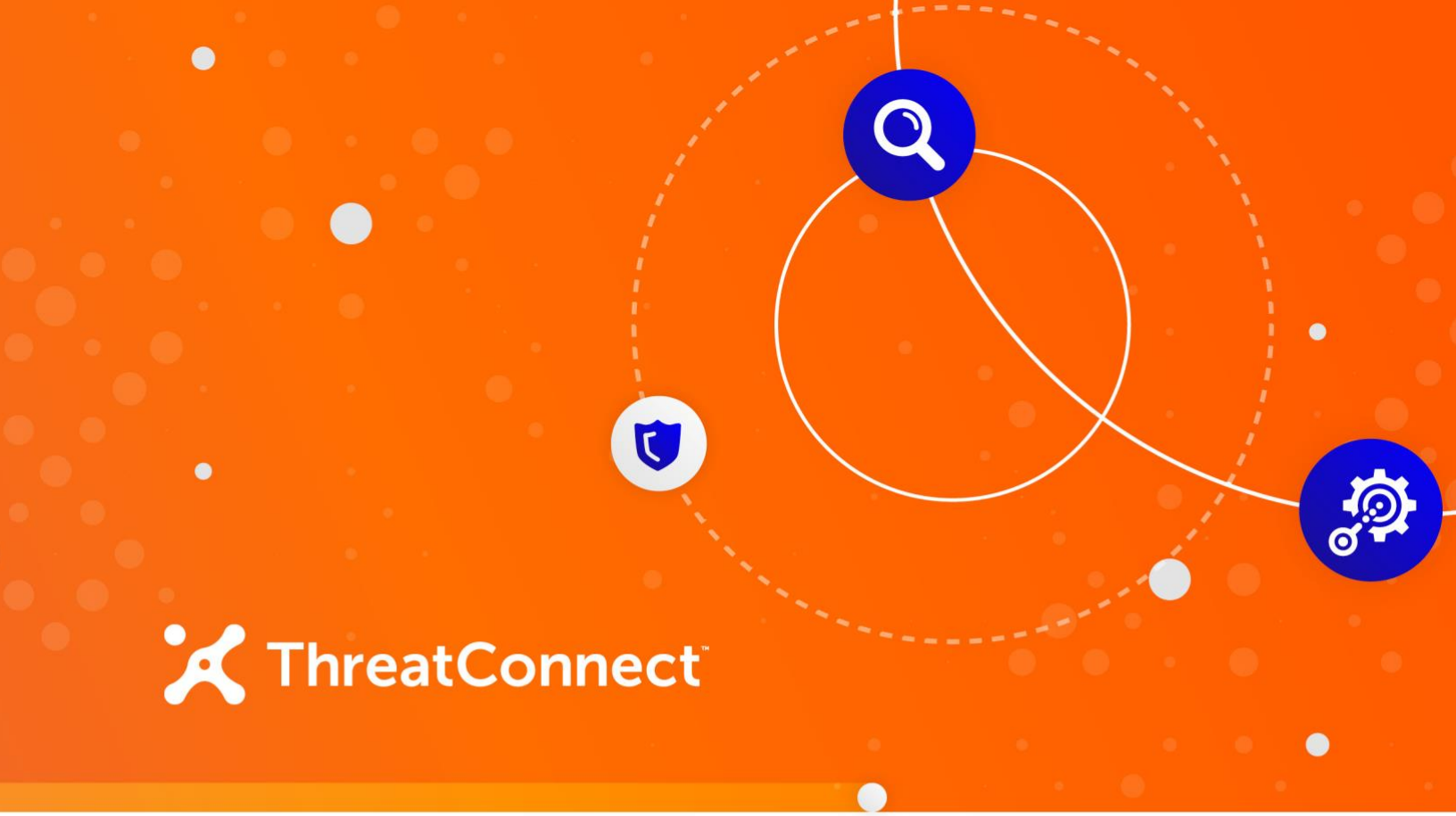

Account Administration

User Guide

Software Version 6.2

June 21, 2021

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

SYSTEM ADMINISTRATION 4

Getting Started 4
System Account Familiarization 4
Organization Management 5

Create an Organization 5

Configure an Organization Account 7

Add Additional Users to an Organization 11

Delete an Organization 12

Community Management 12

Create a Community 12

Edi a Community 14

Add Accounts to a Community 15

Delete a Community 16

Performing Other Community Administrative Tasks 16

Source Management 17

Creating a Source 17

Activity Logs 20

View Activity Logs 20

Logged-In Users 20

View Logged-In Users or Administrators 20

Owner Roles 21

View Owner Roles 21

Create a New Owner Role 22

Edit Owner Roles 25

ThreatAssess 26

Configure ThreatAssess 26

Configure ThreatAssess of an Individual Record 31

Analyze an Indicator in Real Time 32

View or Create ThreatAssess Overrides 32

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 be displayed (Figure 2).

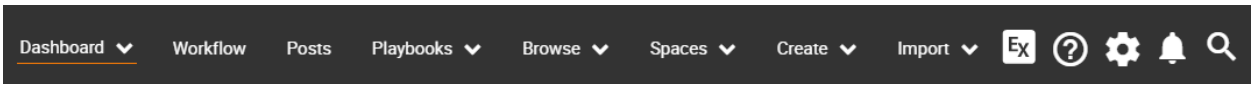

Figure 1

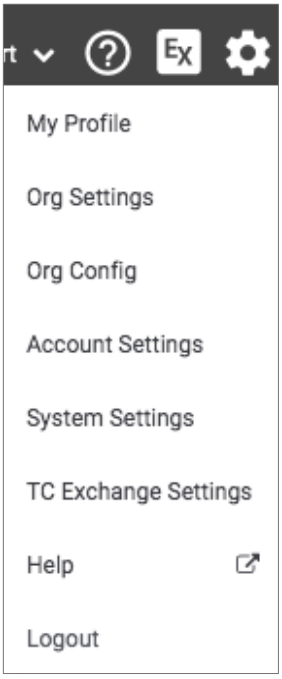

Figure 2

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 an 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 *ThreatConnect* System Administration User Guide.

Organization Management

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

Create 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 be displayed (Figure 2).

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

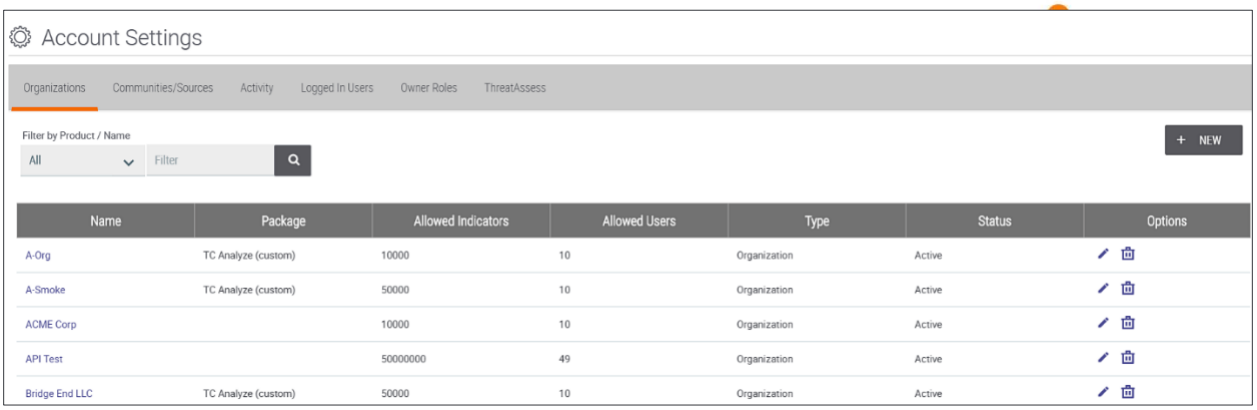

Figure 3

4. Click the **+ NEW** button, and the **Create Organization** window will be displayed (Figure 4).

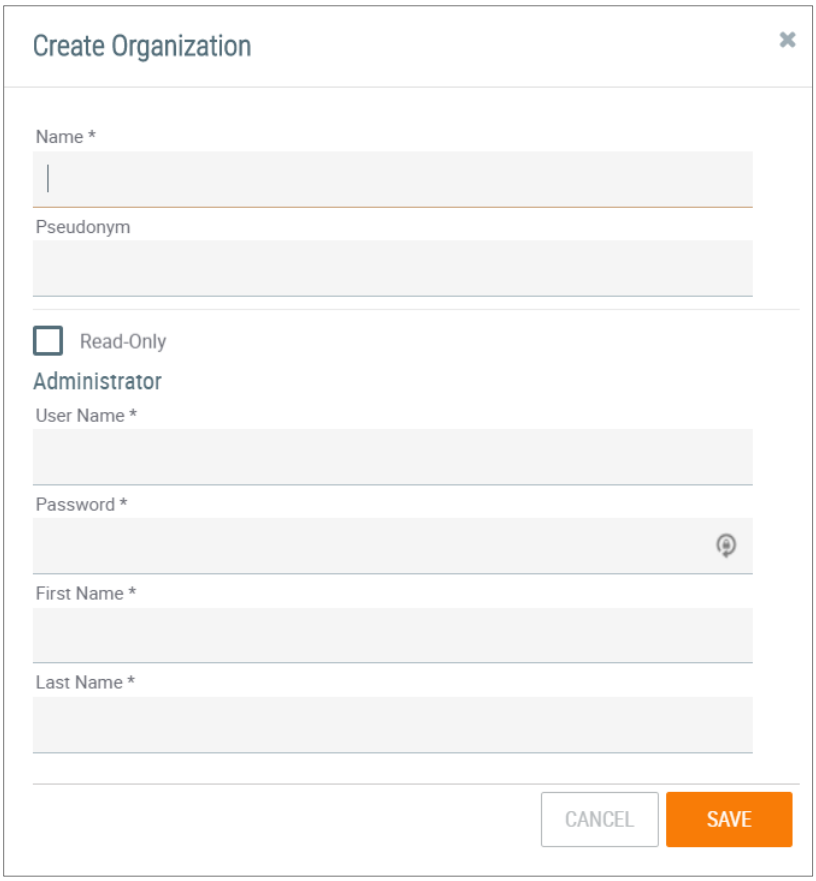

Figure 4

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. Select 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.

Configure 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.

1. Repeat Steps 1–3 in the "Create an Organization" section.

2. Click the **Edit** icon in the **Options** column of the Organization whose information is to be configured. The **Organization Information** window will be displayed (Figure 5) with the **Standard Options** tab underlined.

