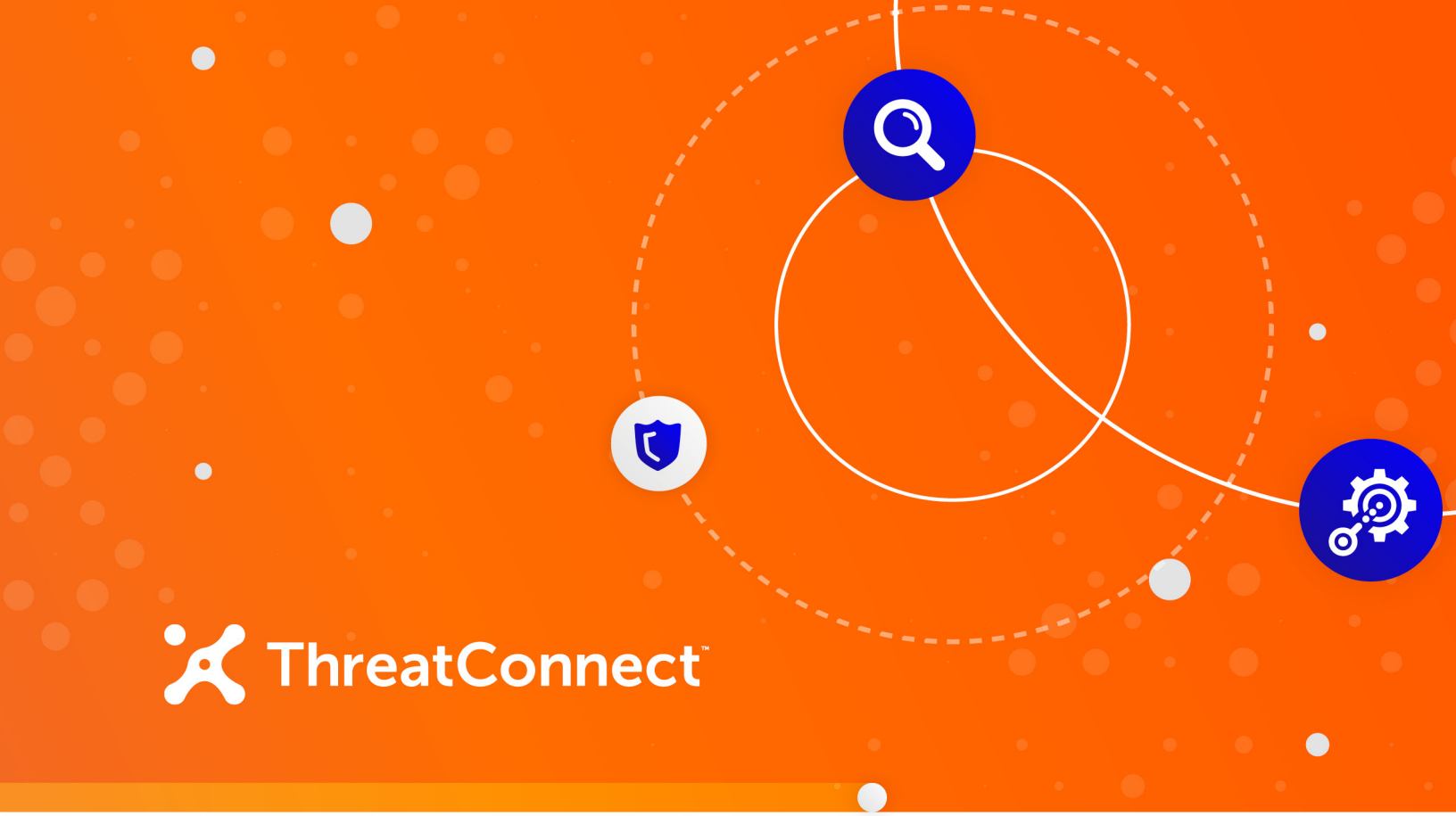

ThreatConnect™

Account Administration

User Guide

Software Version 6.0.1

March 30, 2020

10010-08 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

ThreatConnect™

Table of Contents

SYSTEM ADMINISTRATION

Getting Started

A System Administrator account within ThreatConnect® works, in many ways, just like a normal Organization account—it even belongs to an Organization that can contain other System Administrator accounts—but it has additional permissions and capabilities that allow the user to configure system settings within On Premises and Private Cloud ThreatConnect Instances. This section explains many of the tasks requiring system privileges.

Because of the account's ability to change system settings, it is advised that the account be used only for these tasks and not for Organization administration, Community administration, or regular analysis. In general, administrative tasks should always be carried out by the least-privileged account possible to help maintain system security and functionality.

System Account Familiarization

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).

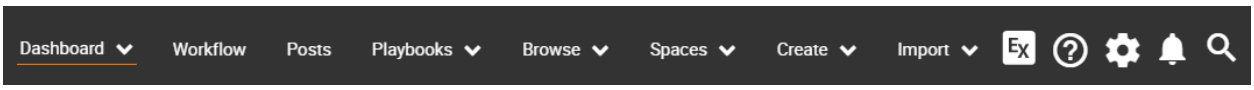

Figure 1

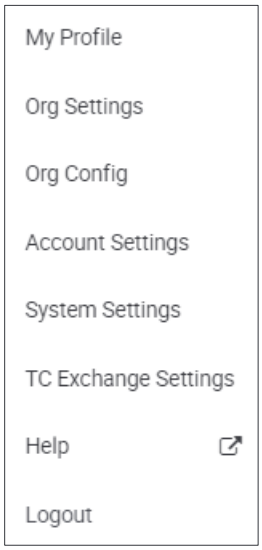

Figure 2

Table 1 provides an overview of the **Settings** menu options.

Table 1

Setting Types	Description
My Profile	Use this option to configure basic user settings for this account, including password changes.
Org Settings	Use this option to create and configure other user accounts within the Organization. Typically, these are other System Administrator accounts.
Org Config	Use this option to modify Attributes, Indicator Exclusion Lists, Security Labels, and Deprecation for a given Organization.
Account Settings	Use this option to create, configure, and manage all Organizations and accounts within an On Premises Instance.
System Settings	Use this option to configure System-wide properties for On Premises Instance.
TC Exchange™ Settings	Use this option to view loaded apps, to install apps, and to configure System Jobs, among other features.
Help	Use this option to access the ThreatConnect Knowledge Base in a new window.
Logout	Use this option to log out of ThreatConnect.

This section focuses on the system-wide tasks that are performed primarily in **Account Settings**. For further information on tasks performed in **System Settings**, refer to the *System Administration User Guide*.

Organization Management

All tasks related to system-wide account management are available from the **Account Settings** screen.

Creating an Organization

Follow these steps to create a new Organization:

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).

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

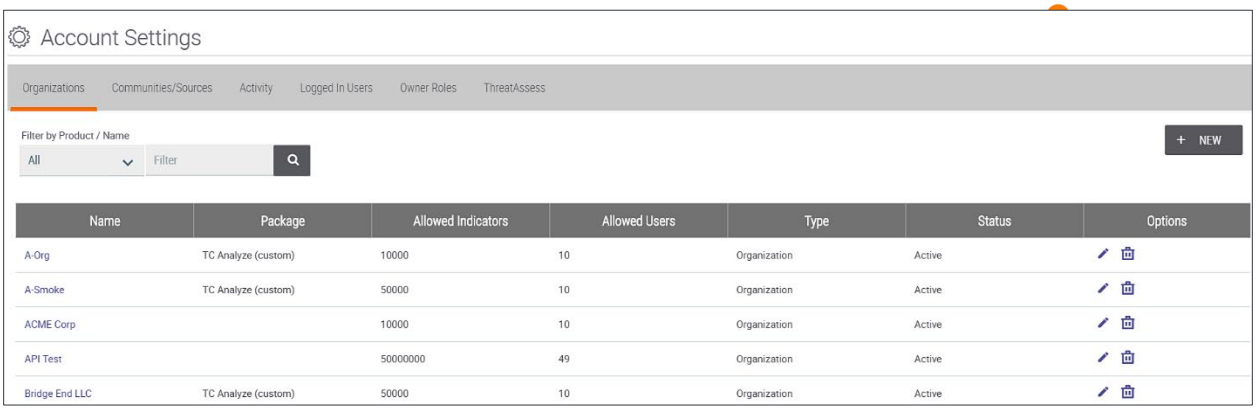

Figure 3

4. Click the **+ NEW** button, and the **Create Organization** pop-up screen will appear (Figure 4).

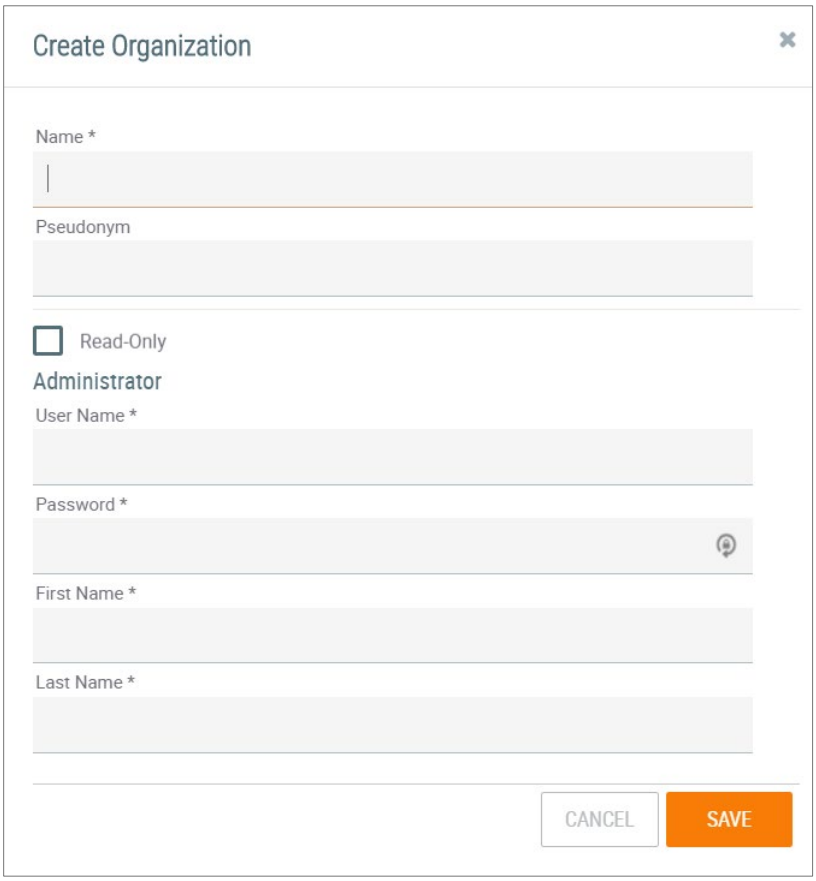

Figure 4

NOTE: If the + NEW button is not visible, check if all licensed user accounts have been allocated. Either deallocate any unused user accounts, or purchase a license upgrade to allow more user accounts.

