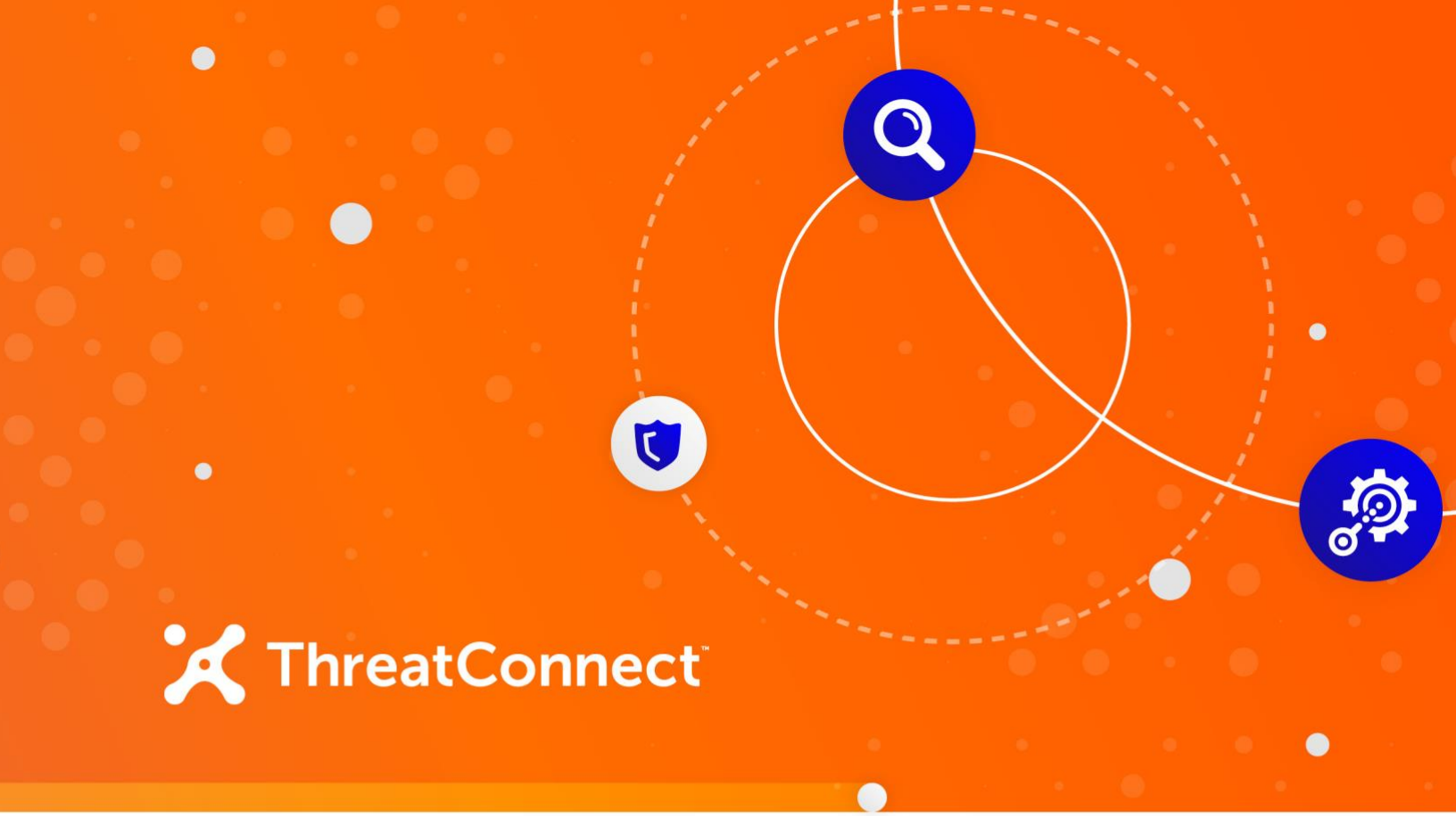

ThreatConnect

Account Administration

User Guide

Software Version 6.3

September 13, 2021

10010-11 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

Overview

This guide focuses on the capabilities provided on the **Account Settings** screen:

- View, create, modify, and delete Organizations on the ThreatConnect instance
- View, create, modify, and delete Communities and Sources on the ThreatConnect instance
- View and filter all user and data activity on the ThreatConnect instance
- View all users currently logged into the ThreatConnect instance
- View owner roles and permission levels and create and modify custom owner roles on the ThreatConnect instance
- View and configure ThreatAssess parameters for the ThreatConnect instance

ThreatConnect user accounts with a System role of Administrator or Operations Administrator have full access to the **Account Settings** screen. Accounts with a System role of Accounts Administrator can view the **Account Settings** screen and perform a limited set of functionalities. All other accounts have either read-only or no access to the **Account Settings** screen.