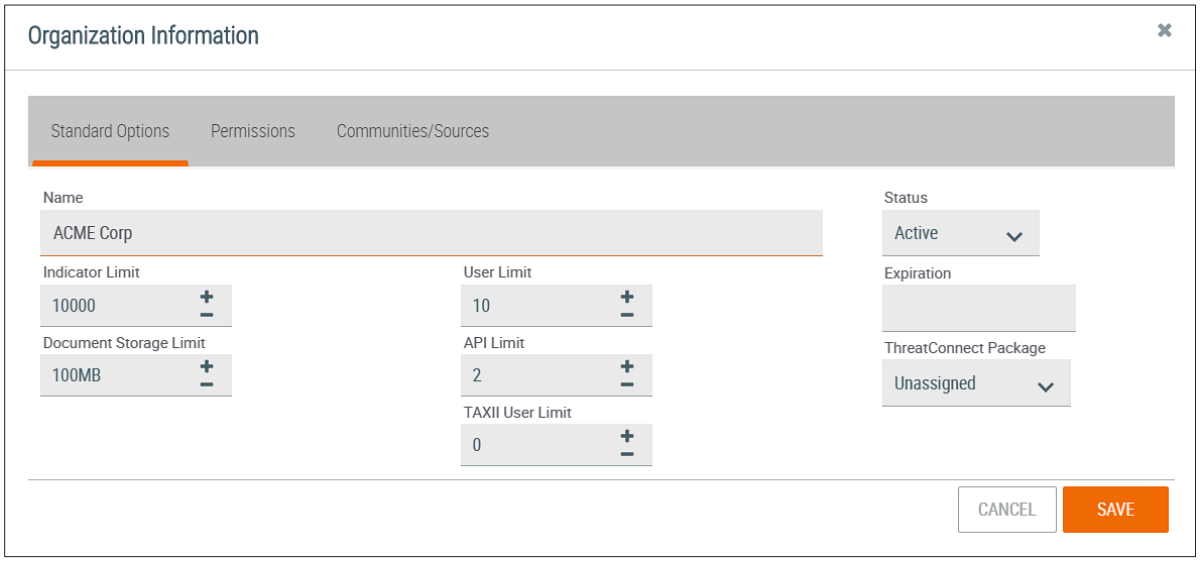

Figure 5

- **Name**: Enter an Organization account name.
- **Indicator Limit**: Enter Indicator Limits for the Organization, or use the plus and minus symbols to add or subtract increments of 1, respectively.

  NOTE: If the** Indicator Limit **is not configured, an Organization will not be able to create any internal Indicators.

- **Document Storage Limit**: Enter the amount of space an Organization has for storing documents, , or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **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.
- **API Limit**: Enter the number of API users that can exist within an Organization, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Taxii User Limit**: Enter the number of Taxii users that can exist within an Organization, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Status**: Select whether the status of the Organization is Active or Expired. An Organization with Expired status exists, but is not accessible.
- **Expiration**: Enter 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**.
- **ThreatConnect Package:** Select a ThreatConnect package. This selection will determine the options available under the Permissions tab.

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

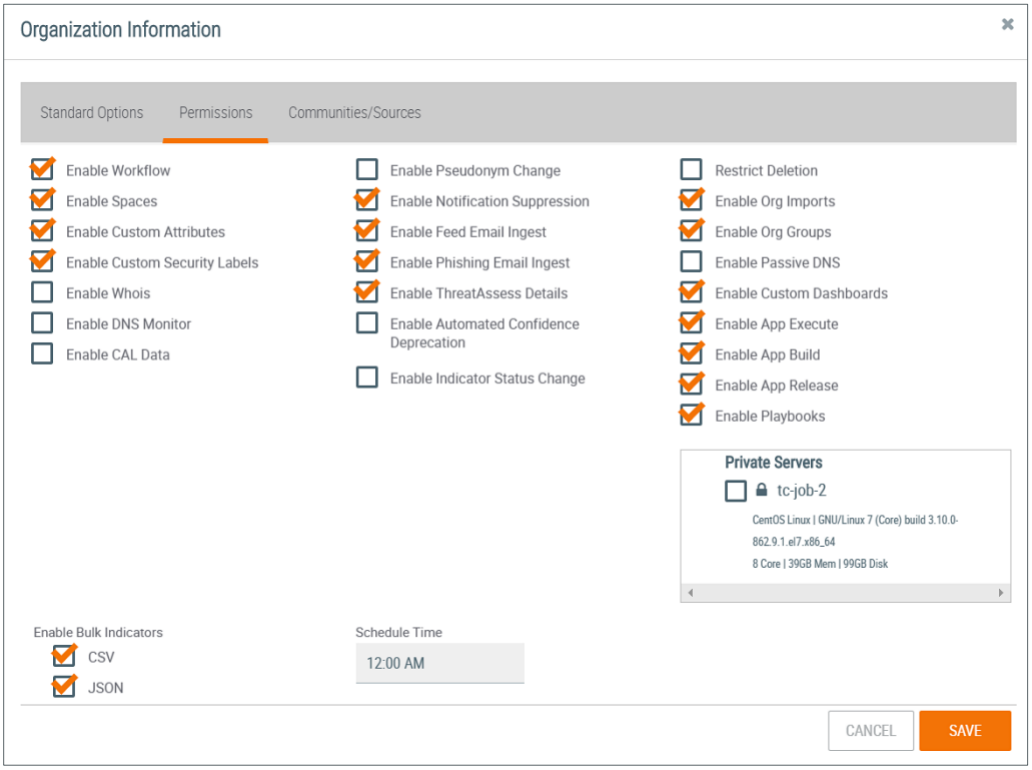

Figure 6

- **Enable Workflow**: Select the checkbox to enable the Workflow Tasks feature.
- **Enable Spaces**: Select the checkbox to enable the creation of Spaces.
- **Enable Custom Attributes**: Select the checkbox to enable the creation of custom Attribute Types.

- **Enable Custom Security Labels**: Select the checkbox to enable the creation of custom Security Labels.
- **Enable Whois**: Select the checkbox to enable the Whois feature.
- **Enable DNS Monitor**: Select the checkbox to enable the DNS Monitor feature.
- **Enable CAL Data**: Select the checkbox to enable the compilation of CAL Data.
- **Enable Pseudonym Change**: Select 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 cleared and will require the System Administrator to select it again if another pseudonym change is needed.***
- **Enable Notification Suppression**: Select 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.
- **Enable Feed Email Ingest**: Select the checkbox to allow the Feed Email Ingest feature for the Organization.
- **Enable Phishing Email Ingest**: Select the checkbox to allow the Phishing Email Ingest feature for the Organization.
- **Enable ThreatAssess Details**: Select the checkbox to enable the display of ThreatAssess details.
- **Enable Automated Confidence Deprecation**: Select the checkbox to enable the Confidence Deprecation feature.
- **Enable Indicator Status Change**: Select the checkbox to enable the ability to change an Indicator's status.
- **Restrict Deletion**: Select the checkbox to prevent users from deleting an Organization. Doing so will remove the **Delete** icon from the Organization name displayed in the table.
- **Enable Org Imports**: Select the checkbox to enable Organization Imports.
- **Enable Org Groups**: Select 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 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 dropdown 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.
- **Enable Passive DNS**: Select 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.
- **Enable Custom Dashboards**: Select the checkbox to enable the ability to create custom Dashboards.

- **Enable App Execute**: Select the checkbox to enable the ability to execute apps.
- **Enable App Build**: Select the checkbox to enable the ability to build apps.
- **Enable App Release**: Select the checkbox to enable the ability to release apps.
- **Enable Playbooks**: Select the checkbox to enable the Playbooks Apps feature.
- **Enable Bulk Indicators**: Select the **CSV** (Comma-Separated Values) or **JSON** (JavaScript® Object Notation) checkboxes to enable the Bulk Indicator Export feature.
- **Private Servers**: Select the checkbox to enable the Private Server feature.

4. 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.

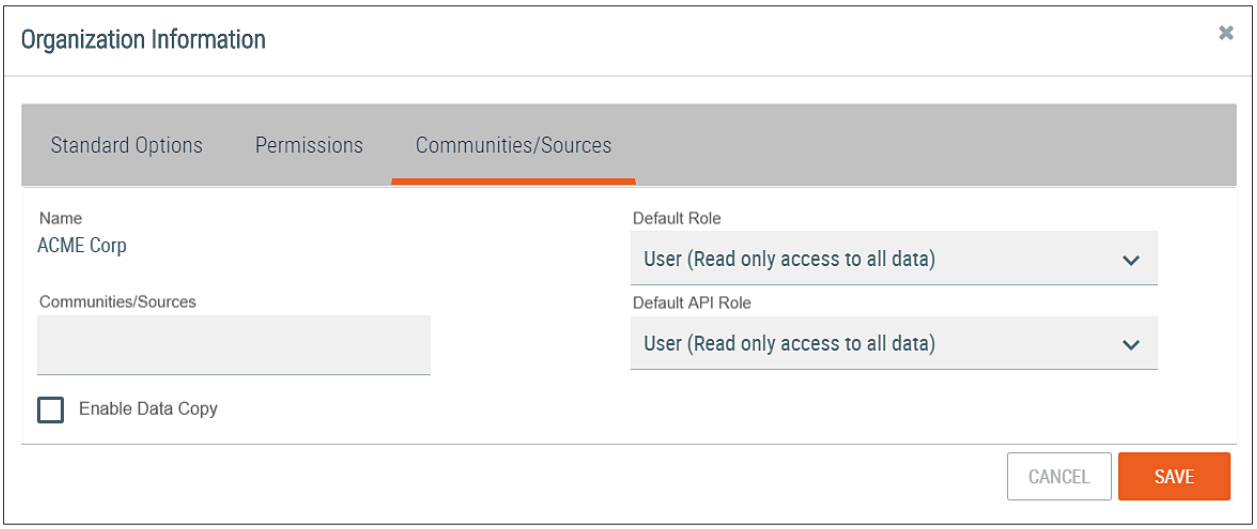

Figure 7

- **Communities/Sources**: Enter the name of a Community or Source for the Organization to join. As a name is typed, matching options will be displayed below the box. Select one or more options until all desired Communities and Sources are chosen.
- **Default Role**: 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.

- **Default API Role**: Select the Default Role all API accounts within the Organization will be given.
- **Allow Data Copy**: Select the checkbox to allow Community users to copy data from the Community to their private Organization.

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

Add 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. Repeat Steps 1–3 in the "Create an Organization" section.
2. Click on the hyperlinked Organization name in the **Name** column. The **Organization Settings** screen for the selected Organization will be displayed (Figure 8).

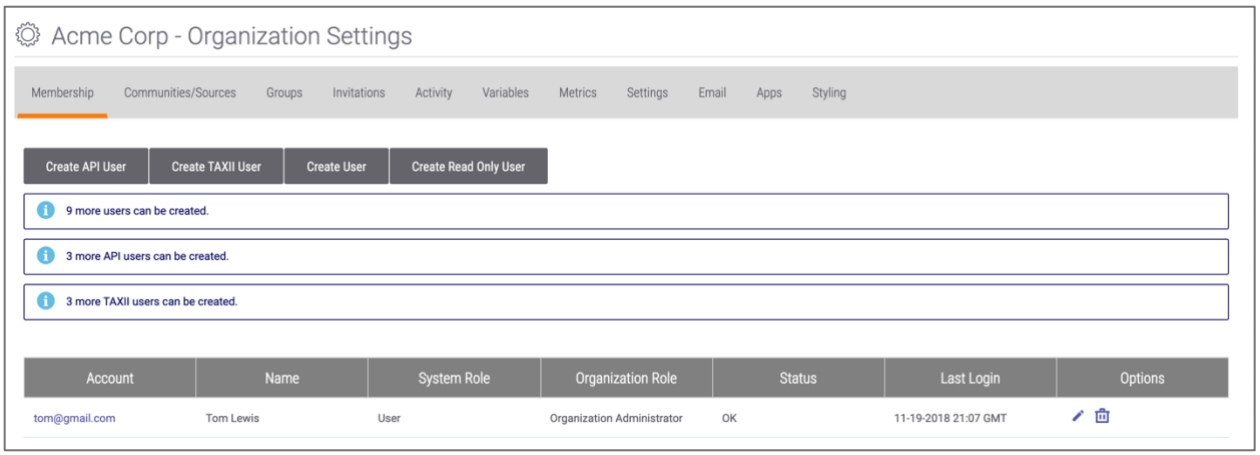

Figure 8

3. Click the **Create API User**, **Create TAXII User**, **Create User**, or **Create Read Only 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.