5. Fill in the fields to create the Organization and its initial Administrator account. Fields with asterisks are required. Click the **Read-Only** checkbox to restrict the permissions to read-only status.

   NOTE: It is advised that all user names be a valid email address so that system invites, follow updates, and other system-generated notifications can be sent to the user.

6. Click the **SAVE** button to save the settings and create the Organization.

Configuring an Organization Account

The **Organizations** tab of the **Account Settings** screen displays a table of existing accounts. Most account configuration is done from the options in this table.

Follow these steps to configure an account:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Edit** icon in the **Options** column of the Organization whose information is to be configured. The **Organization Information** pop-up screen will appear (Figure 5) with the **Standard Options** tab underlined.

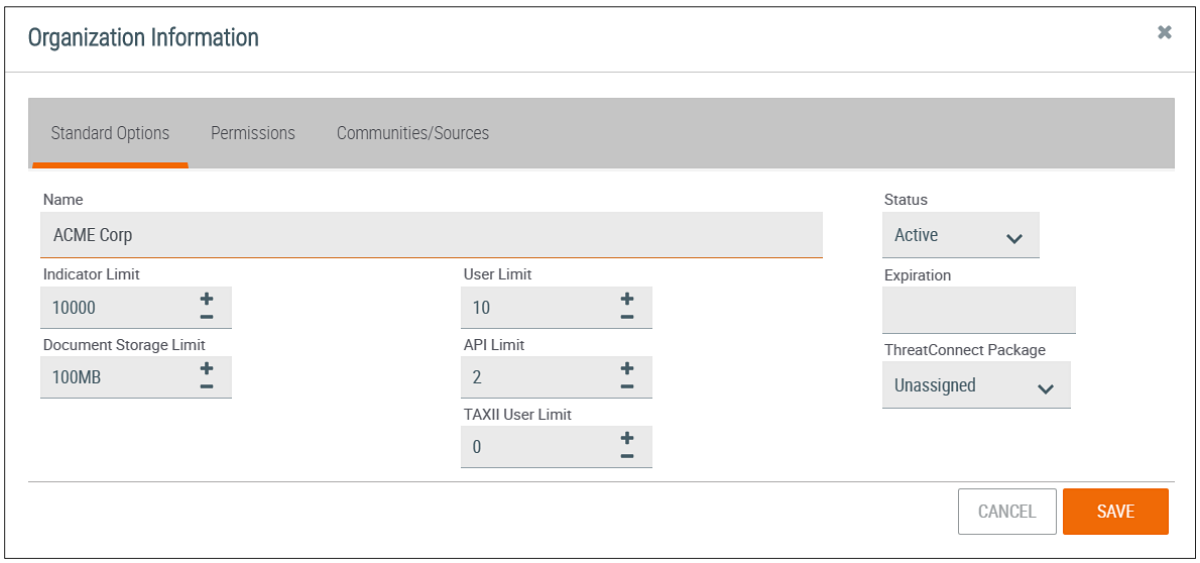

Figure 5

   a. **Name**: Click in the box to enter an Organization account name.

   b. **Indicator Limit**: Click in the box (or use the plus and minus signs) to configure Indicator Limits for the Organization.

NOTE: If this limit is not configured, an Organization will not be able to create any internal Indicators.

c. **Document Storage Limit**: Click in the box (or use the plus and minus signs) to enter the amount of space an Organization has for storing documents.

d. **User Limit**: Click in the box (or use the plus and minus signs) to limit the number of users that can exist within an Organization.

NOTE: The default value is 1.

e. **API Limit**: Click in the box (or use the plus and minus signs) to limit the number of API users that can exist within an Organization.

f. **Taxii User Limit**: Click in the box (or use the plus and minus signs) to limit the number of Taxii users that can exist within an Organization.

g. **Status**: Click in the box to select whether the status of the Organization is Active or Expired. An Organization with Expired status exists, but is not accessible.

h. **Expiration**: Click in the box to set a date for when the Organization will no longer be accessible within ThreatConnect. On this date, the status of the Organization will change from **Active** to **Expired**.

i. **ThreatConnect Package:** Click the drop-down arrow to select one of the TC packages. The selection will determine the options available under the Permissions tab.

5. Click the **Permissions** tab to view the Permissions screen (Figure 6).

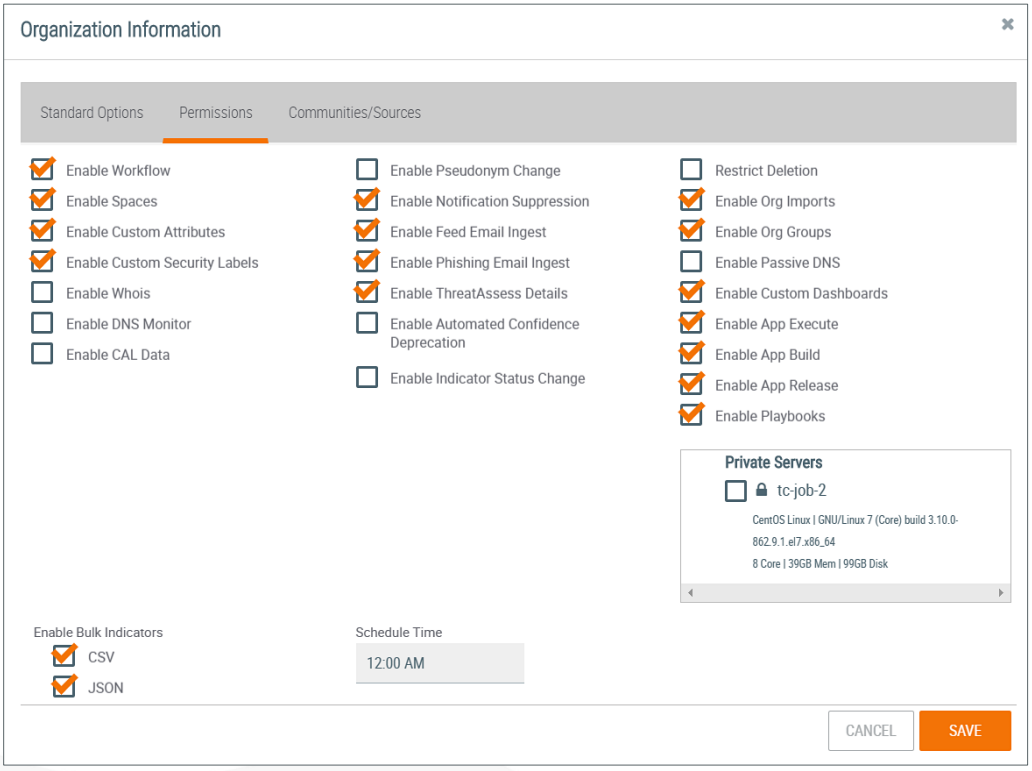

Figure 6

a. **Enable Workflow**: Click the checkbox to enable the workflow tasks feature.

b. **Enable Spaces**: Click the checkbox to enable the creation of Spaces.

c. **Enable Custom Attributes**: Click the checkbox to enable the creation of Custom Attributes.

d. **Enable Custom Security Labels**: Click the checkbox to enable the creation of Custom Security Labels.

e. **Enable Whois**: Click the checkbox to enable the Whois feature.

f. **Enable DNS Monitor**: Click the checkbox to enable the DNS Monitor feature.

g. **Enable CAL Data**: Click the checkbox to enable the compilation of CAL data.

h. **Enable Pseudonym Change**: Click the checkbox to allow the Organization to change its pseudonym.

NOTE: An Organization is able to set or change its pseudonym once. After the pseudonym is set or changed, the Allow Pseudonym Change checkbox will be unchecked and will require the System Administrator to check it again if another pseudonym change is necessary.

i. **Enable Notification Suppression**: Click the checkbox to enable a feature that gives the user the ability to turn off notifications for communication threads in which the user is actively participating.

j. **Enable Feed Email Ingest**: Click the checkbox to allow the Feed Email Ingest feature for the Organization.

k. **Enable Phishing Email Ingest**: Click the checkbox to allow the Phishing Email Ingest feature for the Organization.

l. **Enable ThreatAssess Details**: Click the checkbox to enable the display of ThreatAssess details.

m. **Enable Automated Confidence Deprecation**: Click the checkbox to enable the Confidence Deprecation feature.

n. **Enable Indicator Status Change**: Click the checkbox to enable the ability to change an Indicator's status.

o. **Restrict Deletion**: Click the checkbox to prevent users from deleting an Organization. Doing so will remove the **Delete**  icon from the Organization name displayed in the table.

p. **Enable Org Imports**: Click the checkbox to enable Organization Imports.

q. **Enable Org Groups**: Click the checkbox to enable Organization Groups. When the permission checkbox is left unchecked, there are no obvious changes to an Organization's user interface, so that Groups are still accessible via the **Browse** screen. When a user attempts to create a Group, however, the user's Organization is not listed in the Owner drop-down menu, effectively restricting the user's ability to create Groups in the organization. Depending on users' Community and Source permissions, they may be granted access to create Groups elsewhere.

r. **Enable Passive DNS**: Click the checkbox to enable Passive Domain Name System (DNS) data service.

NOTE: A Passive DNS API key is still required for this feature to work.

s. **Enable Custom Dashboards**: Click the checkbox to enable the ability to create custom Dashboards.

t. **Enable App Execute**: Click the checkbox to enable the ability to execute apps.

u. **Enable App Build**: Click the checkbox to enable the ability to build apps.

v. **Enable App Release**: Click the checkbox to enable the ability to release apps.

w. **Enable Playbooks**: Click the checkbox to enable the Playbooks Apps feature.

x. **Enable Bulk Indicators**: Click the **CSV** (Comma-Separated Values) or **JSON** (JavaScript® Object Notation) checkboxes to enable the Bulk Indicator Export feature.

y. **Private Servers**: Click the checkbox to enable the Private Server feature.

6. Click the **Communities/Sources** tab to view the **Communities/Sources** screen (Figure 7). From this screen, an Organization can be added to a Community or Source.