Accessing the Account Settings Screen

1. On the top navigation bar, hover the cursor over **Settings** . The **Settings** menu will be displayed (Figure 1).

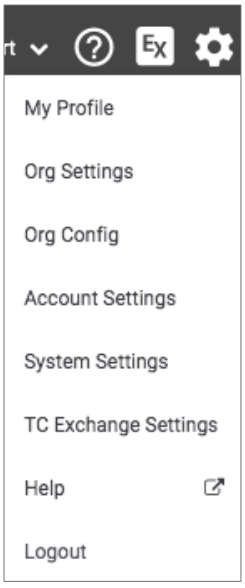

Figure 1

2. Select **Account Settings**. The **Account Settings** screen will be displayed with the **Organizations** tab selected (Figure 2).

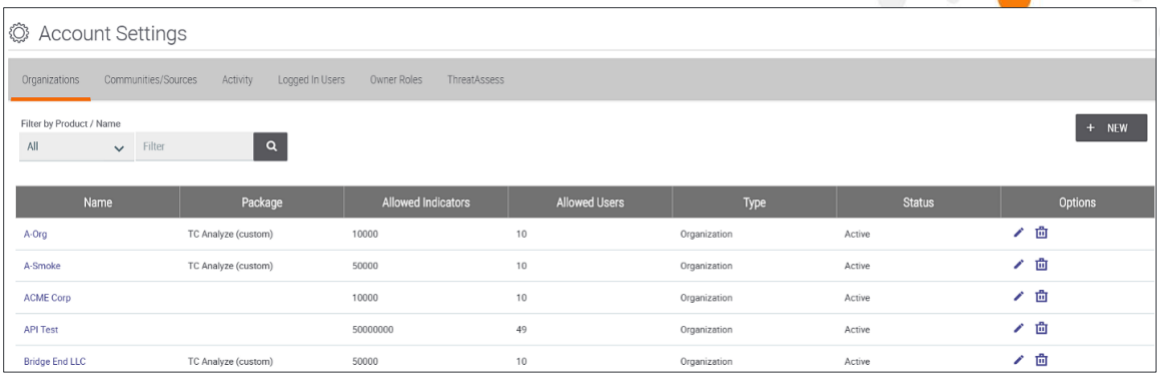

Figure 2

Organizations Tab

The **Organizations** tab of the **Account Settings** screen (Figure 2) provides options for viewing, creating, editing, and deleting Organizations on the ThreatConnect instance.

Create an Organization

1. Click the **+ NEW** button. The **Create Organization** window will be displayed (Figure 3).

NOTE: If the** + NEW **button is not visible, check the** Import License **section of the** Settings **tab of the** System Settings **screen to determine whether all licensed Organizations have been allocated. If this is the case, either deallocate any unused Organizations or purchase a license upgrade to allow more Organizations.