Delete an Organization

Follow these steps to delete an Organization:

1. Repeat Steps 1–3 in the "Create an Organization" section.
2. Click the **Delete** icon in the **Options** column of the Organization to be deleted.
3. The **Delete Organization** window will be displayed (Figure 9). Click the **YES** button to delete the account.

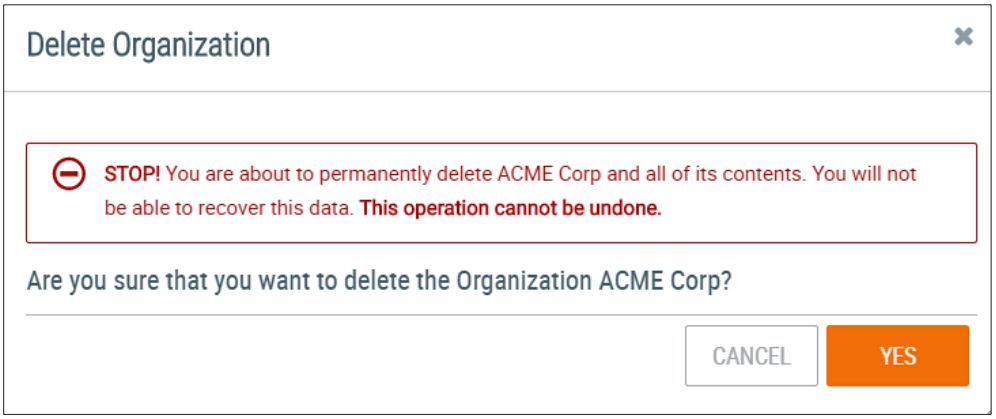

Figure 9

4. Click the **YES** button.

Community Management

Create 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 be displayed (Figure 2).
3. Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 3).
4. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will be displayed (Figure 10).

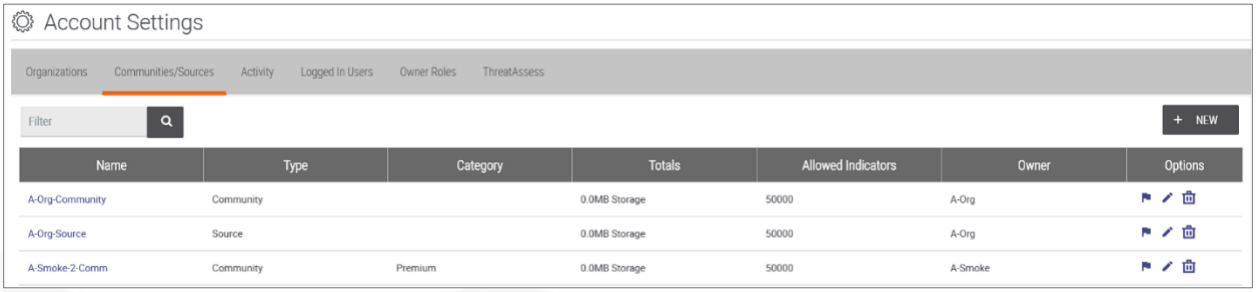

Figure 10

5. Click the **+ NEW** button, and the **Create Community/Source** window will be displayed 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.

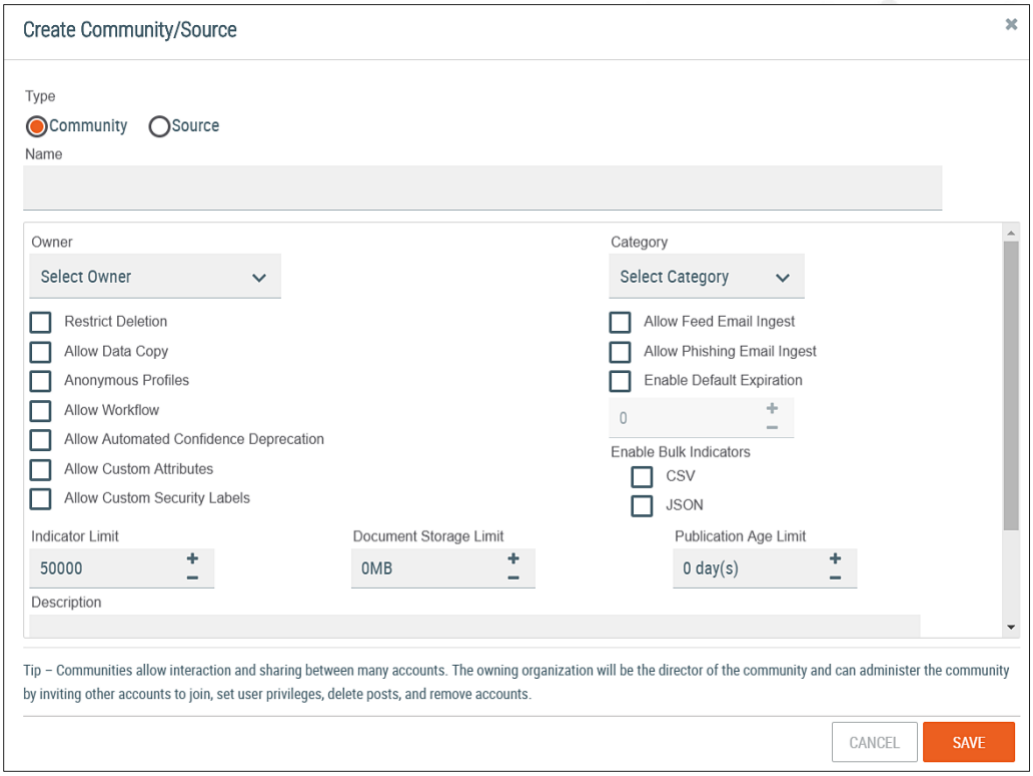

Figure 11

- **Name**: Enter the name of the Community.
- **Owner**: Select the Organization that will administer the Community and be given a Director role.
- **Category**: Select the type of Community to create.
- **Restrict Deletion**: Select the checkbox to prevent users from deleting a Community. Doing so will remove the **Delete** icon from the Community name displayed in the table.
- **Allow Data Copy**: Select the checkbox so that Community users are able to copy data from the Community to their private Organization.
- **Anonymous Profiles**: Select 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.
- **Allow Workflow**: Select the checkbox to enable Workflow Tasks for the Community's objects.

- **Allow Automated Confidence Deprecation**: Select the checkbox to create Deprecation Rules for the Community's Indicators.
- **Allow Custom Attributes**: Select the checkbox to allow the creation of custom Attribute Types.
- **Allow Custom Security Labels**: Select the checkbox to allow the creation of custom Security Labels.
- **Enable Feed Email Ingest**: Select the checkbox to allow the Feed Email Ingest feature for the Community.
- **Enable Phishing Email Ingest**: Select the checkbox to allow the Phishing Email Ingest feature for the Community.
- **Enable Default Expiration**: Select the checkbox to enable the setting of a date for when the Community will no longer be accessible within ThreatConnect.
- **Enable Bulk Indicators**: Select the **CSV** or **JSON** checkbox to enable the Bulk Indicator Export feature.
- **Indicator Limit**: Enter Indicator Limits for the Community, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Document Storage Limit**: Enter the amount of document storage space available to a Community, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Publication Age Limit**: Enter the number of days after which a publication created using the Publish feature within the Community will be aged off, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Description:** 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 Attribute Types 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.

Edi a Community

1. Repeat Steps 1–4 in the "Create a Community" section.
2. Click the **Edit** icon in the **Options** column of the selected Community, and the **Create Community/Source** window will be displayed (Figure 11).

3. Make the desired changes, and click the **SAVE** button.

Add Accounts to a Community

1. Repeat Steps 1–4 in the "Create a Community" section.
2. Click on the **Community Membership** icon in the **Options** column of the Community to which the accounts will be added to. The **Community/Source** Membership window will be displayed (Figure 12).

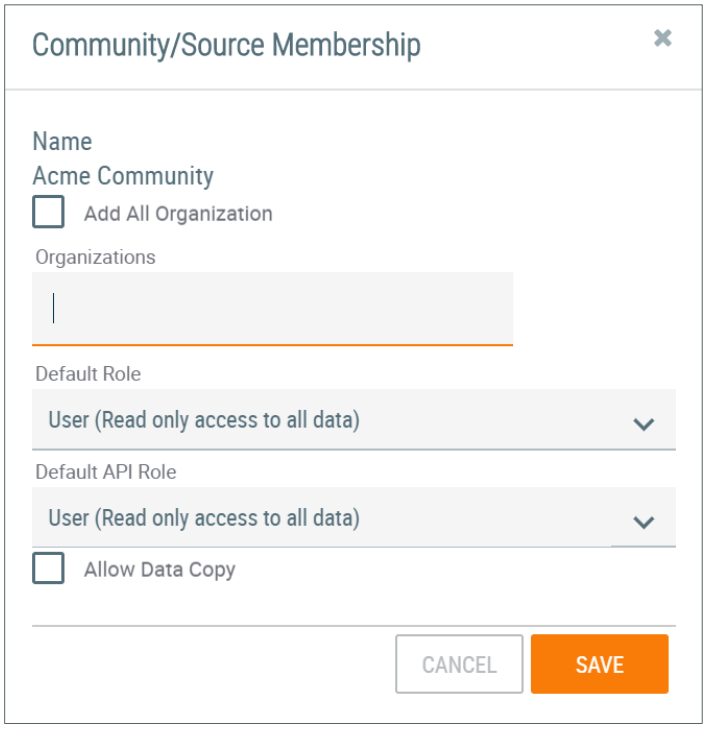

Figure 12

- **Add All Organizations**: Select the checkbox to add all Organizations to the Community.
- **Organizations**: Enter the name of an Organization to add to the Community. As a name is typed, matching options will be displayed below the box. Select one or more options until all Organizations that will participate in the Community are chosen.
- **Default Role**: Select the Default Role all the accounts within the Organization will be given in the Community.
- **Default API Role**: Select the Default Role all API accounts within the Organization will be given in the Community.
- **Allow Data Copy**: Select 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.*

3. Click the **SAVE** button to add the Organizations to the Community.

Delete a Community

1. Repeat Steps 1–4 in the "Create a Community" section.
2. Click on the **Delete** icon in the **Options** column of the Community to be deleted. The Delete Community window will be displayed (Figure 13).

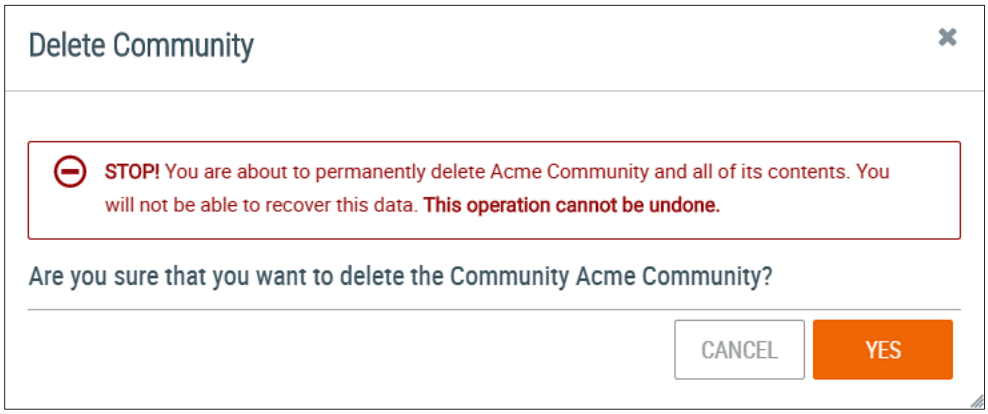

Figure 13

3. Click the **YES** button.

Performing Other Community Administrative Tasks

1. Repeat Steps 1–4 in the "Create a Community" section.
2. Click on the Community name, and the **Community Information** screen will be displayed (Figure 14).

