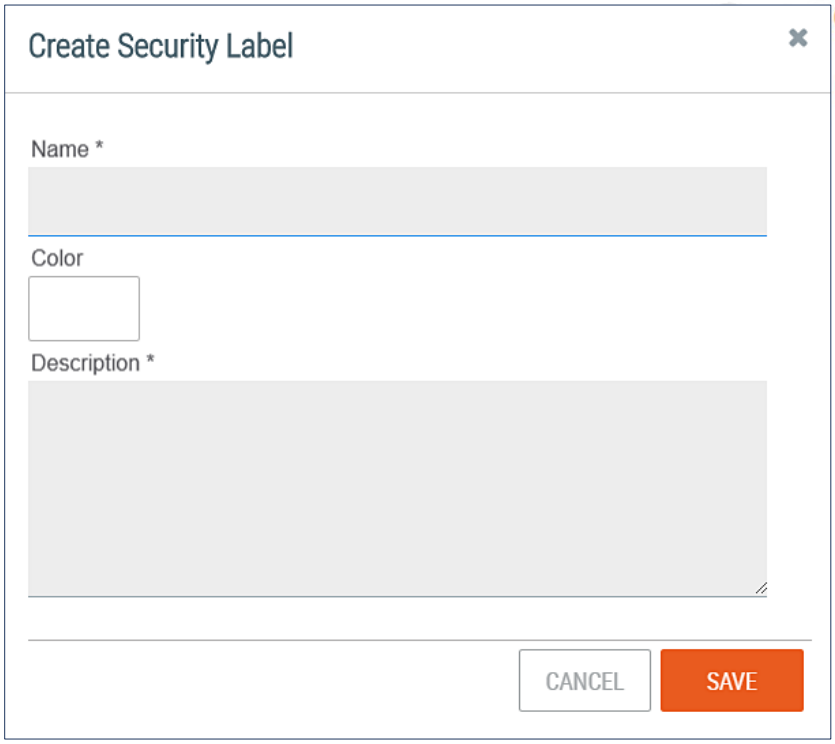

Figure 55

5. Click in the boxes to enter the **Name**, **Color**, and **Description** of the Security Label.

   NOTE: These fields are provided solely for user and Administrator readability, as no policy enforcement is derived from this screen.

6. Click the **SAVE** button.

Editing Custom Security Labels

Follow these steps to edit a custom Security Label:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38).
3. Click the **Security Labels** tab, and the **Security Labels** screen will appear (Figure 54).
4. Select a Security Label from the table, and click the **Edit** icon, and the **Create Security Label** pop-up screen will appear (Figure 56).

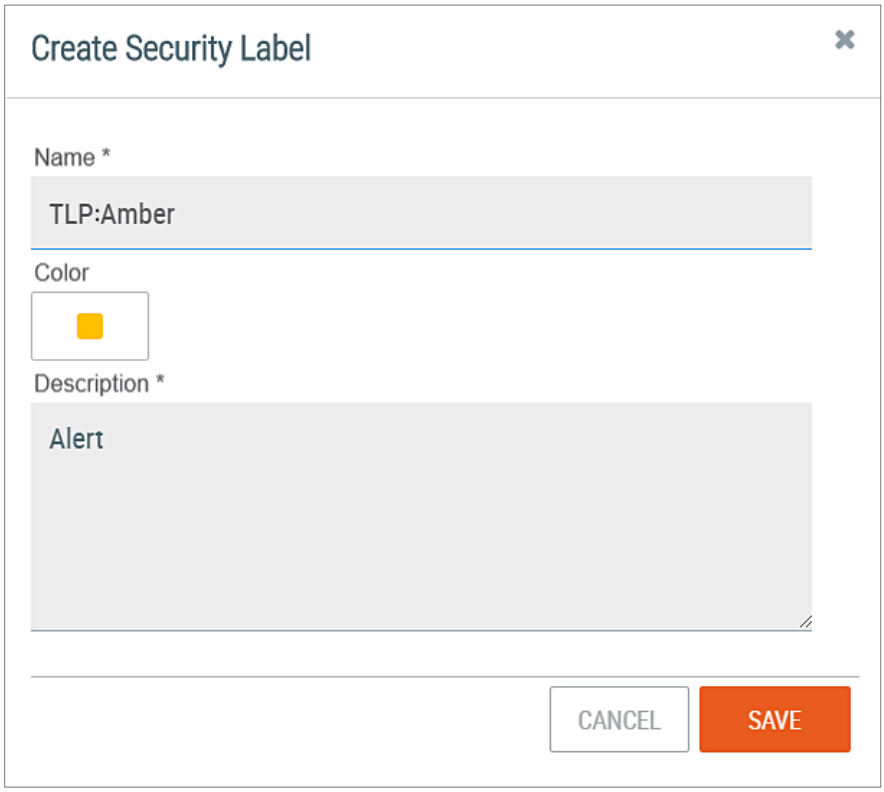

Figure 56

1. Click within the boxes to edit the Security Label.
2. Click the **SAVE** button.
3. To delete a Security Label, select an entry from the table and click the **Delete** icon.