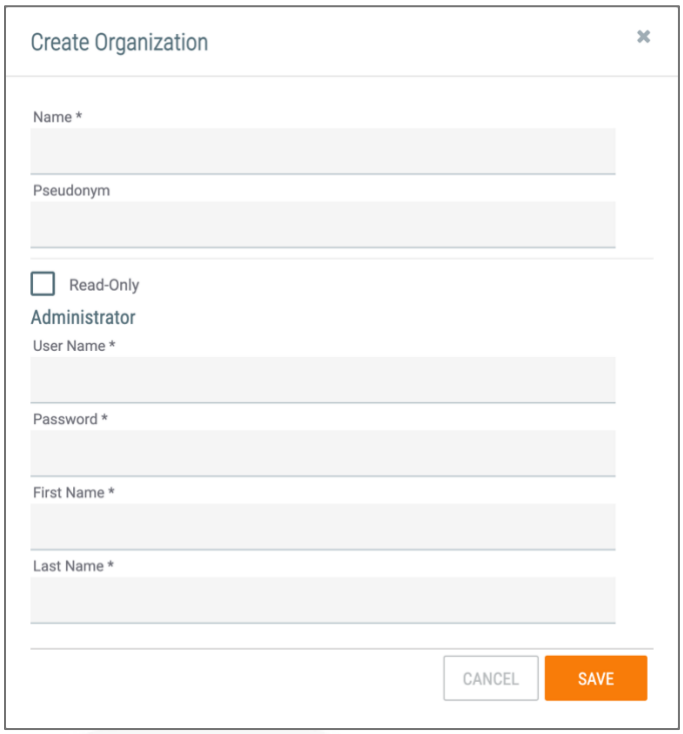

Figure 3

- **Name**: Enter the name of the Organization.
- **Pseudonym**: Enter a pseudonym for the Organization.
- **Read-Only**: Select this checkbox to restrict the permissions to read-only status.
- **User Name**: Enter the User Name for the initial Administrator account. It is recommended 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.
- **Password**: Enter the password for the initial Administrator account.
- **First Name**: Enter the first name for the initial Administrator account.
- **Last Name**: Enter the last name for the initial Administrator account.

2. 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 Organization accounts. Most account configuration is done from the options in this table. Click on the name of an Organization to view its **Organization Settings** screen. See the *ThreatConnect Organization Administration Guide* for more information about the **Organization Settings** screen and *Creating User Accounts* for instruction on creating user accounts in an Organization in ThreatConnect.

1. Click **Edit** in the **Options** column of the Organization whose information is to be configured. The **Organization Information** window will be displayed with the **Standard Options** tab selected (Figure 4).

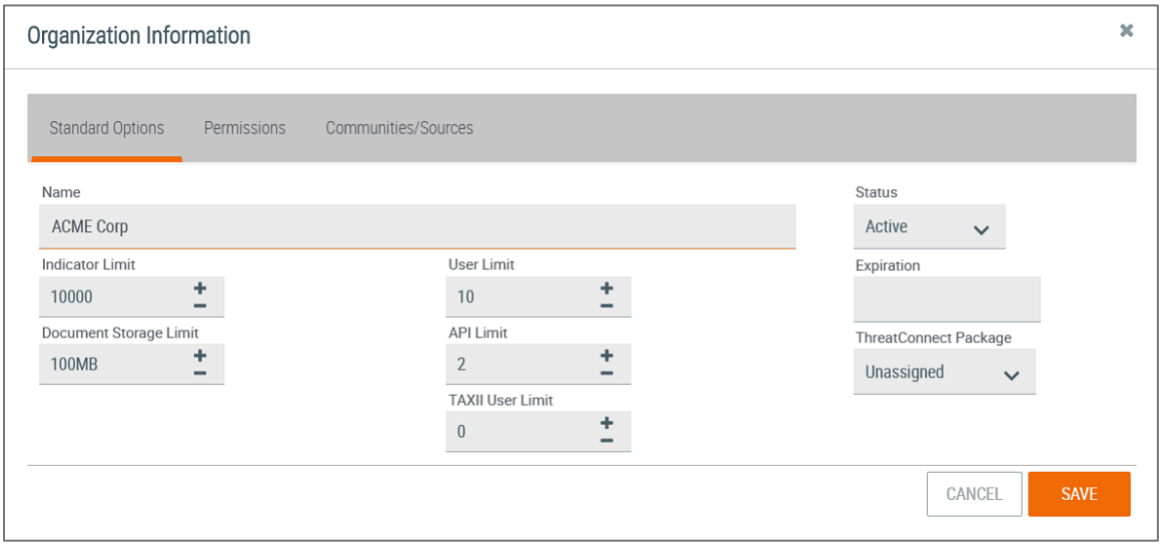

Figure 4

- **Name**: Modify the Organization account name if desired.
- **Indicator Limit**: Enter the Indicator Limit for the Organization, or use the plus and minus buttons 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 buttons to add or subtract increments of 1, respectively.
- **User Limit**: Enter the maximum number of users that can exist in an Organization, or use the plus and minus buttons to add or subtract increments of 1, respectively.

  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 buttons 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 buttons 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 will still exist, but it will not be accessible.
- **Expiration**: Select or enter a date for when the Organization will no longer be accessible within ThreatConnect. On this date, the status of the Organization will automatically change from **Active** to **Expired**.
- **ThreatConnect Package:** Select a ThreatConnect package. This selection will determine the options available under the **Permissions** tab.