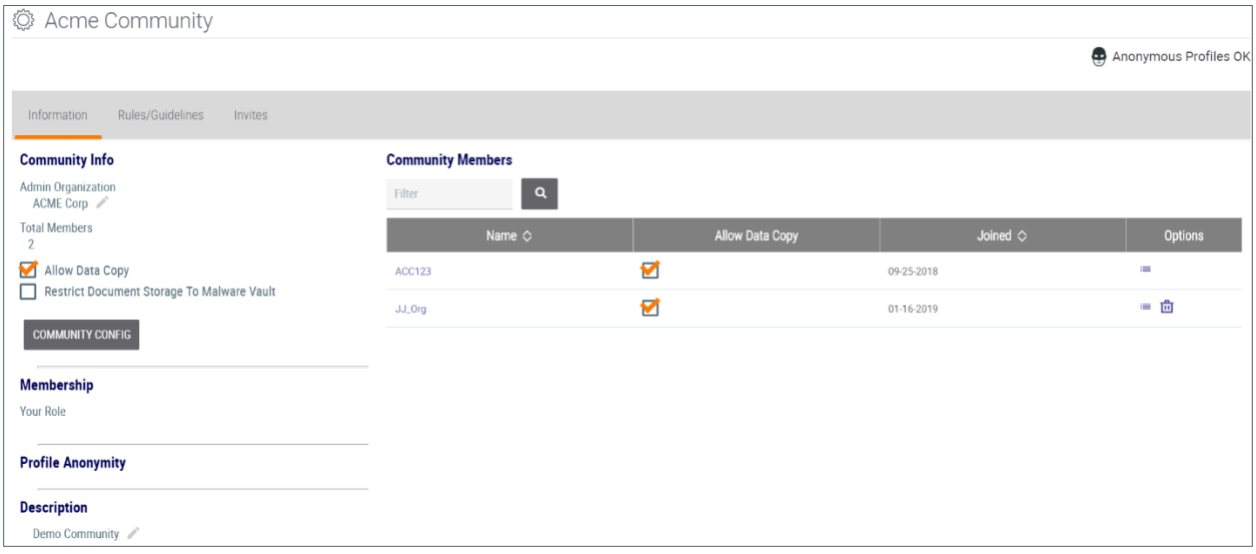

Figure 14

3. 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 be displayed(Figure 15).

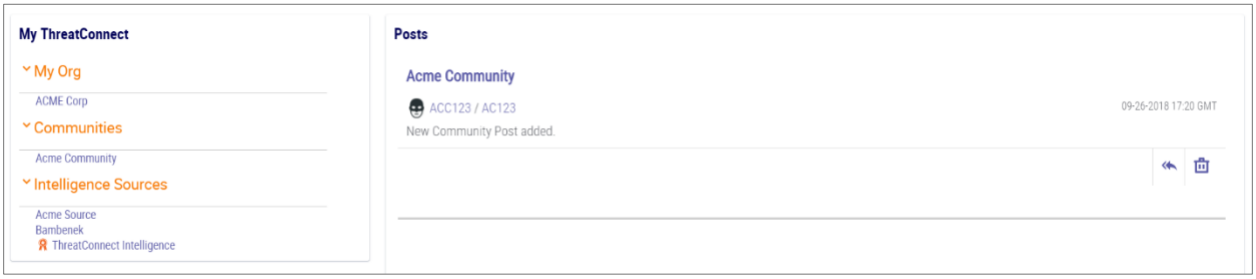

Figure 15

3. Click on the desired Community in the **My ThreatConnect** column, and its **Community Card** will be displayed at the upper-left corner of the screen (Figure 16).

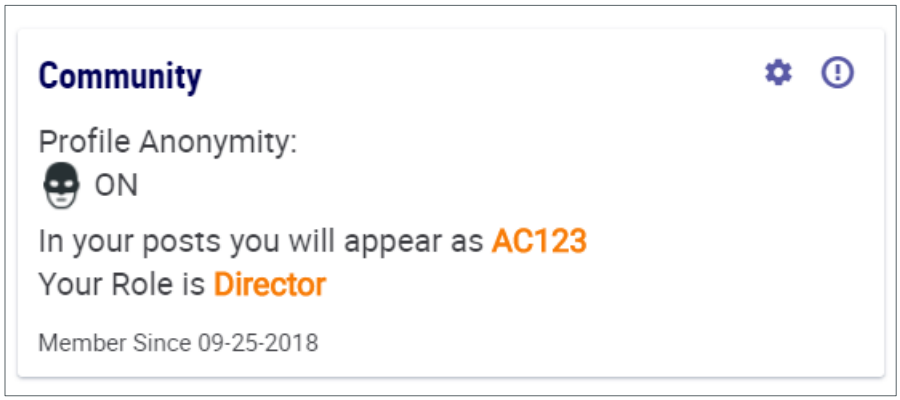

Figure 16

4. Click on the **Community Info** icon, and the **Community Info** screen will be displayed (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 be displayed 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 be displayed (Figure 2).
3. Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 3).
4. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will be displayed (Figure 10).
5. Click the **+ NEW** button, and the **Create Community/Source** window will be displayed 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.

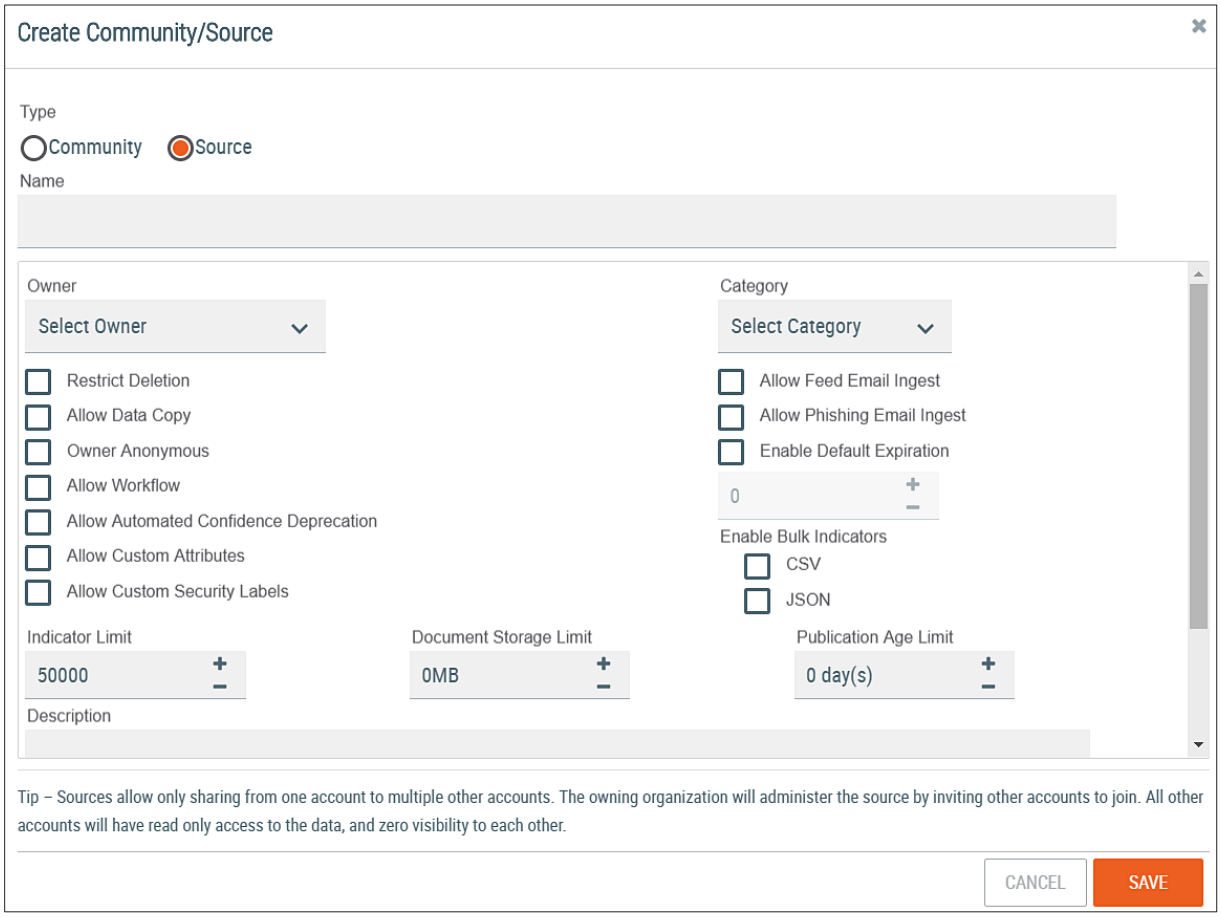

Figure 17

- **Name**: Enter the name of the Source.
- **Owner**: Select the Organization that will administer the Source.
- **Category**: Select the type of Source to create.
- **Restrict Deletion:** Select the checkbox to prevent users from deleting a Source. Doing so will remove the **Delete** icon from the Source name displayed in the table.
- **Allow Data Copy**: Select the checkbox to enable Source consumers to copy data from the Source to their private Organization.

- **Owner Anonymous**: Select the checkbox to allow Source consumers to see the identity of the Source owner.
- **Allow Workflow**: Select the checkbox to enable Workflow Tasks for the Source's objects.
- **Allow Automated Confidence Deprecation**: Select the checkbox to enable the Deprecation Rules feature for the Source's Indicators.
- **Allow Custom Attributes**: Select the checkbox to allow the creation of custom Attribute Types.
- **Allow Custom Security Labels**: Select the checkbox to allow the creation of custom Security Labels.
- **Allow Feed Email Ingest**: Select the checkbox to allow the Feed Email Ingest feature for the Source.
- **Allow Phishing Email Ingest**: Select the checkbox to allow the Phishing Email Ingest feature for the Source.
- **Enable Default Expiration**: Select the checkbox to enable the setting of a date for when the Source will no longer be accessible within ThreatConnect.
- **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 Attribute Types 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.***
- **Indicator Limit**: Enter Indicator Limits for the Community, or use the plus and minus symbols to add or subtract increments of 1, respectively.

  NOTE: If the Indicator Limit ***is not configured, a Source will not be able to create any Indicators within its Organization.***
- **Document Storage Limit**: Enter the amount of document storage space available to a Community, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Publication Age Limit**: Enter the number of days after which a publication created using the Publish feature within the Source will be aged off, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Description:** Enter a 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

View Activity Logs

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

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 be displayed (Figure 2).
3. Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 3).
4. Click the **Activity** tab, and the **Activity** screen will be displayed (Figure 18).