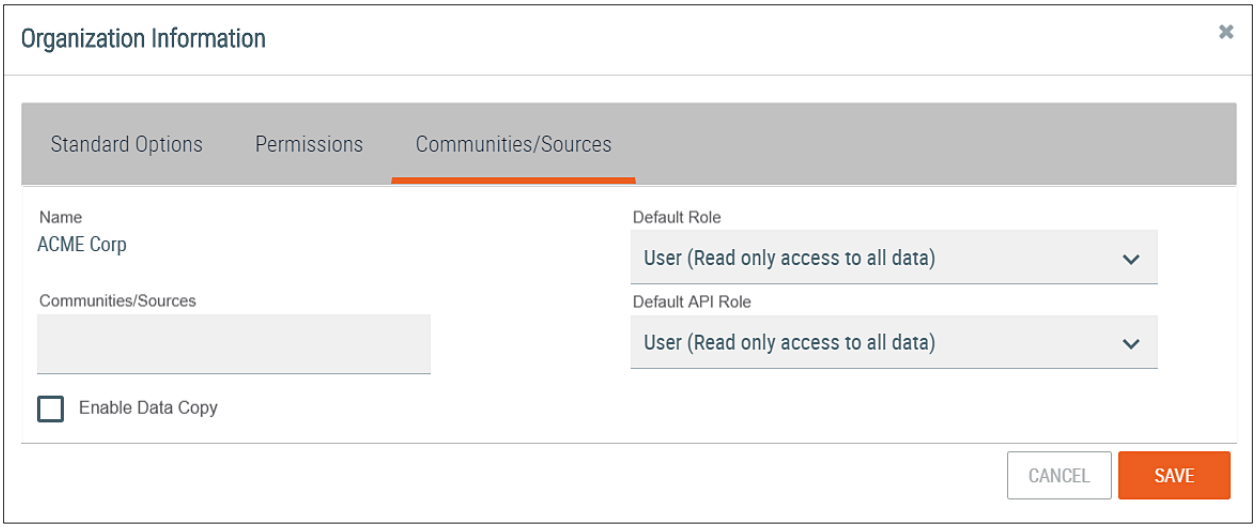

Figure 7

a. **Communities/Sources**: Click in the box and type the name of a Community or Source for the Organization to join. As a name is typed, matching options will appear below the box. Select one or more options until all desired names are chosen.

b. **Default Role**: Click on the drop-down menu to select the Default Role all the accounts within the Organization will be given in the Community or Source.

NOTE: Details on Community and Source roles can be found in the ThreatConnect Community and Source Administration User Guide.

c. **Default API Role**: Click on the drop-down menu to select the Default Role all API accounts within the Organization will be given.

d. **Allow Data Copy**: Click the checkbox to allow Community users to copy data from the Community to their private Organization.

7. Click the **SAVE** button to save the settings.

Adding Additional Users to an Organization

NOTE: ThreatConnect advises that the Org Administrator, not a System Administrator, create the user accounts for the Organization, particularly for a new Organization. This practice allows the Org Administrator to set the Org pseudonym and assign specific privileges to the Org users prior to System login.

Follow these steps to add users to an existing Organization account:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click on the hyperlinked **Organization** name in the **Name** column. The **Organization Settings** screen for that account will appear (Figure 8).

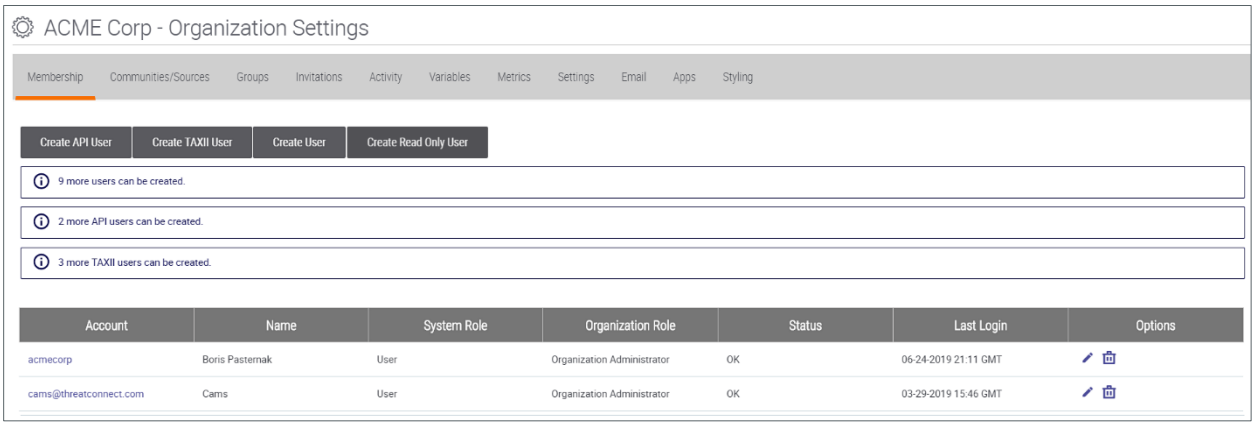

Figure 8

5. Click on the **Create API User**, **Create TAXII User**, or **Create User** button to create a new user. The details of this configuration are covered in the *ThreatConnect Organization Administration Guide*.

   NOTE: A System Administrator account can create two other account roles that Organization accounts do not have the ability to create: Operations Administrator and Administrator. Typically, these account roles are created only within an Organization specifically used for system administration, such as the System Organization.

Deleting an Organization

Follow these steps to delete an Organization:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click on the **Delete** icon in the **Options** column of the Organization to be deleted.
5. The **Delete Organization** pop-up screen will appear (Figure 9). Click the **YES** button to delete the account.

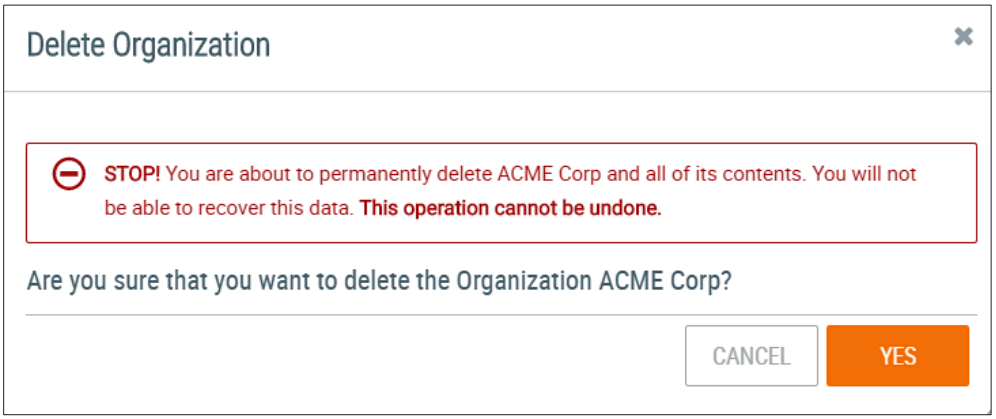

Figure 9

6. Click the **YES** button.

Community Management

Creating a Community

Follow these steps to create a new Community:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will appear (Figure 10).

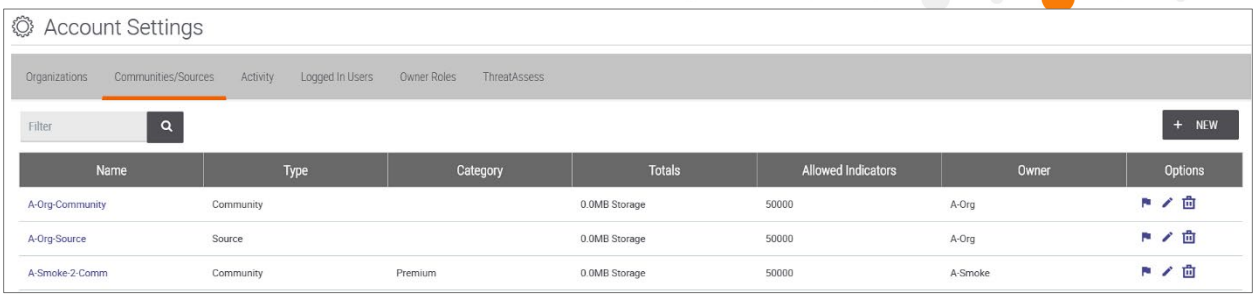

Figure 10

5. Click the **+ NEW** button, and the **Create Community/Source** pop-up screen will appear with the default **Community** radio button selected (Figure 11). Use the scroll bar on the right of the screen to access the **Description** text box.

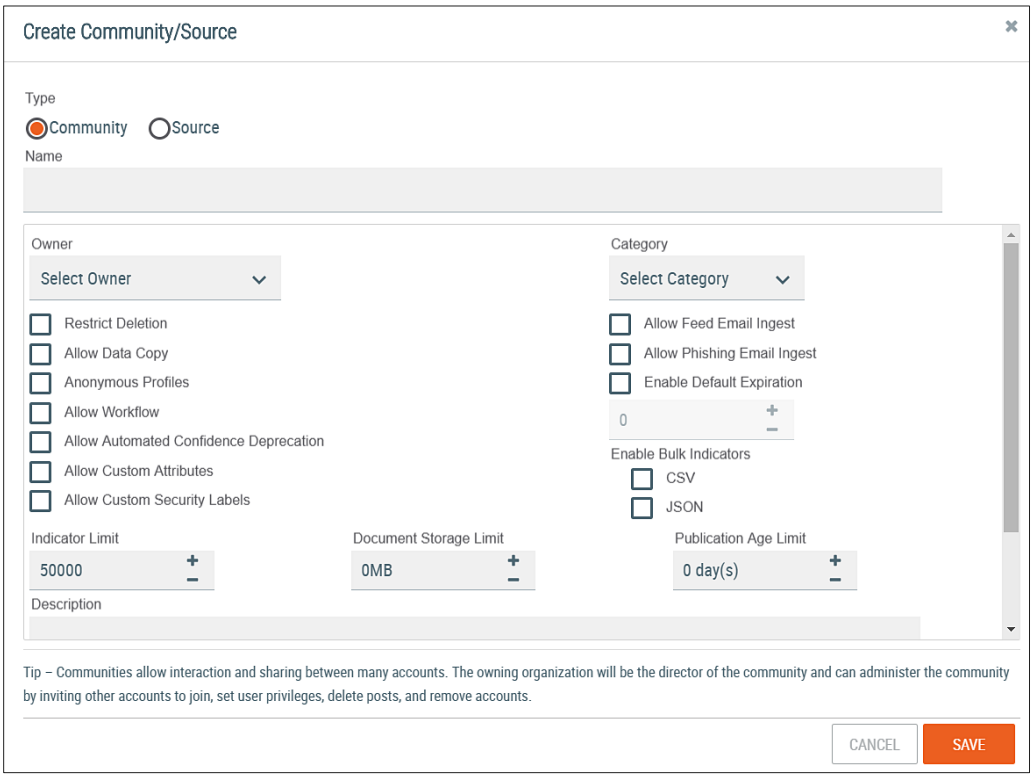

Figure 11

a. **Name**: Click in the box to enter the name of the Community.

b. **Owner**: Click on the **Select Owner** drop-down menu to select the Organization that will administer the Community and be given a Director role.

c. **Category**: Click on the **Select Category** drop-down menu to select the kind of Community to create.

d. **Restrict Deletion**: Click the checkbox to prevent users from deleting a Community. Doing so will remove the **Delete** icon from the Community name displayed in the table.

e. **Allow Data Copy**: Click the checkbox so that Community users are able to copy data from the Community to their private Organization.

f. **Anonymous Profiles**: Click the checkbox to enable the Community to allow anonymous profiles.