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

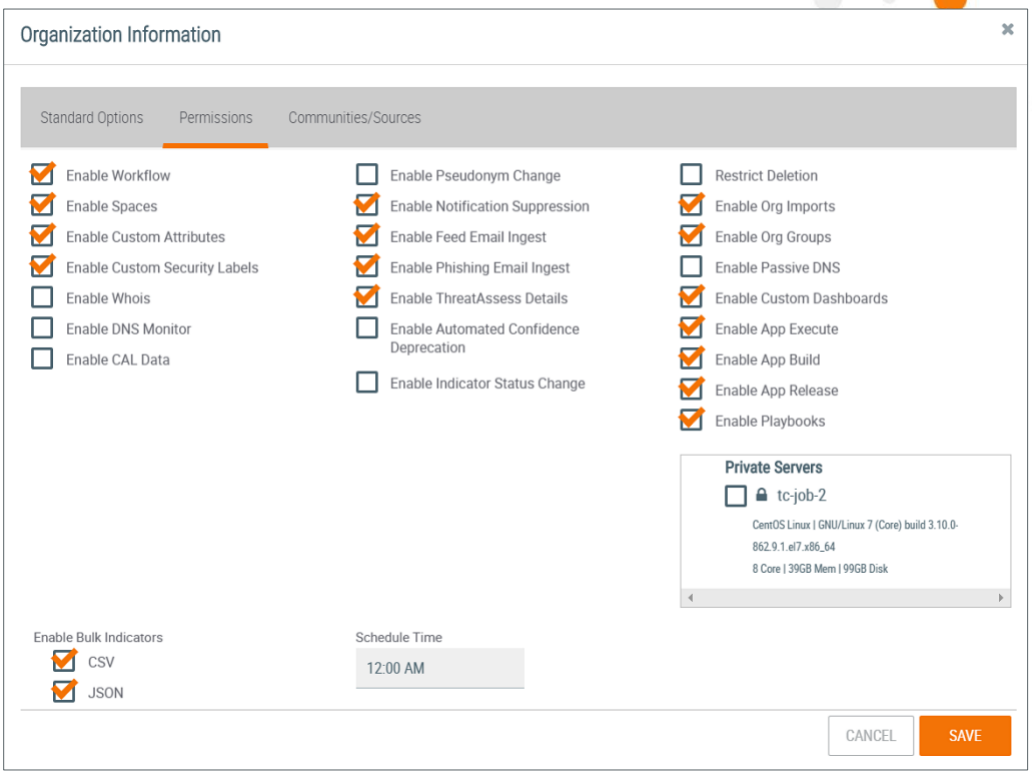

Figure 5

- **Enable Workflow**: Select the checkbox to enable the Workflow feature.
- **Enable Spaces**: Select the checkbox to enable the creation and use 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 Collective Analytics Layer (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 cleared, 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 will not be 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 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 feature.
- **Enable Bulk Indicators**: Select the **CSV** (Comma-Separated Values) or **JSON** (JavaScript® Object Notation) checkbox, or both, to enable the Bulk Indicator Export feature.
- **Schedule Time**: Click in the field to set the time at which bulk Indicator exports are to be scheduled.
- **Private Servers**: Select the checkbox to enable the Private Server feature.