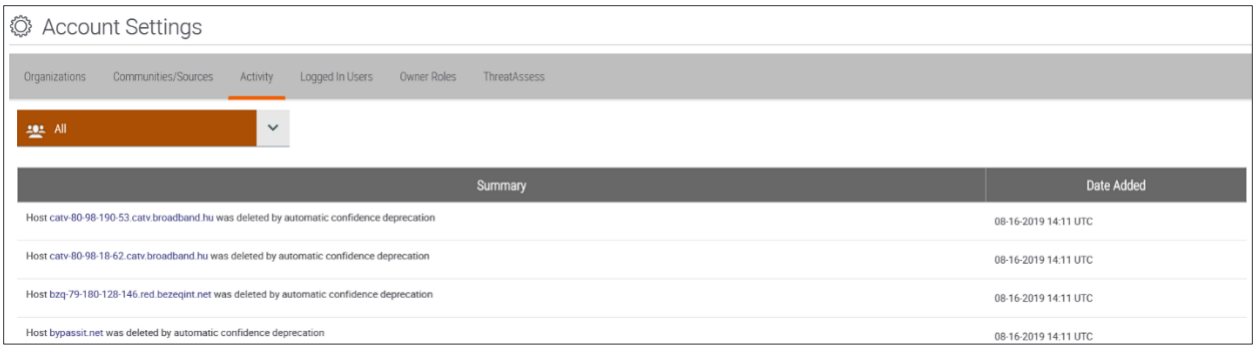

Figure 18

5. Use the **Filter** dropdown menu above the **Summary** column (with a default value of **ALL**) to select the activities of interest (Figure 19).

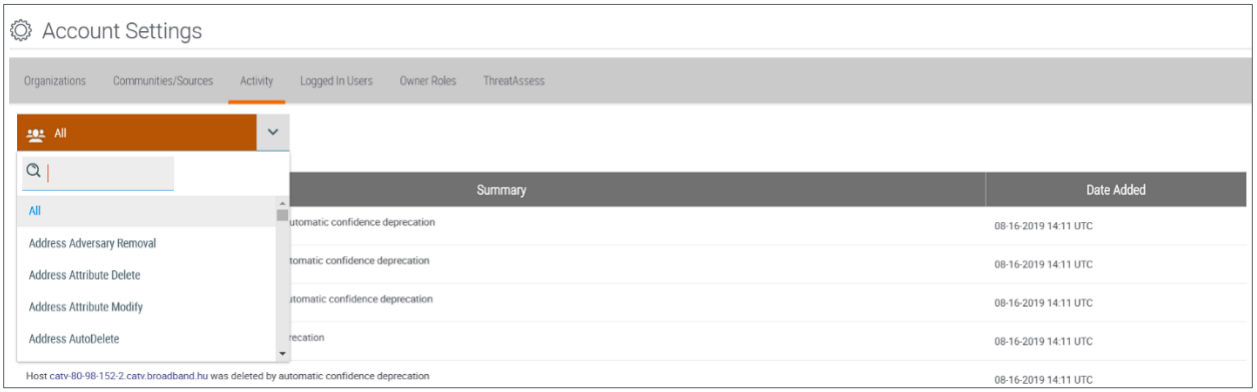

Figure 19

Logged-In Users

View Logged-In Users or Administrators

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 be displayed(Figure 2).
3. Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 3).Click the **Logged In Users** tab, and the **Logged In Users** screen will be displayed (Figure 20), displaying a table with the User Name, Organization, and IP Address from which the account is logged in.

Figure 20

Owner Roles

View Owner Roles

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 be displayed (Figure 2).
3. Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 3).
4. Click the **Owner Roles** tab, and the **Owner Roles** screen will be displayed (Figure 21). This screen displays a list of all available roles and a description of their function within an Organization or Community and as carried out by an Administrator.

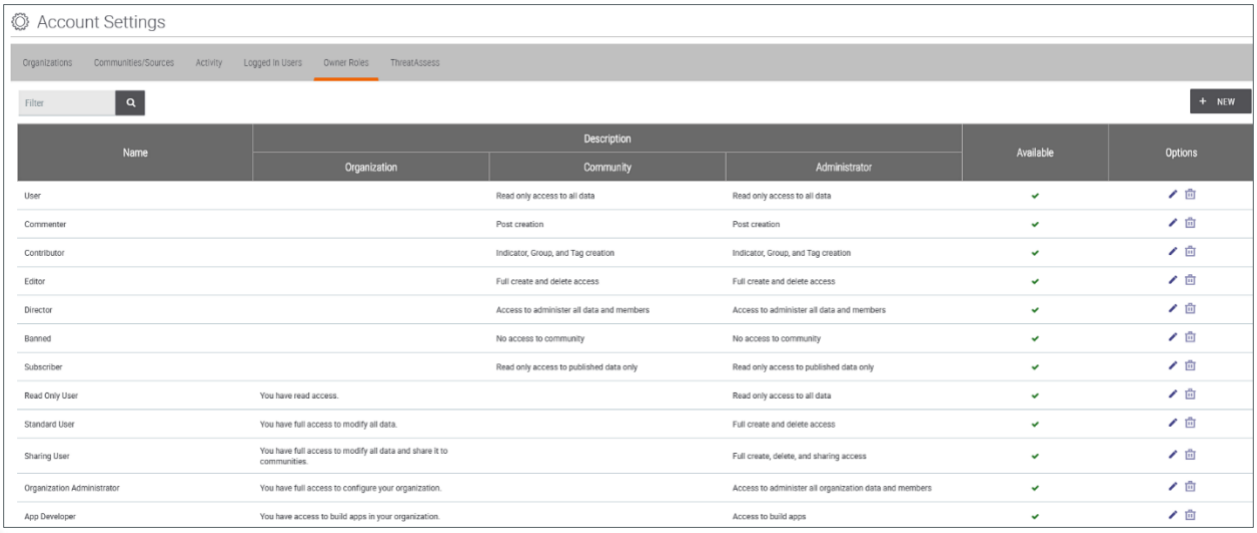

Figure 21

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

Create a New Owner Role

1. Repeat Steps 1–4 in the "View Owner Roles" section.
2. Click the **+ NEW** button, and the **Create Owner Role** window will be displayed (Figure 22).

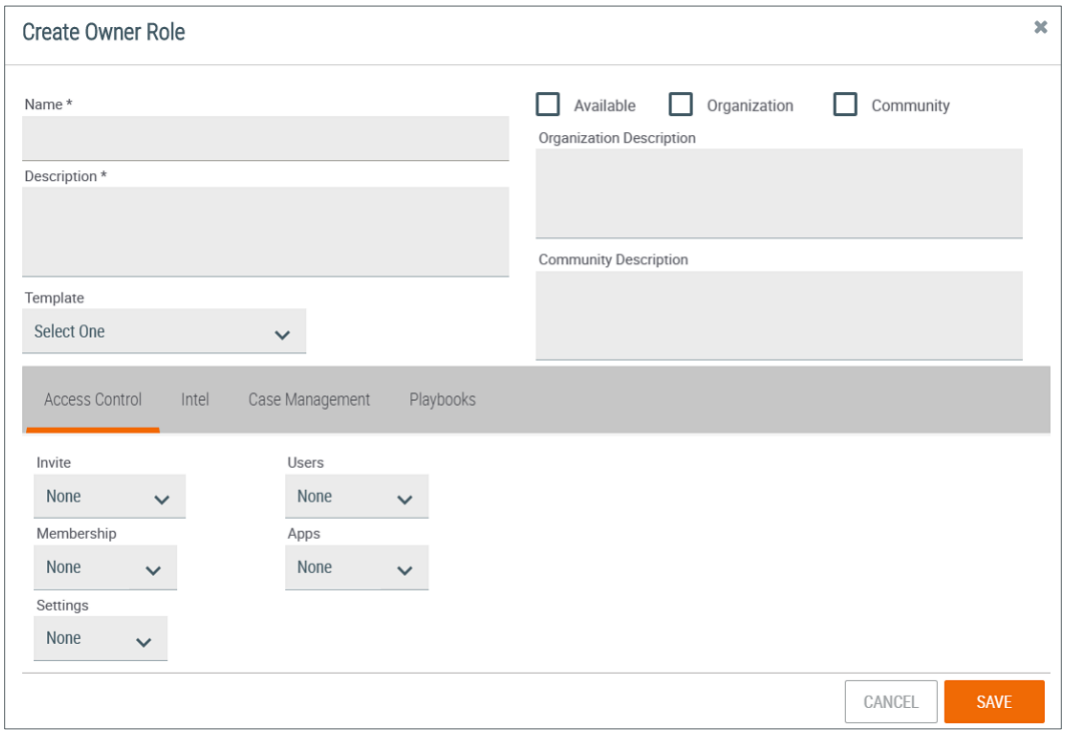

Figure 22

- **Name**: Enter a name for the Owner role.
- **Description**: Enter a description for the Owner role.
- **Available**: Select the checkbox to make the role available in the System.
- **Organization**: Select the checkbox to make the role available in the Organization.
- **Community**: Select the checkbox to make the role available in the Community.

NOTE: A role can be simultaneously available in all three.

3. The **Access Control** permissions tab will be already selected. These parameters regulate the basic actions that users can take within their Organizations.

4. Click the **Intel** tab, and the **Intel** screen will be displayed (Figure 23). These parameters regulate the intel-data actions that users can take within their Organizations.

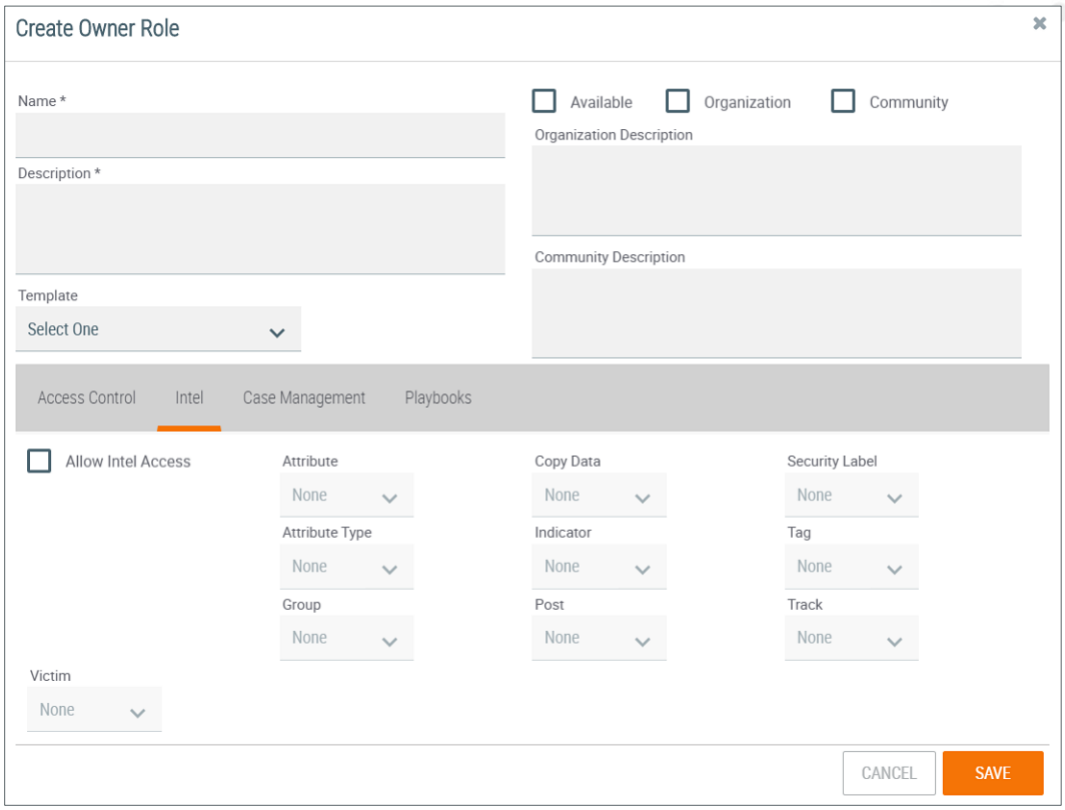

Figure 23

- **Allow Intel Access**: Select this checkbox to customize the permissions displayed on the **Intel** tab. When this checkbox is selected, all permissions will automatically be set to a minimum value of **Read**.