NOTE: A Community Director may change a full-profile Community to one that allows anonymous profiles, but is not able to change a Community that allows anonymous profiles to one that requires full profiles.

g. **Allow Workflow**: Click the checkbox to enable workflow tasks for the Community's objects.

h. **Allow Automated Confidence Deprecation**: Click the checkbox to create Deprecation Rules for the Community's Indicators.

i. **Allow Custom Attributes**: Click the checkbox to allow the creation of Custom Attributes.

j. **Allow Custom Security Labels**: Click the checkbox to allow the creation of Custom Security Labels.

k. **Enable Feed Email Ingest**: Click the checkbox to allow the Feed Email Ingest feature for the Community.

l. **Enable Phishing Email Ingest**: Click the checkbox to allow the Phishing Email Ingest feature for the Community.

m. **Enable Default Expiration**: Click the checkbox to enable the setting of a date for when the Community will no longer be accessible within ThreatConnect.

n. **Enable Bulk Indicators**: Click the **CSV** or **JSON** checkbox to enable the Bulk Indicator Export feature.

o. **Indicator Limit**: Click in the box (or use the plus and minus signs) to manually configure Indicator limits for the Community.

p. **Document Storage Limit**: Click in the box (or use the plus and minus signs) to enter the amount of document storage space available to a Community.

q. **Publication Age Limit**: Click the drop-down menu to limit what can be pulled (in days).

r. **Description:** Click in the box to enter an initial description for the Community.

NOTE: The Indicators are retrieved via the API, and bulkIndicatorEnabled must be true in System Settings, while bulkIndicatorTempLocation must be a valid writable directory. If JSON is selected, the API will return the latest version of the JSON report with a content-type header of application/json. The output is very similar to that returned by the Indicators Collection (e.g., in /v2/Indicators), with the addition of Attributes and Tags where relevant. If CSV is selected, the API will return the latest CSV report with a content-type header of text/csv. The report will contain all of the Indicators in the Community and their Indicator types. The report will also include each Indicator's Threat Rating and Confidence Rating values, if set, or null otherwise.

6. Click the **SAVE** button to create the Community.
7. If the new Community is not displayed, log out and log back in.

Configuring a Community

Follow these steps to configure a Community:

1. Follow the same steps as in the previous section, except instead of clicking on the **+ NEW** button, click on the Edit  icon of the selected Community.
2. After the changes have been saved, return to the Community listing and click on the Community's name to view other pertinent settings and information.

Adding Accounts to a Community

Follow these steps to add accounts to a Community:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Communities/Sources** tab, and the Communities/Sources screen will appear (Figure 10).
5. Click on the **Community Membership**  icon in the **Options** column of the Organization to which the accounts to be added belong. The **Community/Source** Membership pop-up screen will appear (Figure 12).

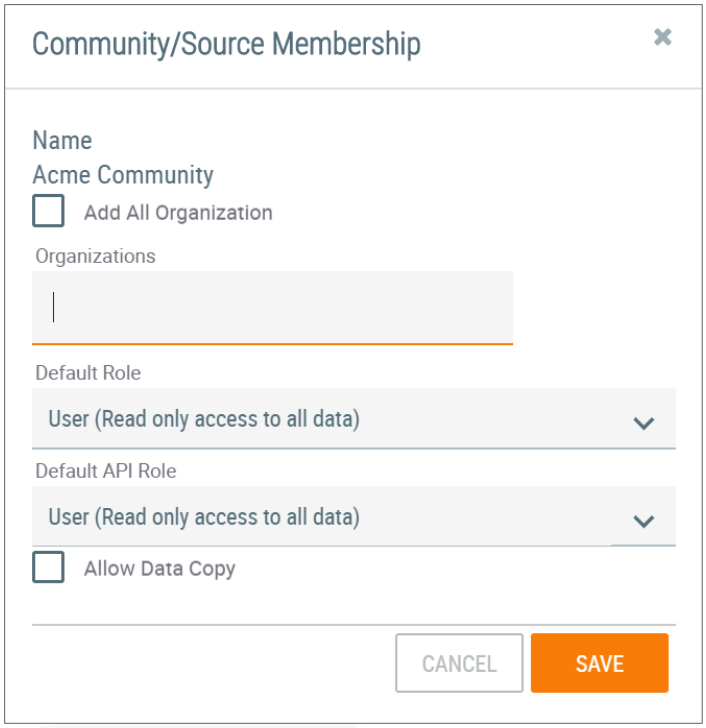

Figure 12

a. **Add All Organizations**: Click the checkbox to add all Organizations to the Community.

b. **Organizations**: Click in the box and type the name of an Organization to add to the Community. As a name is typed, matching options will appear below the box. Select one or more options until all Organizations that will participate in the Community are chosen.

c. **Default Role**: Click on the drop-down menu to select the Default Role all the accounts within the Organization will be given in the Community.

d. **Default API Role**: Click on the drop-down menu to select the Default Role all API accounts within the Organization will be given.

e. **Allow Data Copy**: Click the checkbox to allow Community users to copy data from the Community to their private Organization.

NOTE: For more information on the Default and Default API Roles, see the ThreatConnect Community and Source Administration User Guide.

6. Click the **SAVE** button to add the Organizations.

Deleting a Community

Follow these steps to delete a Community:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will appear (Figure 10).
5. Click on the **Delete** icon in the **Options** column of the Community to be deleted. The Delete Community pop-up screen will appear (Figure 13).

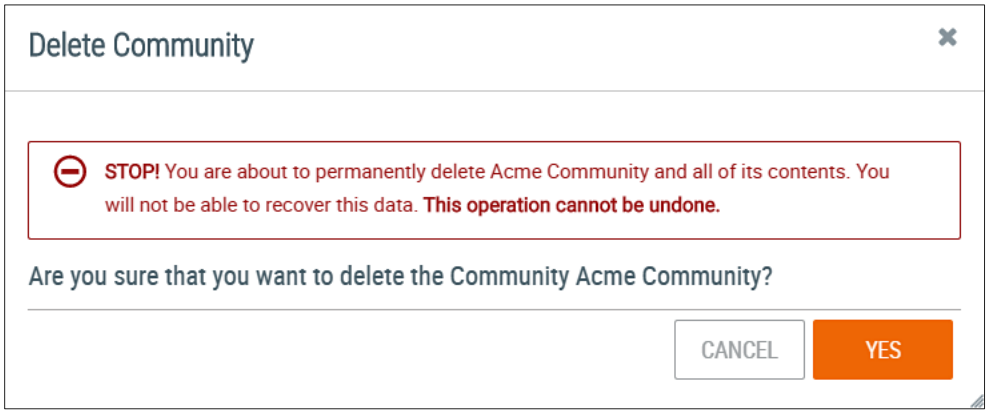

Figure 13

6. Click the **YES** button.

Performing Other Community Administrative Tasks

Follow these steps to perform other administrative tasks for a Community:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will appear (Figure 10).
5. Click on the Community name, and the **Community Information** screen will appear (Figure 14).

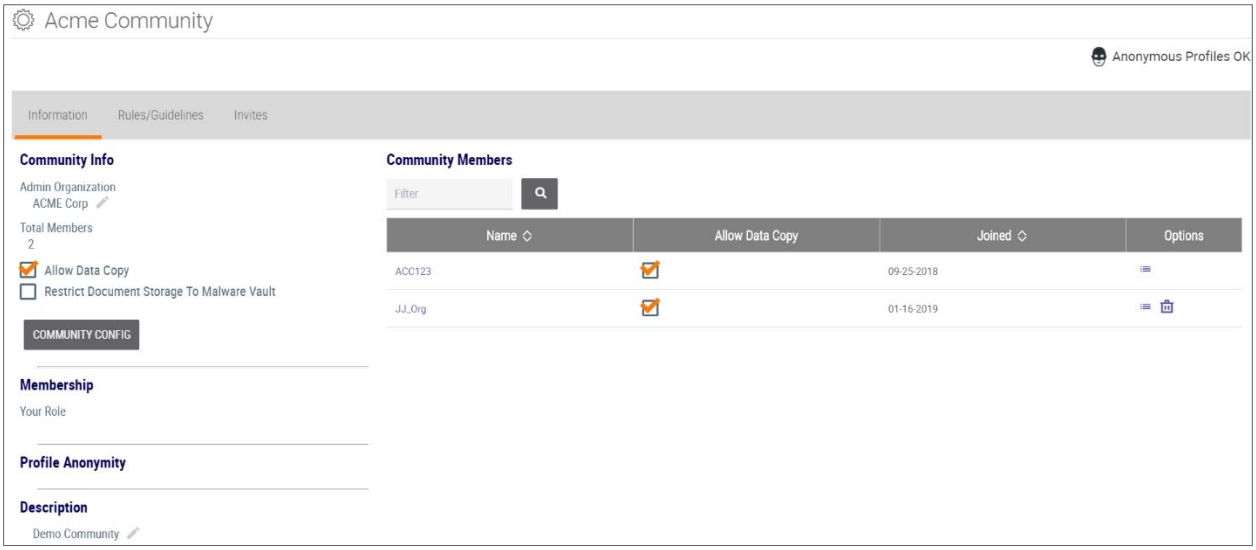

Figure 14

6. The **Community Information** screen allows the Administrator to send Community invites, set specific roles for Organizations and users within the Community, and edit Community rules and guidelines. These tasks are all covered in detail within the *ThreatConnect Community and Source Administration User Guide*.

Alternatively, the **Community Information** screen may be accessed by following these steps:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community.
2. On the top navigation bar (Figure 1), click **Posts**, and the Posts screen will appear(Figure 15).