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

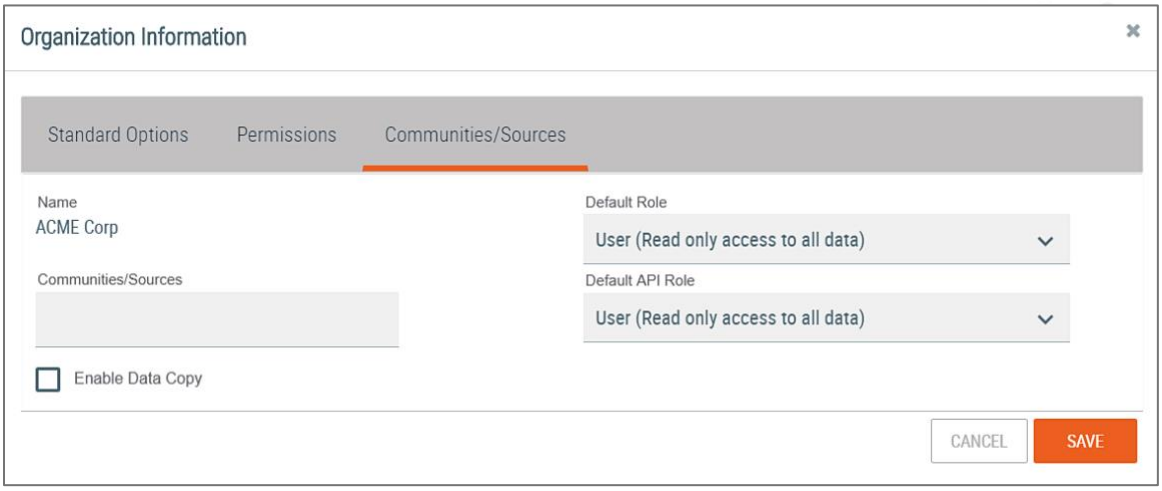

Figure 6

- **Communities/Sources**: Enter the name of a Community or Source that the Organization will 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 accounts in the Organization will be given in the Community or Source.

  ***NOTE: More information about Community and Source roles can be found in the* ThreatConnect Community and Source Administration User Guide *and* ThreatConnect Owner Roles and Permissions.**
- **Default API Role**: Select the default role all API accounts in the Organization will be given.
- **Enable Data Copy**: Select the checkbox to allow Community users to copy data from the Community to their Organization.

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

Delete an Organization

1. Click **Delete** in the **Options** column of the Organization to be deleted. The **Delete Organization** window will be displayed.
2. Click the **YES** button to delete the Organization.

Communities/Sources Tab

The **Communities/Sources** tab of the **Account Settings** screen (Figure 7) provides options for viewing, creating, editing, and deleting Communities and Sources on the ThreatConnect instance.

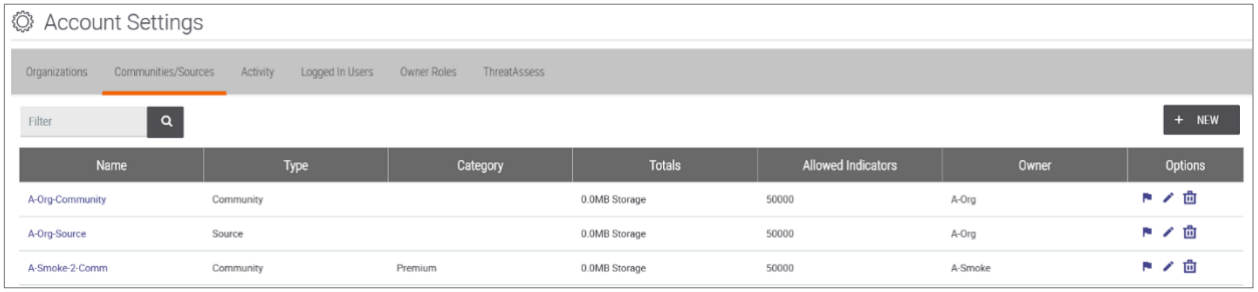

Figure 7

Community Management

Create a Community

1. Click the **+ NEW** button. The **Create Community/Source** window will be displayed with the **Community** option selected by default (Figure 8). Use the scroll bar on the right side of the window to access the full **Description** text box.