5. Click the **Case Management** tab, and the **Case Management** screen will be displayed (Figure 24). These parameters regulate the case-management actions that users can take within their Organizations. The checkbox and permissions on this tab will continue to be disabled when configuring a Community Role.

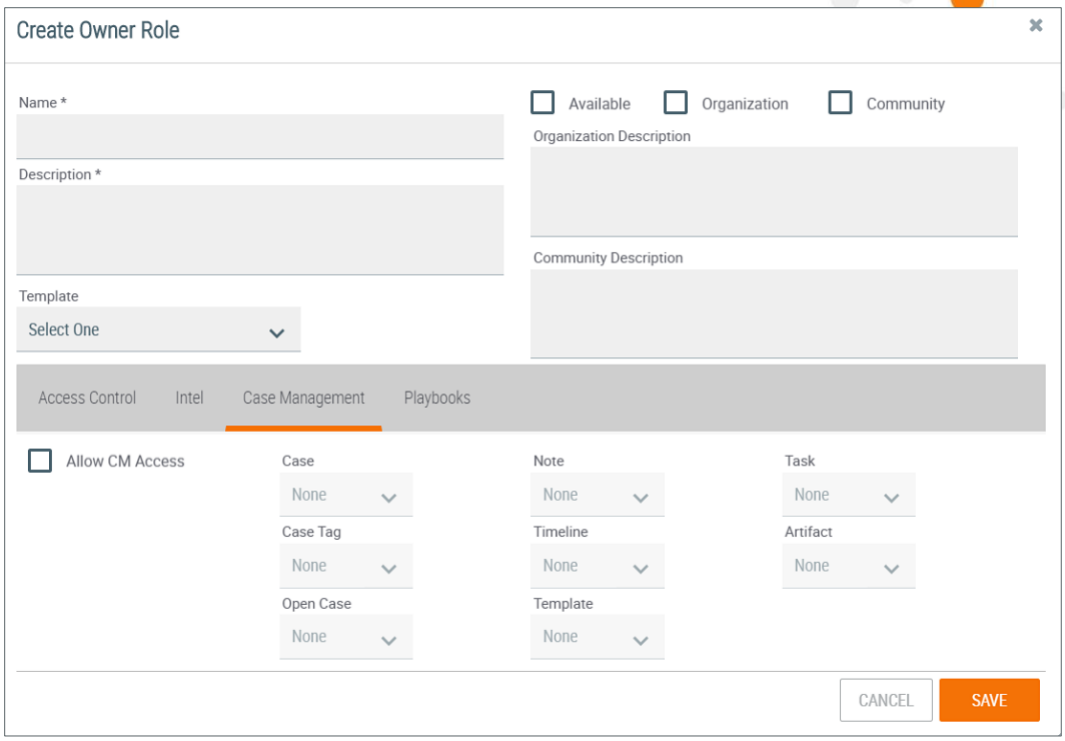

Figure 24

- **Allow CM Access**: Select this checkbox to customize the permissions displayed on the **Case Management** tab. When this checkbox is selected, all permissions will automatically be set to a minimum value of **Read**, and the **None** option will be unavailable.

6. Click the **Playbooks** tab and the **Playbooks** screen will be displayed (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.

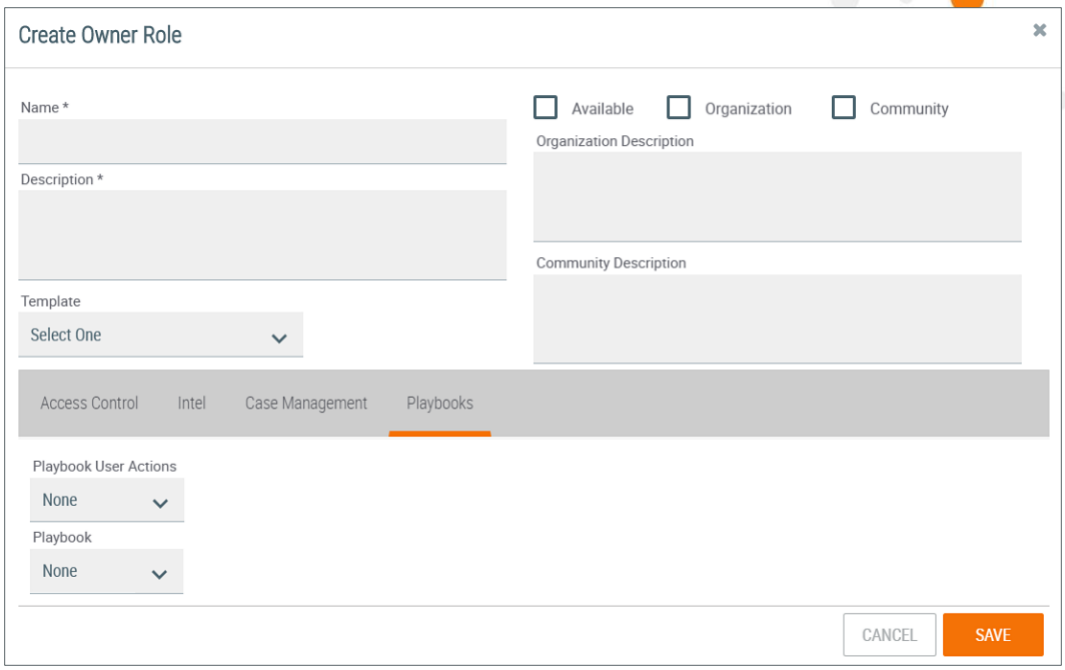

Figure 25

7. Click the **SAVE** button.

Edit 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. Repeat Steps 1–4 in the "View Owner Roles" section.

2. Choose a role, and click the **Edit** icon in the **Options** column. The **Edit Owner Role** window will be displayed (Figure 26).

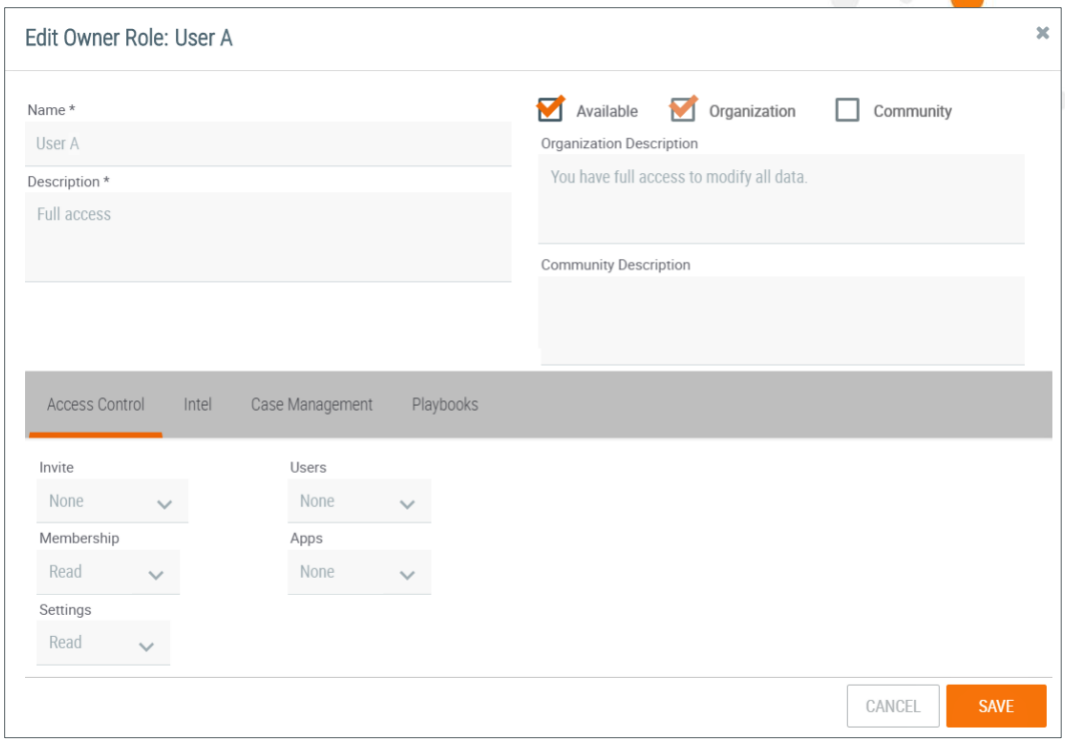

Figure 26

3. Configure the Owner role as described in the "Create a New Owner Role" section.

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

4. Click the **SAVE** button.

ThreatAssess

ThreatAssess gives a basic risk assessment of an Indicator through a single, actionable score. The score, which is found on the Details window and on the **Details** screen for an Indicator, represents the overall potential impact that an Indicator might have to a security organization. It also provides a breakdown of those factors that went into the calculation of that score, all of which come from data from within the user's ThreatConnect instance.

ThreatAssess is initially set up with general default parameters until these parameters are configured by the user.

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 be displayed (Figure 2).
3. Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 3).
4. Click the **ThreatAssess** tab, and the **ThreatAssess** screen will be displayed (Figure 27). This

screen displays a **ThreatAssess Default Organization 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** window will be displayed with the **General** tab selected (Figure 28). 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.

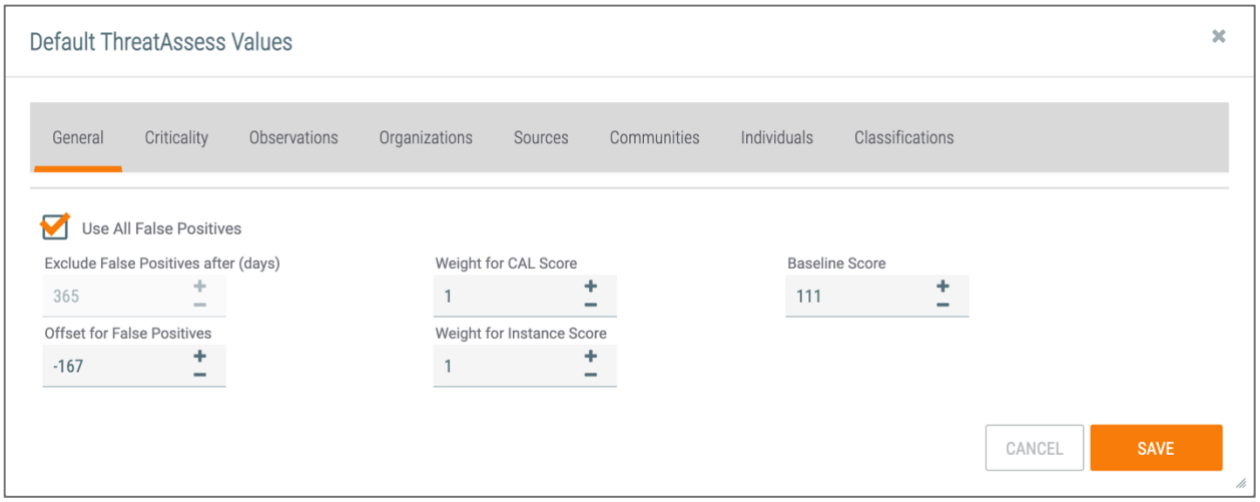

Figure 28

6. Select the **Criticality** tab (Figure 29Figure 30) to configure the **Criticality Base Coefficient**, **Criticality Linear Coefficient**, **Criticality Quadratic Coefficient**, **Minimum Score Contribution from Criticality**, and **Maximum Score Contribution from Criticality** parameters. Enter the values manually, or use the plus and minus symbols to add or subtract increments of 1, respectively.