4. To consolidate a Security Label, select an entry from the table and click the **Consolidate** icon, and the **Consolidate Security Label** pop-up menu will appear (Figure 57).

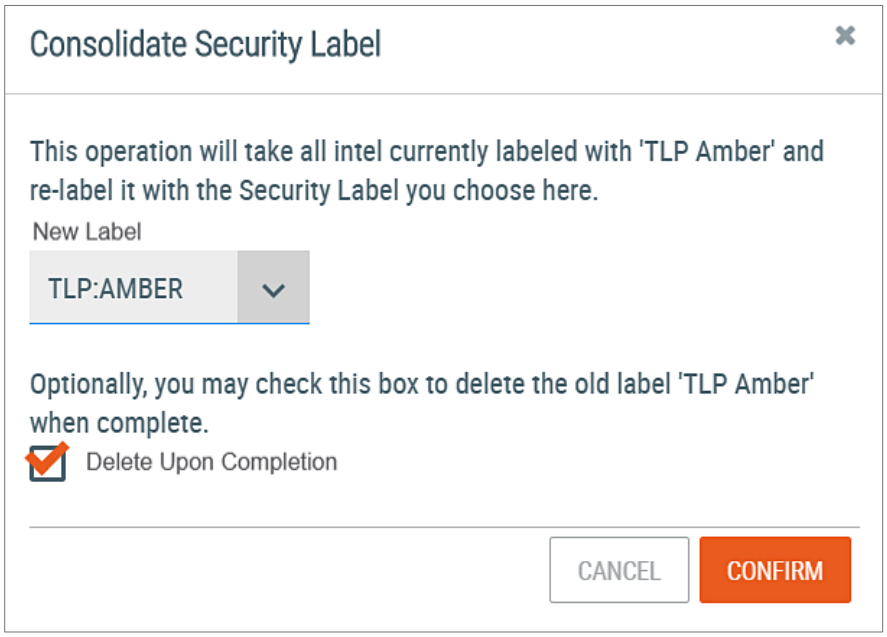

Figure 57

5. Click the drop-down arrow to select a new Security Label under which to consolidate all Intel labeled with the current Label. If the **Delete Upon Completion** box is checked, the old Label will be deleted once the selection is confirmed.
6. Click the **CONFIRM** button to save the selection.

Deprecation Rules

Deprecation Rules define how ThreatConnect handles Indicators made irrelevant because of inactivity—queuing them up for deletion when they have met specified deprecation criteria. The next sub-section demonstrates a Deprecation Rule for IP addresses that have not been modified or updated in 180 days. After 180 days of inactivity, ThreatConnect decrements the confidence of the IP Address by 100%, effectively making the Confidence Rating value be 0. ThreatConnect then deletes those Indicators from the system.

Creating Deprecation Rules

Follow these steps to create a Deprecation Rule:

1. Log in with an Org Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **Org Config**, and the **Organization Config** screen will appear (Figure 38).

3. Click the **Deprecation Rules** tab, and the **Deprecation Rules** screen will appear (Figure 58).

Figure 58

4. To create a new Deprecation Rule, click **+ NEW** button, and the **Create/Edit Deprecation Rule** pop-up screen will appear (Figure 59), with fields to enter the **Indicator Type**, **Confidence Amount,** what **Action At Minimum** to take (when an Indicator reaches or goes below **0** Confidence), deprecation time **Interval**, and checkboxes to indicate whether to express the Confidence as a **Percentage** and whether the Deprecation Rule should be **Recurring**.

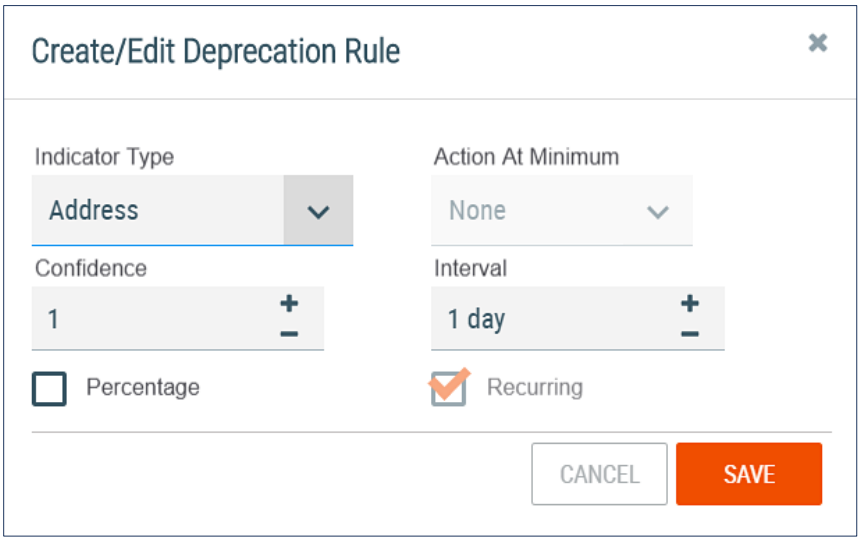

Figure 59

5. Click the **SAVE** button when finished.