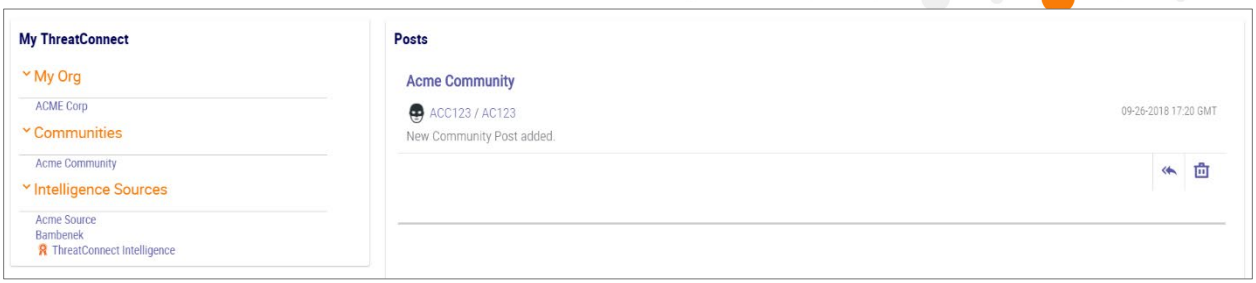

Figure 15

3. Click on the desired Community in the **My ThreatConnect** column, and its **Community Card** will appear on the top left of the screen (Figure 16).

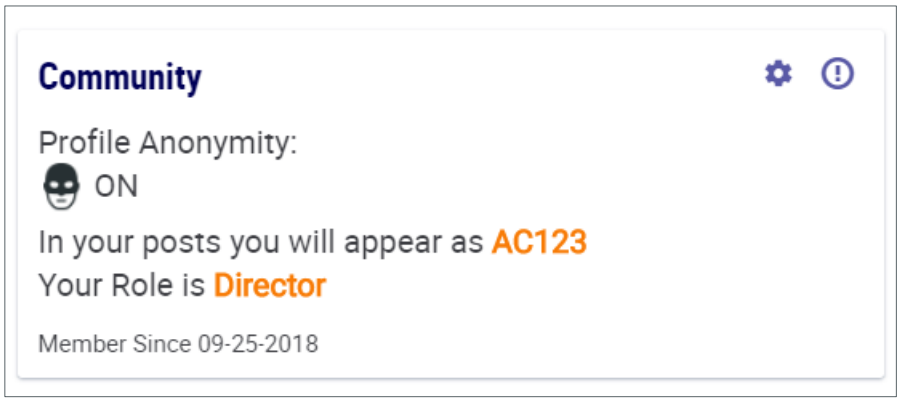

Figure 16

4. Click on the **Community Info** icon, and the **Community Info** screen will appear (Figure 14).

Source Management

Creating a Source

Follow these steps to create a new Source:

NOTE: When creating a new Source, users must log out of their account and log back in to see the newly created Source. Otherwise, it will appear as if the Source had not been created.

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will appear (Figure 10).

5. Click the **+ NEW** button, and the **Create Community/Source** pop-up screen will appear with the default **Community** radio button selected (Figure 11). Click the **Source** radio button(Figure 17), and use the scroll bar on the right of the screen to access the **Description** text box.

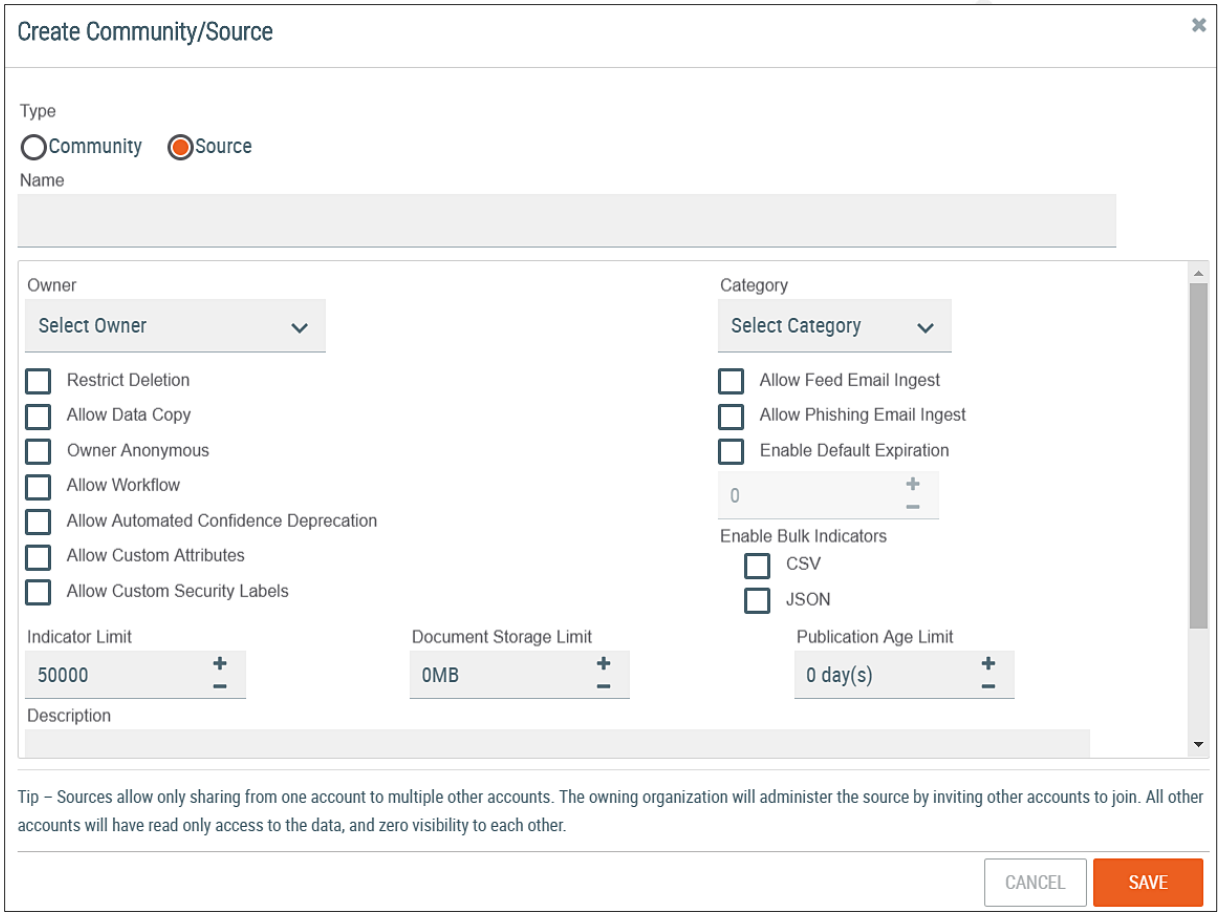

Figure 17

a. **Name**: Click in the box to enter the name of the Source.

b. **Owner**: Click on the **Select Owner** drop-down menu to select the Organization that will administer the Source.

c. **Category**: Click on the **Select Category** drop-down menu to select the kind of Source to create.

d. **Restrict Deletion:** Click the checkbox to prevent users from deleting a Source. Doing so will remove the **Delete** icon from the Source name displayed in the table.

e. **Allow Data Copy**: Click the checkbox to enable Source consumers to copy data from the Source to their private Organization.

f. **Owner Anonymous**: Click the checkbox to allow Source consumers to see the identity of the Source owner.

g. **Allow Workflow**: Click the checkbox to enable workflow tasks for the Source's objects.

h. **Allow Automated Confidence Deprecation**: Click the checkbox to enable the Deprecation Rules feature for the Source's Indicators.

i. **Allow Custom Attributes**: Click the checkbox to allow the creation of Custom Attributes.

j. **Allow Feed Email Ingest**: Click the checkbox to allow the Feed Email Ingest feature for the Source.

k. **Allow Phishing Email Ingest**: Click the checkbox to allow the Phishing Email Ingest feature for the Source.

l. **Enable Default Expiration**: Click the checkbox to enable the setting of a date for when the Source will no longer be accessible within ThreatConnect.

m. **Enable Bulk Indicators**: Click the **CSV** or **JSON** checkbox to enable the Bulk Indicator Export feature.

NOTE: The Indicators are retrieved via the API, and bulkIndicatorEnabled must be true in System Settings, while bulkIndicatorTempLocation must be a valid writable directory. If JSON is selected, the API will return the latest version of the JSON report with a content-type header of application/json. The output is very similar to that returned by the Indicators Collection (e.g., in /v2/Indicators), with the addition of Attributes and Tags where relevant. If CSV is selected, the API will return the latest CSV report with a content-type header of text/csv. The report will contain all of the Indicators in the Source and their Indicator types. The report will also include each Indicator's Threat Rating and Confidence Rating values, if set, or null otherwise.

n. **Indicator Limit**: Click in the box (or use the plus and minus signs) to manually configure Indicator limits for the Source.

NOTE: If this limit is not configured, a Source will not be able to create any Indicators within its Organization.

o. **Document Storage Limit**: Click in the box (or use the plus and minus signs) to enter the amount of document storage space available to a Source.

p. **Publication Age Limit**: Click the drop-down menu to limit what can be pulled (in days).

q. **Description:** Click in the box to enter an initial description for the Source.

6. Click the **SAVE** button to create the Source.
7. Log out and log back in to see the newly created Source.

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Activity** tab, and the **Activity** screen will appear (Figure 18).

Figure 18

5. Click on the **Filter** drop-down menu above the **Summary** column (with a default value of **ALL**) to select the activities of interest (Figure 19).

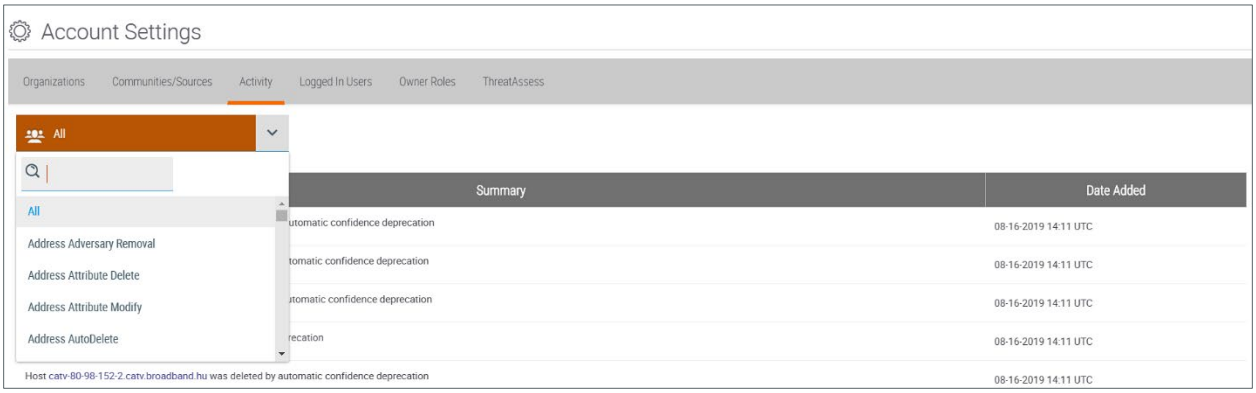

Figure 19

Logged-In Users

Viewing Logged-In Users or Administrators

Follow these steps to view users or administrators who are currently logged in:

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

4. Click the **Logged In Users** tab, and the **Logged In Users** screen will appear (Figure 20), displaying a table with the User Name, Organization, and IP Address from which the account is logged in.