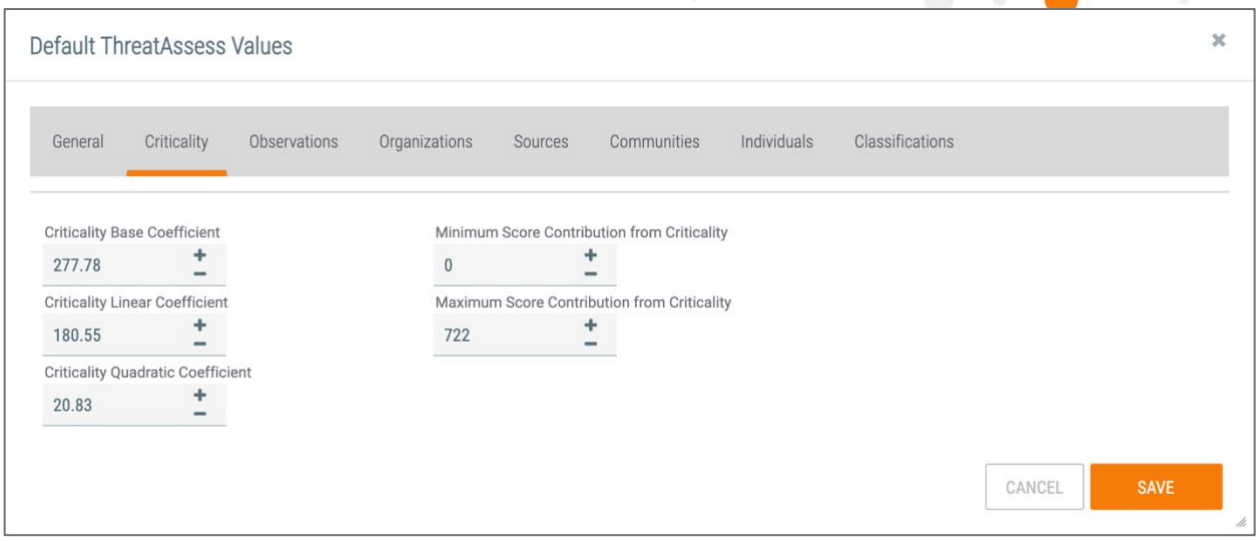

Figure 29

7. Select the **Observations** tab (Figure 30) to configure the **Exclude Observations after (days)**, **Base Coefficient for Observation Points**, **Linear Coefficient for Observation Points**, **Minimum Score Contribution from Observations**, and **Maximum Score Contribution from Observations** parameters. Enter the values manually, or use the plus and minus symbols to add or subtract increments of 1, respectively.

Figure 30

8. Select the **Organizations** tab (Figure 31) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** for Organizations. Enter the values manually, or use the plus and minus symbols to add or subtract increments of 1, respectively.

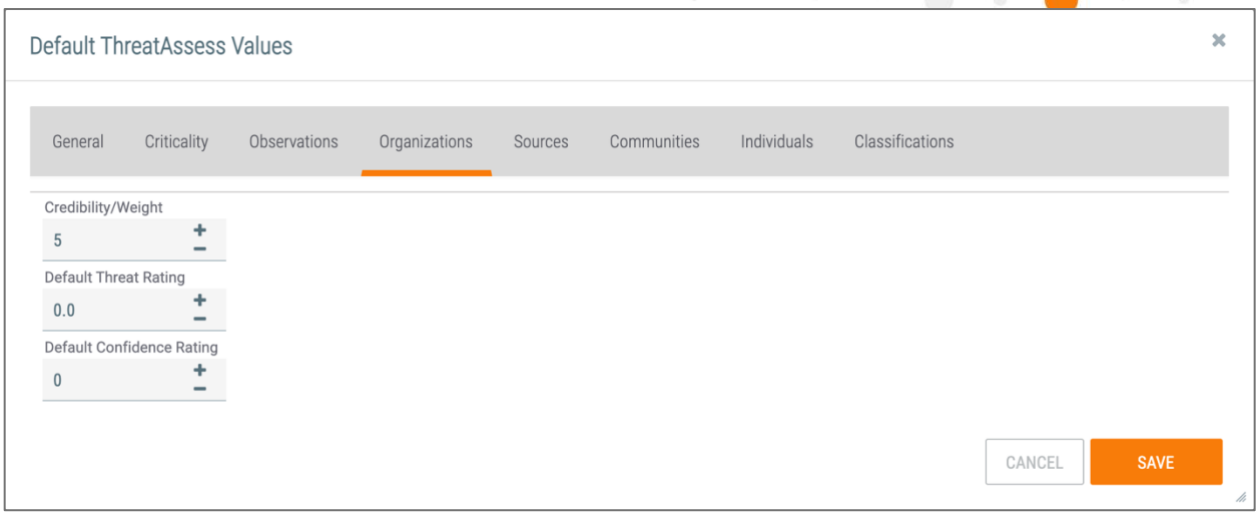

Figure 31

9. Select the **Sources** tab (Figure 32) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** for Sources. Enter the values manually, or use the plus and minus symbols to add or subtract increments of 1, respectively. To exclude Indicators from Sources in ThreatAssess calculations, select the **Exclude Sources** checkbox.

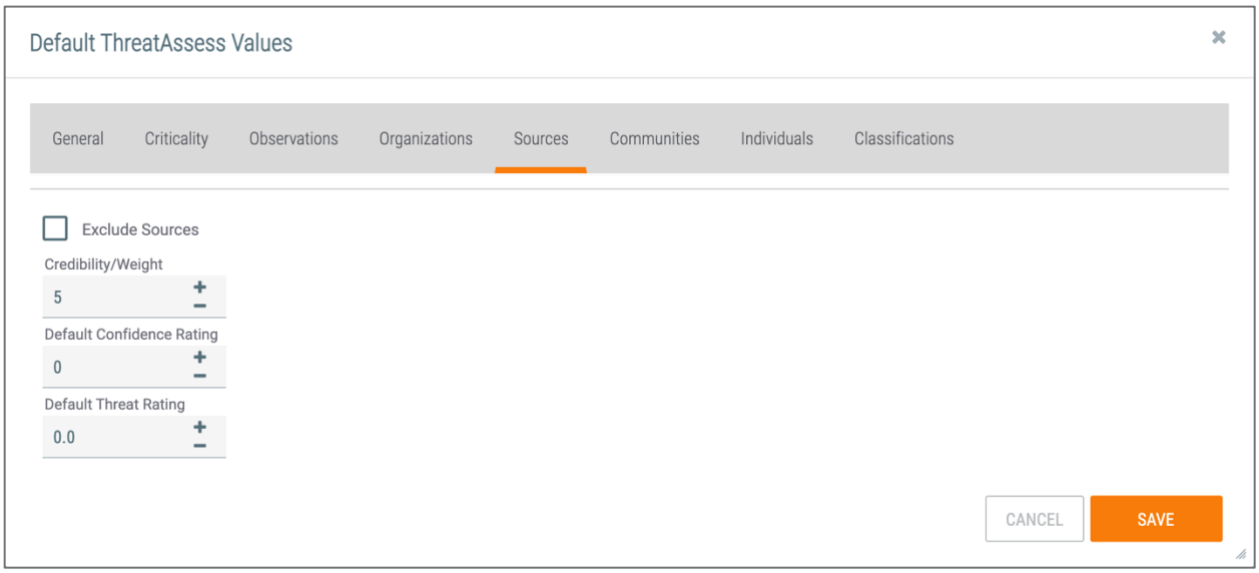

Figure 32

10. Select the **Communities** tab (Figure 33) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** for Communities. Enter the values manually, or use the plus and minus symbols to add or subtract increments of 1, respectively.

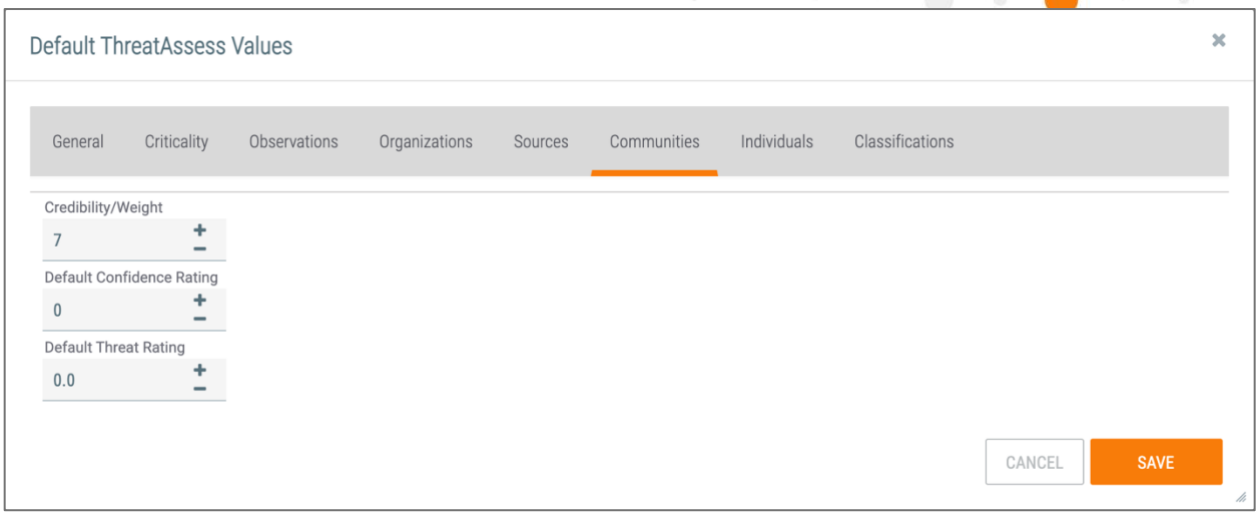

Figure 33

11. Select the **Individuals** tab (Figure 34) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** parameters for individuals. Enter the values manually, or use the plus and minus symbols to add or subtract increments of 1, respectively.

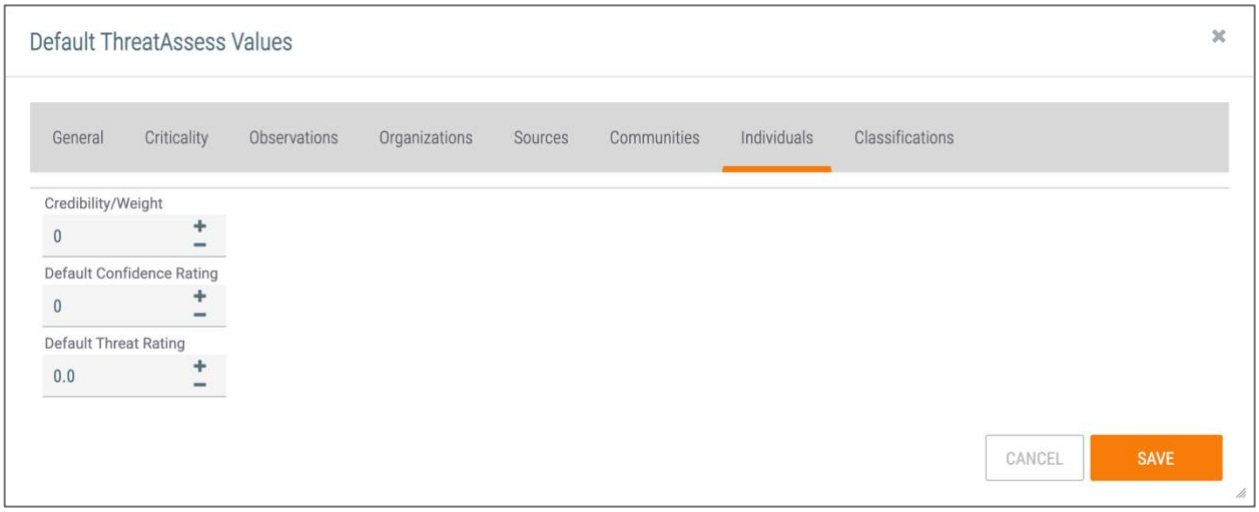

Figure 34

12. Select the **Classifications** tab (Figure 35) to configure the settings for the four ThreatAssess Assessments, which are displayed on the **Indicator Analytics** card of the **Details** window and the **Details** screen for an Indicator. Enter the values manually, or use the plus and minus symbols to add or subtract increments of 1, respectively.