Figure 20

Owner Roles

Viewing Owner Roles

Follow these steps to view the Owner Roles and their corresponding descriptions:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Owner Roles** tab, and the **Owner Roles** screen will appear (Figure 21), displaying a list of all available roles and a description of their function within an Organization or Community and as carried out by an Administrator.

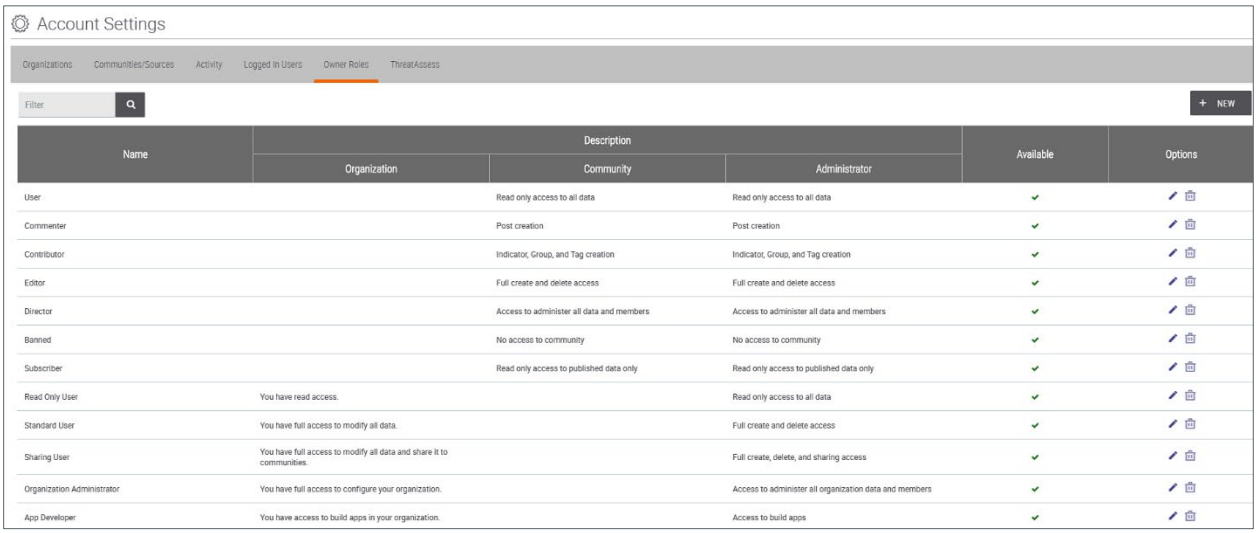

Figure 21

NOTE: The** User, Commenter, **and** App Developer **roles have unlimited 'limited access' capability, and, thus, these roles ignore the licensed user limits.

Creating a New Owner Role

Follow these steps to create a new Owner Role:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Owner Roles** tab, and the **Owner Roles** screen will appear (Figure 21).
5. Click the **+ NEW** button, and the **Create Owner Role** pop-up screen will appear (Figure 22).

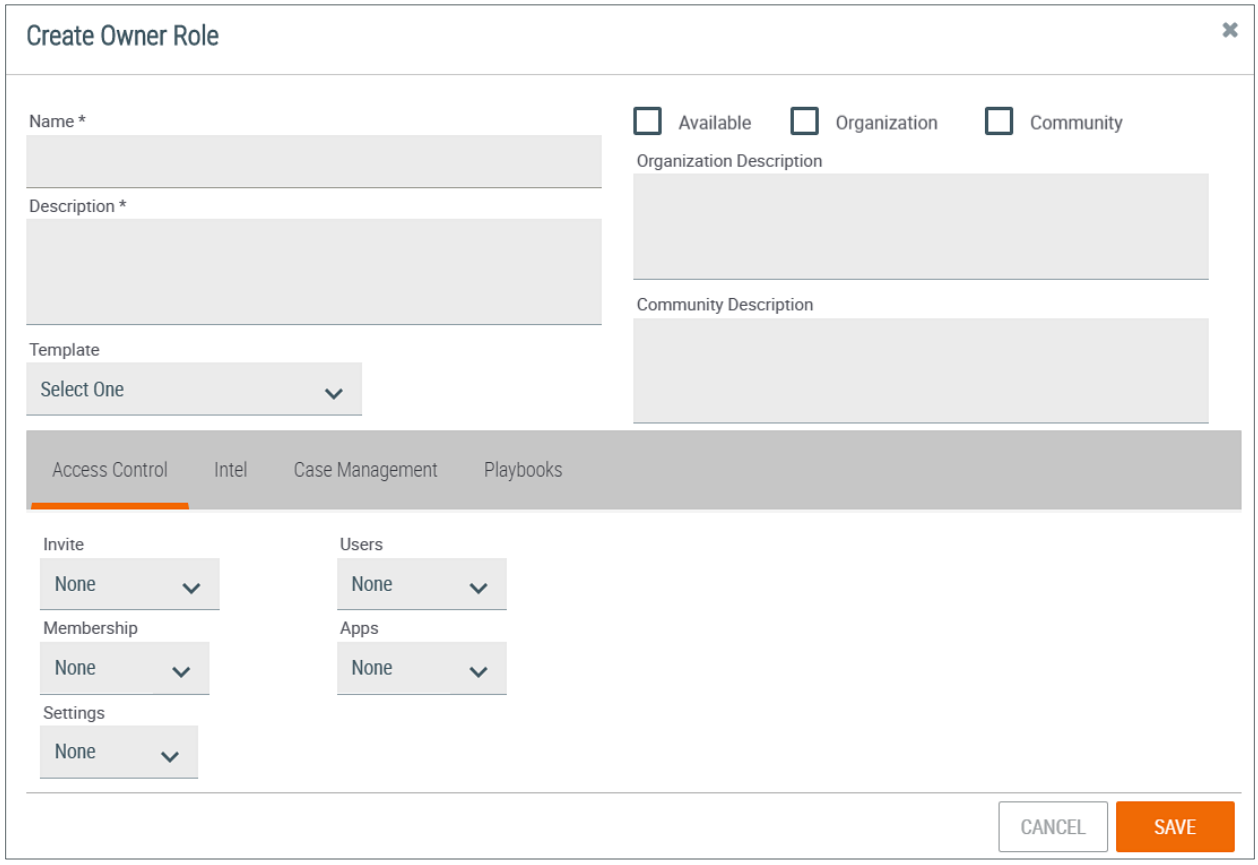

Figure 22

6. Click the **Available** checkbox to make the role available or unavailable in the System; click the **Organization** or **Community** checkbox to make the role available or unavailable in these two entities. A role can be simultaneously available in all three.
7. Click inside the **Name** and **Description** boxes to enter information as desired.
8. The **Access Control** permissions tab will be already selected. These parameters regulate the basic actions that users can take within their Organizations.

9. Click the **Intel** tab, and the **Intel** screen will appear (Figure 23). These parameters regulate the intel-data actions that users can take within their Organizations. When the **Allow Intel Access** checkbox is unchecked, all the permissions on the tab will be disabled and set to **None**. When checked, all the permissions on the tab will have a minimum value of **Read**, and the **None** option will be unavailable.

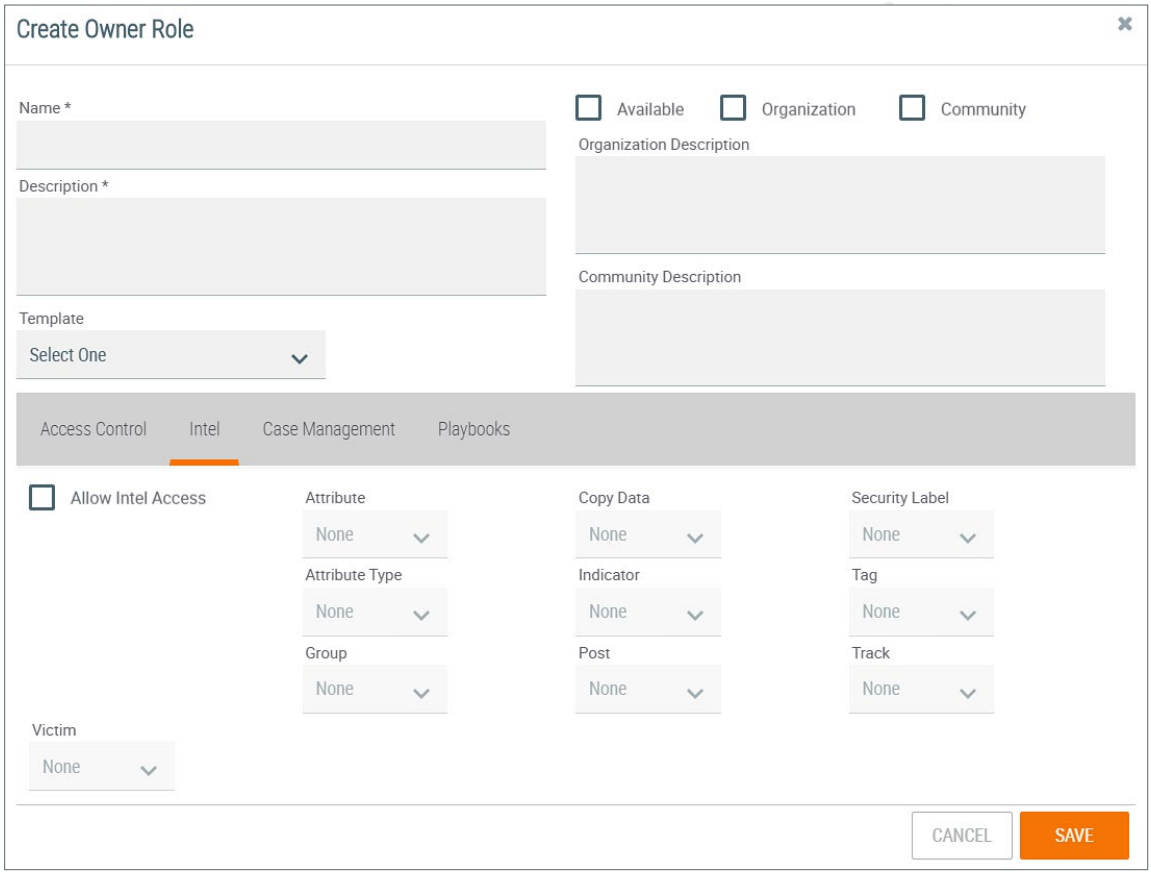

Figure 23

10. Click the **Case Management** tab and the **Case Management** screen will appear (Figure 24). These parameters regulate the case-management actions that users can take within their Organizations. When the **Allow CM Access** tab is unchecked, all the permissions on the tab will be disabled and set to **None**. When checked, all the permissions on the tab will have a minimum value of **Read**, and the **None** option will be unavailable. The checkbox and permissions on this tab will continue to be disabled when configuring a Community Role.

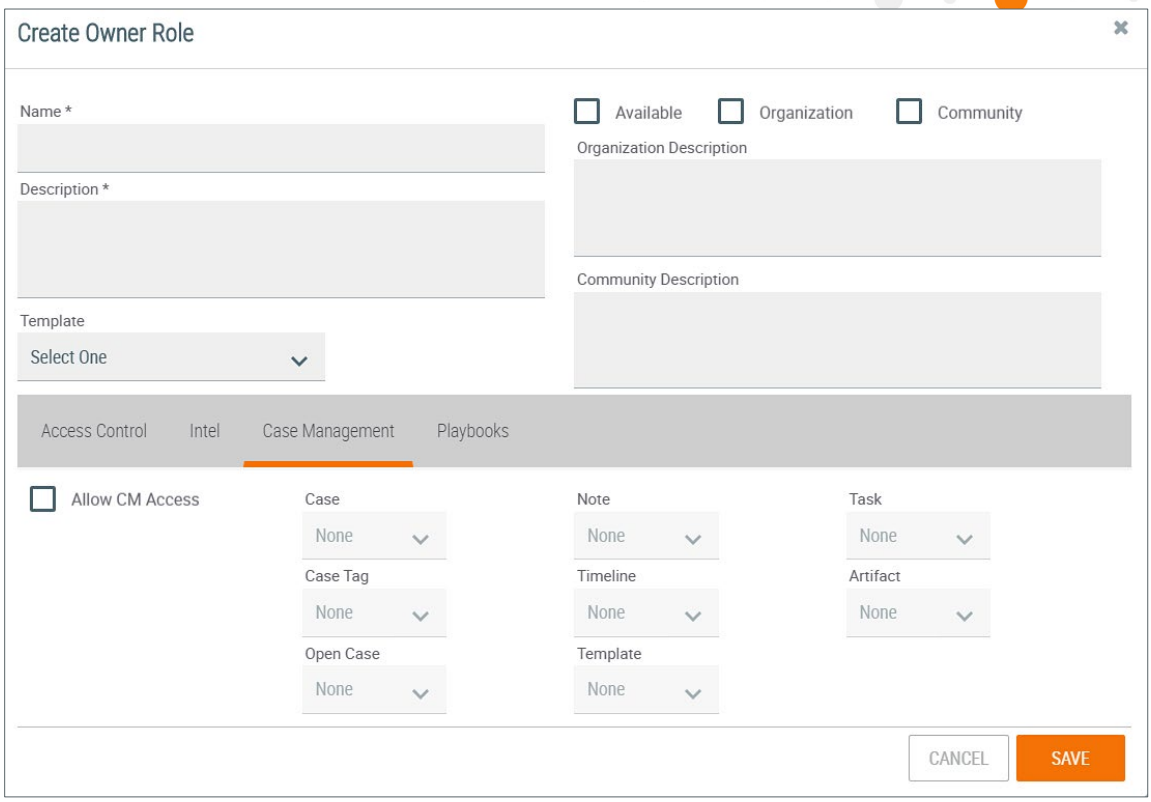

Figure 24

11. Click the **Playbooks** tab and the **Playbooks** screen will appear (Figure 25). These parameters regulate the Playbooks actions that users can take within their Organizations. An Administrator may specify Playbooks actions for a specific user. This is important because it restricts actions on a Playbook only to experienced or designated users.

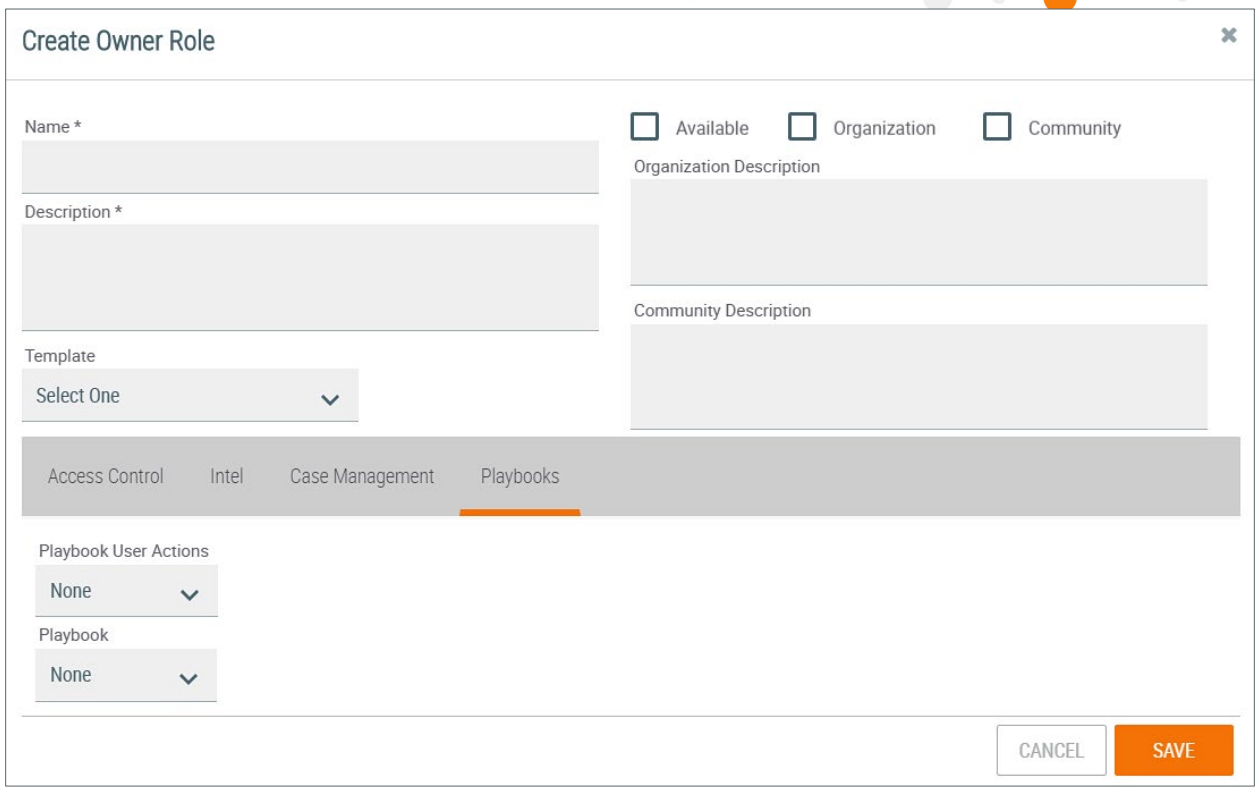

Figure 25

12. Click the **SAVE** button.

Editing Owner Roles

Follow these steps to edit the Owner Roles:

NOTE: Users may only edit the roles they have created and not those that come standard with the platform. The standard roles will have the *Delete* ***icon grayed out in the table, and users will only be allowed to make the role available or unavailable in the system by clicking the designated checkbox.***

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **Owner Roles** tab, and the **Owner Roles** screen will appear (Figure 21.)
5. Choose a role, and click the **Edit** icon in the **Options** column. (**Standard User** role is used in this example.). The **Edit Owner Role** pop-up screen will appear (Figure **26**).

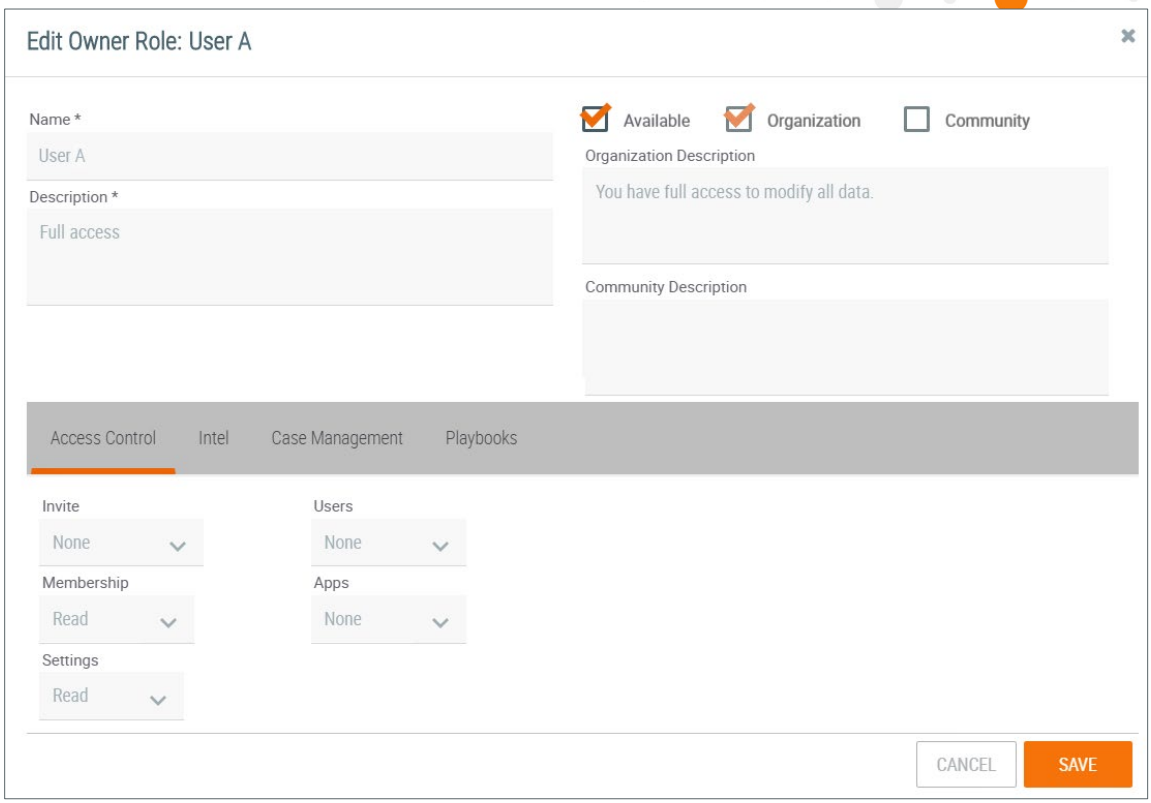

Figure 26

6. Select and enter the parameters and attributes per the instructions in the previous section.

   NOTE: The** Case Management **and** Playbooks **tabs will be grayed out (inaccessible) for roles that are available within a Community.