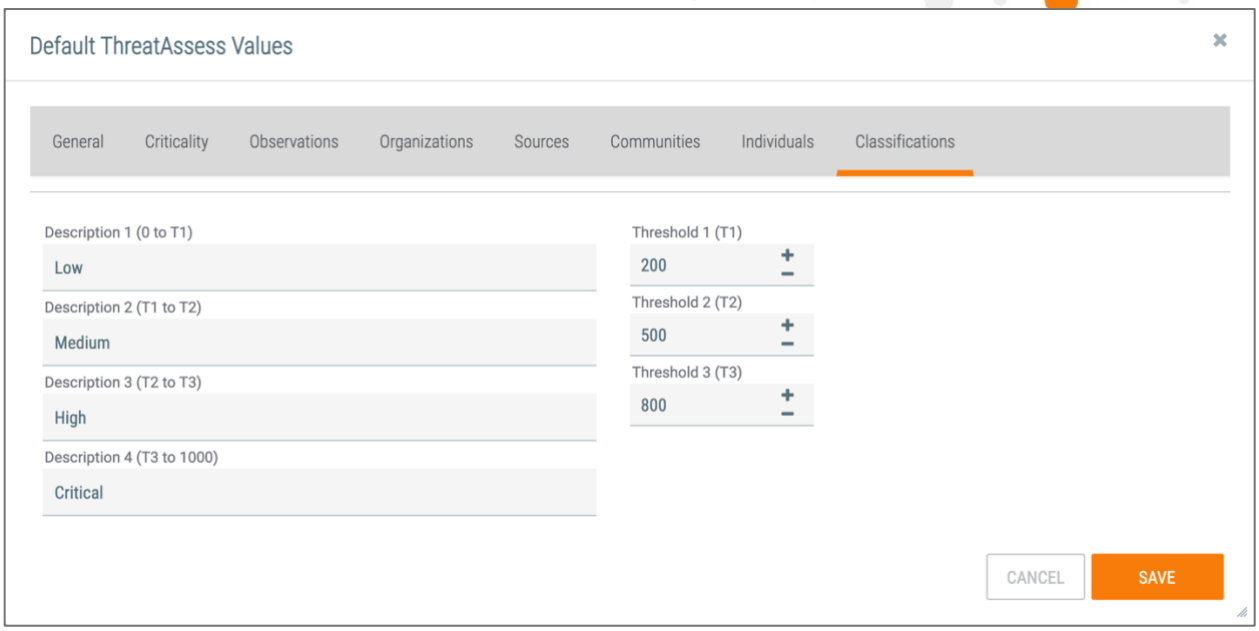

Figure 35

Configure ThreatAssess of an Individual Record

1. 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** window will be displayed (Figure 36).

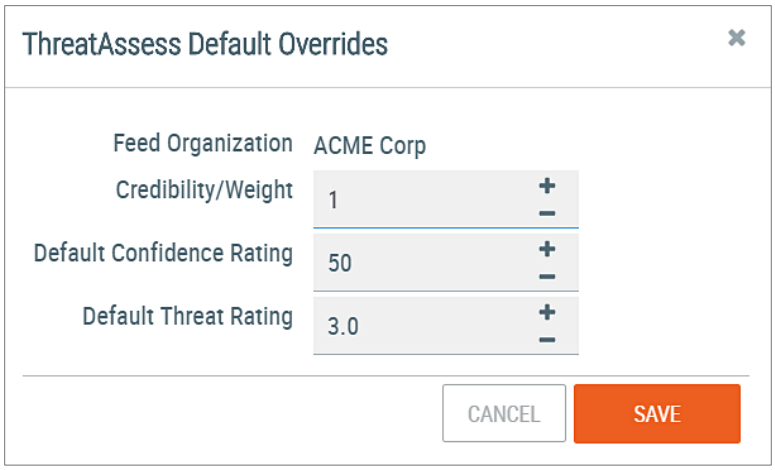

Figure 36

2. Configure the values as desired, and then click the **SAVE** button.

Analyze an Indicator in Real Time

NOTE: This feature is only available to System Administrators.

1. Repeat Steps 1–4 in the "Configure ThreatAssess" section.
2. Click the **ANALYZE INDICATORS** button, and the **ThreatAssess/Statistics** window will be displayed (Figure 37).

Figure 37

3. 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 38).

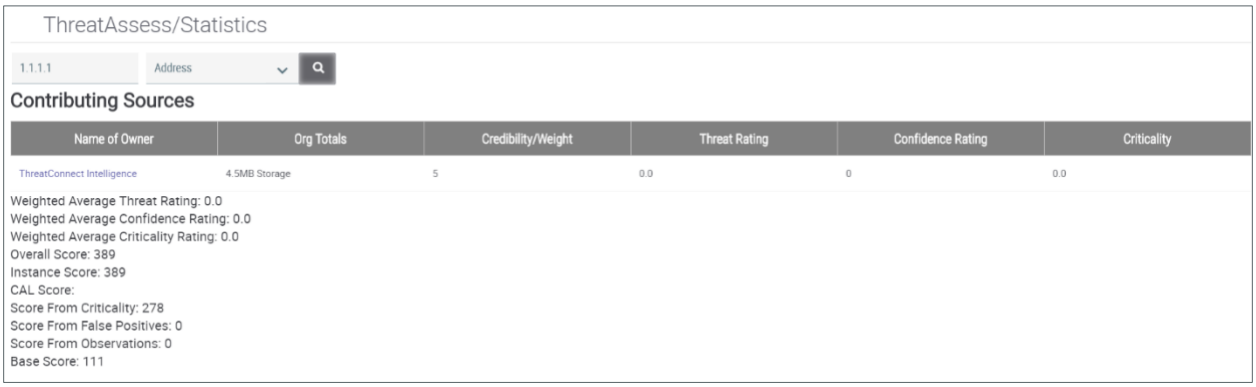

Figure 38

View or Create ThreatAssess Overrides

1. Repeat Steps 1–4 in the "Configure ThreatAssess" section.
2. Click the **+ NEW** button, and the **Create ThreatAssess Overrides** window will be displayed with the **Add for a Single Organization** tab selected (Figure 39). This tab allows users to create a new ThreatAssess override for an existing Data Owner by modifying the parameters displayed, and then clicking the **SAVE** button.

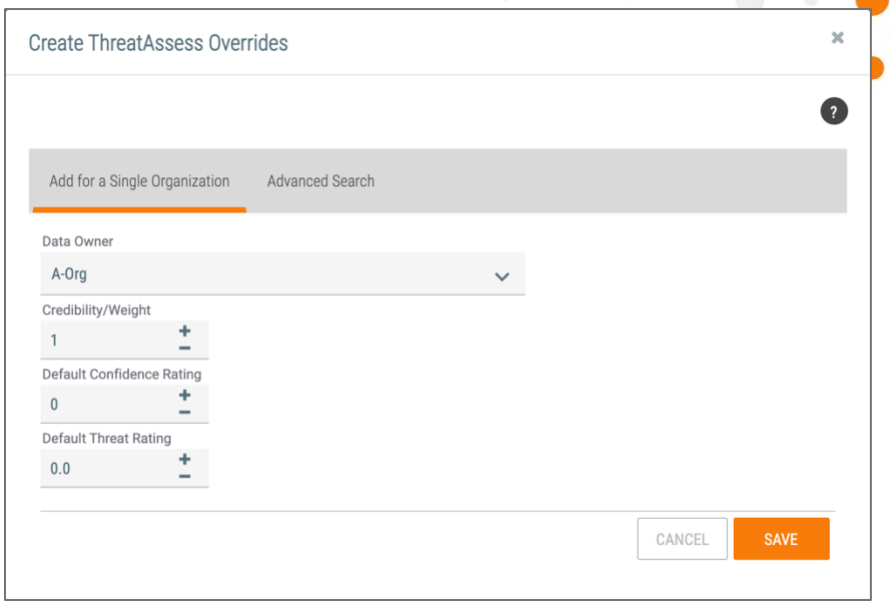

Figure 39

3. Select the **Advanced Search** tab (Figure 40) to search for Data Owners that meet the desired criteria for feeds.

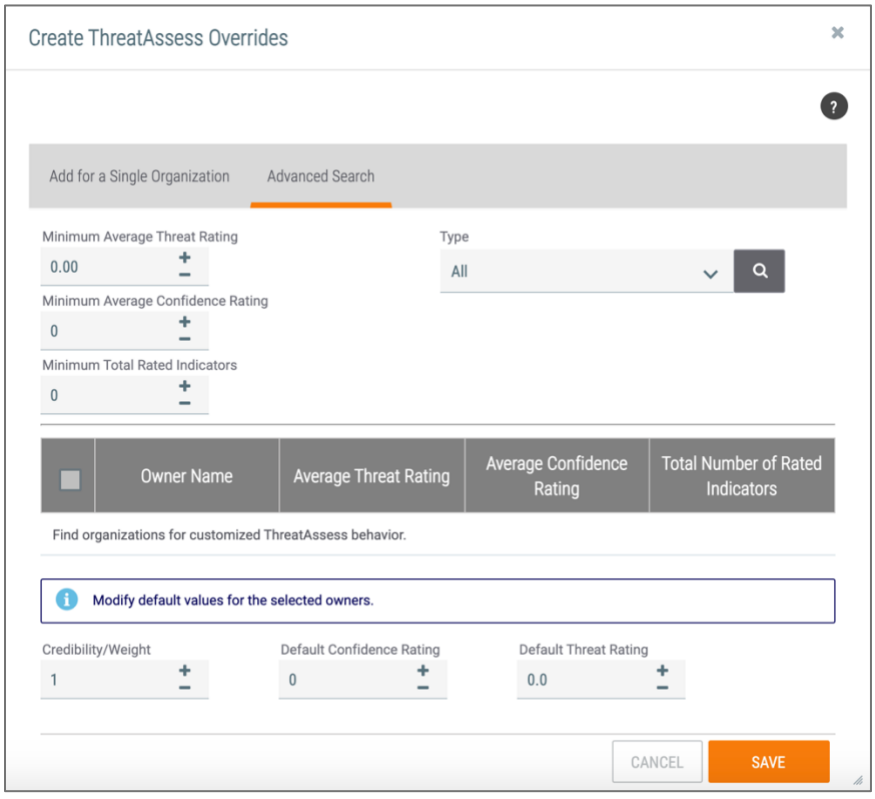

Figure 40