7. Click the **SAVE** button.

ThreatAssess

ThreatAssess is an important tool that appraises the value of an Indicator. This feature examines multiple data points to provide a single score, ranging from 0 to1000, on an Indicator's worth. This score is found on the Details pop-up screen and on the Details Overview screen of a given Indicator, and it is updated once every 24 hours. ThreatAssess is initially set up with general default parameters until these parameters are configured by the user.

Configuring ThreatAssess

Follow these steps to configure ThreatAssess:

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

4. Click the **ThreatAssess** tab, and the **ThreatAssess** screen will appear (Figure 27) displaying an **Overrides** table with the name of the data owner, Indicator metrics, and the assigned credibility criteria.

Figure 27

5. Click the **GENERAL CONFIG** button, and the **Default ThreatAssess Values** pop-up screen will appear (Figure 28).

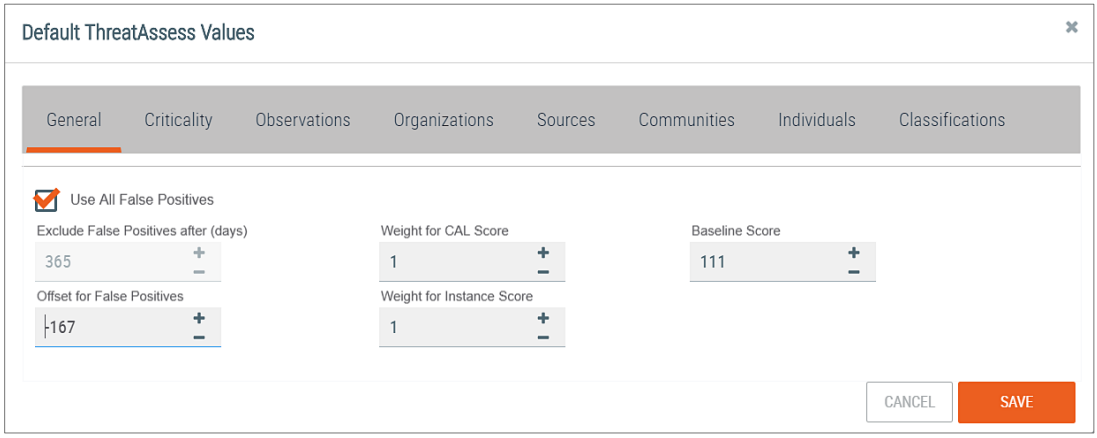

Figure 28

6. From the **General** tab, the number of days after which to exclude False Positives can be set, as well as the Offset for False Positives, the Weights for the CAL Score and the Instance Score, and the Baseline Score.
7. The **Criticality**, **Observations**, and **Classifications** tabs offer several parameters that can be set to configure these criteria.
8. The **Organizations**, **Sources**, **Communities**, and **Individuals** tabs allow for the configuration of the Credibility/Weight, Default Threat Rating, and Default Confidence Rating values. The **Sources** tab also feature an Exclude Sources checkbox, which allows the exclusion of Indicators from Sources in ThreatAssess calculations.
9. To configure the Credibility/Weight, Default Threat Rating, and Default Confidence Rating of an individual record, select the record from the table on the **ThreatAssess** screen (Figure 27) and click the Edit  icon. The **ThreatAssess Default Overrides** pop-up screen will appear (Figure 29).
10. Configure the values as desired, and then click the **SAVE** button.

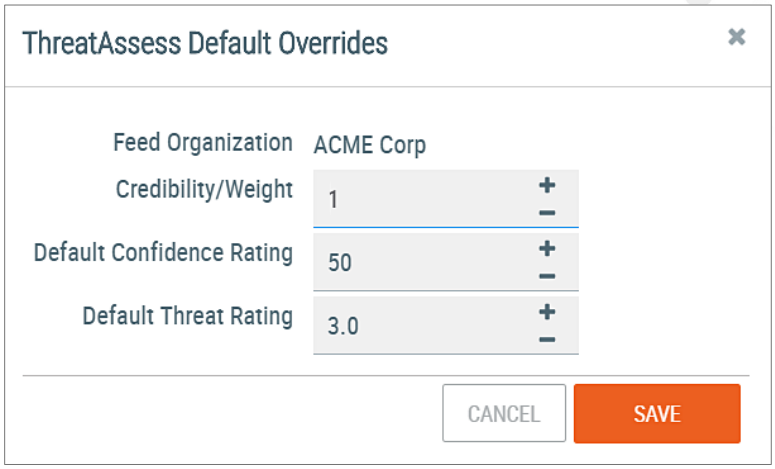

Figure 29

Analyzing an Indicator in Real Time

NOTE: This feature is only available to System Administrators.

Follow these steps to analyze the current overall rating for an Indicator:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **ThreatAssess** tab, and the **ThreatAssess** screen will appear (Figure 27).
5. Click the **ANALYZE INDICATORS** button, and the **ThreatAssess/Statistics** pop-up screen will appear (Figure 30).

Figure 30

6. Enter an Indicator in the **Indicator Name** box, and select an **Indicator Type** (Address Indicator in this example). The screen will now display the latest statistics for that Indicator (Figure 31).

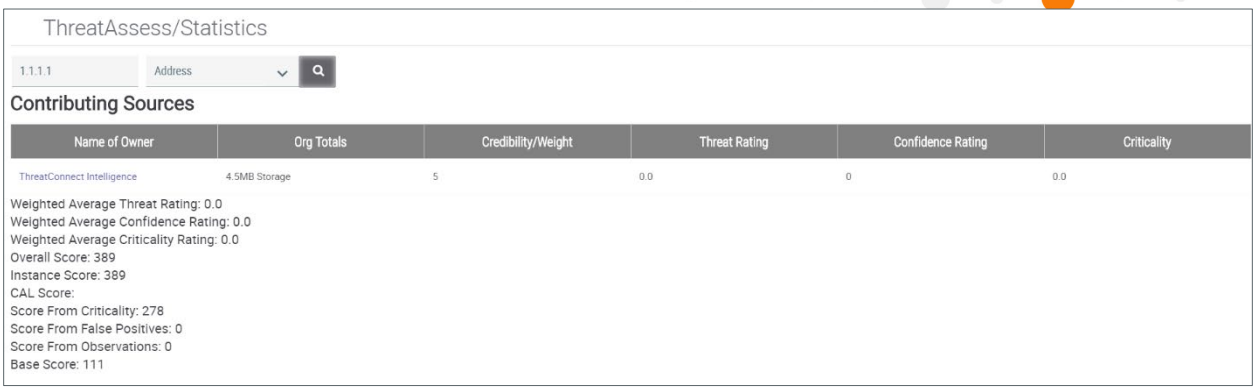

Figure 31

Viewing or Creating ThreatAssess Overrides

Follow these steps to review ThreatAssess overrides or to create a ThreatAssess override:

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).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 3).
4. Click the **ThreatAssess** tab, and the **ThreatAssess** screen will appear (Figure 27).
5. Click the **+ NEW** button, and the **Create ThreatAssess Overrides** pop-up screen will appear (Figure 32).

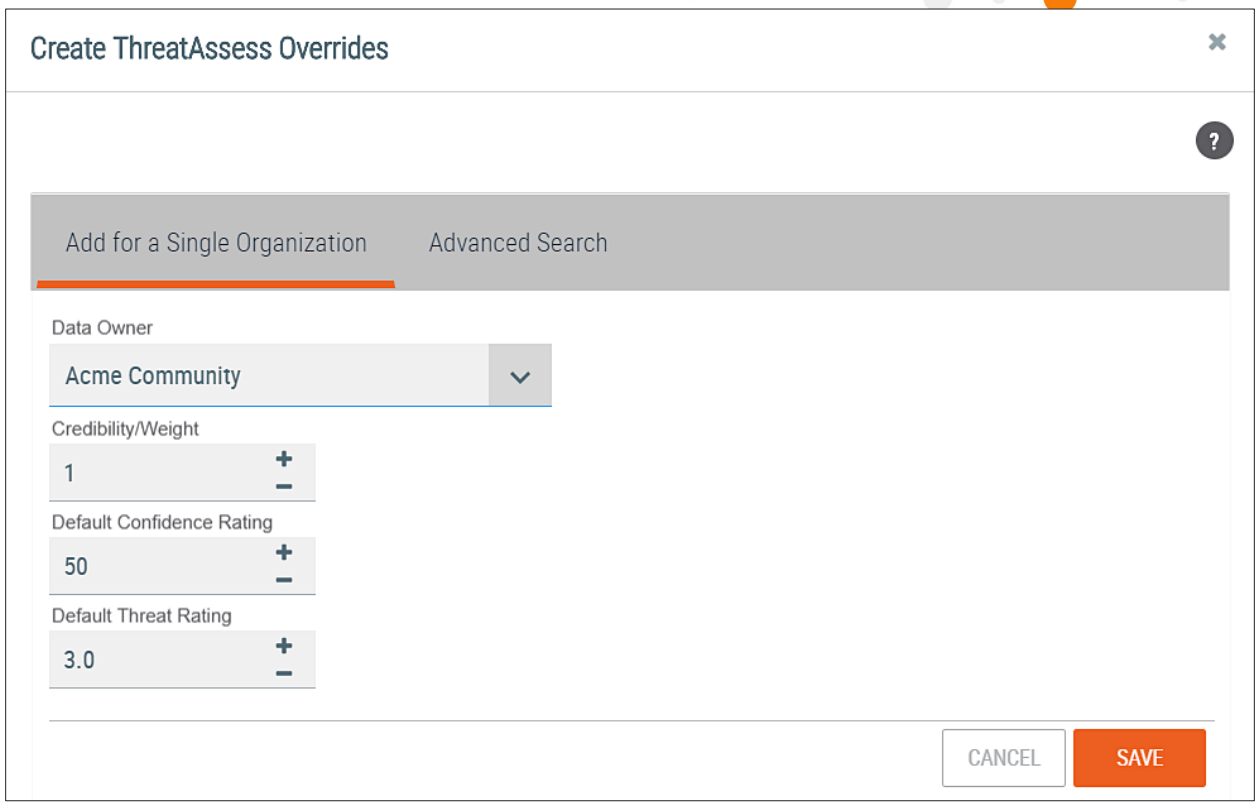

Figure 32

6. This screen allows the user to perform the following tasks:
   - Create a new ThreatAssess override for an existing Data Owner by modifying the parameters displayed on the **Add for a Single Organizations** tab and clicking the **SAVE** button.
   - Search for Data Owners that meet the desired criteria for feeds by clicking on the **Advanced Search** tab.