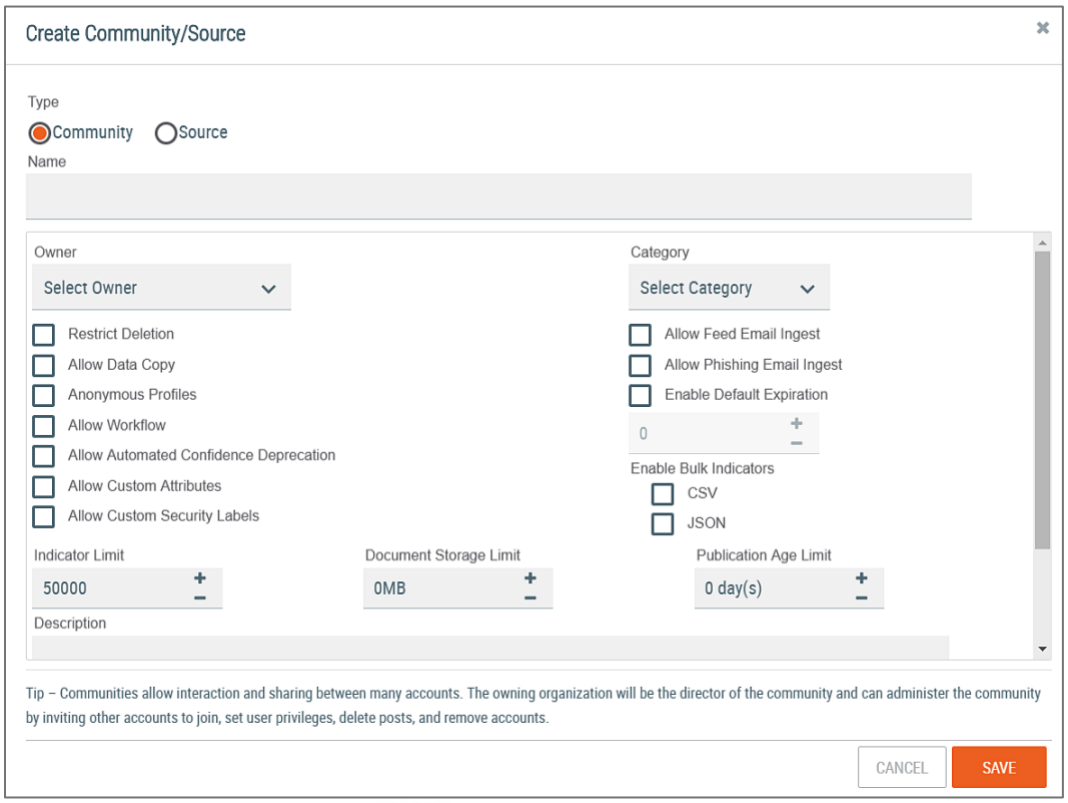

Figure 8

- **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 the Community. Doing so will remove the **Delete** icon from the Community name displayed in the table.
- **Allow Data Copy**: Select the checkbox to enable Community users to copy data from the Community to their 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 the Community's objects to be available in Workflow.
- **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 in the Community.
- **Allow Custom Security Labels**: Select the checkbox to allow the creation of custom Security Labels in the Community.
- **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, or both, to enable the Bulk Indicator Export feature.

  NOTE: Indicators are retrieved via the API, and** bulkIndicatorEnabled **must be true in** System Settings**, while** bulkIndicatorTempLocation **must be a valid writable directory. If the** JSON **checkbox 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 the** CSV **checkbox 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.

- **Indicator Limit**: Enter maximum number of Indicators for the Community, or use the plus and minus buttons to add or subtract increments of 1, respectively.
- **Document Storage Limit**: Enter the amount of document storage space available to the Community, or use the plus and minus buttons 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 buttons to add or subtract increments of 1, respectively.
- **Description:** Enter an initial description for the Community.

2. Click the **SAVE** button to create the Community. If the new Community is not displayed on the **Communities/Sources** screen, log out and log back into ThreatConnect to refresh the screen.

Edit a Community

1. Click **Edit** in the **Options** column of the Community to be edited. The **Create Community/Source** window will be displayed (Figure 8).
2. Make the desired changes, and click the **SAVE** button.

Add Accounts to a Community

1. Click **Community Membership** in the **Options** column of the Community to which the accounts will be added. The **Community/Source Membership** window will be displayed (Figure 9).

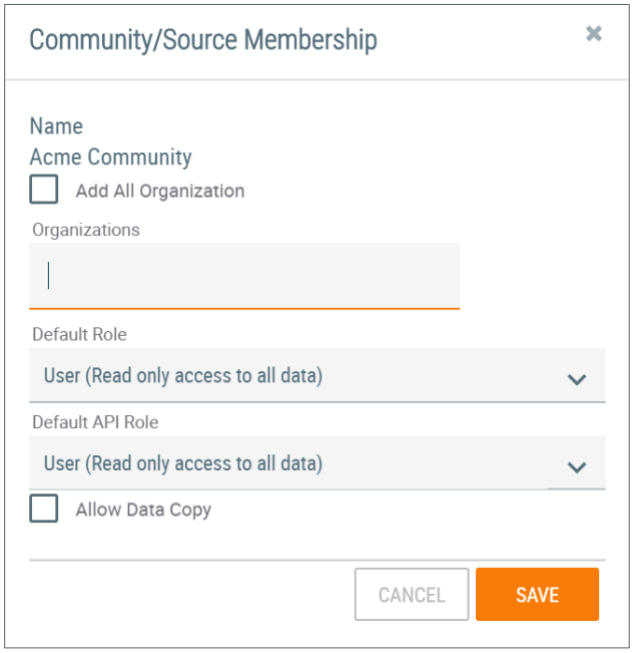

Figure 9

- **Add All Organizations**: Select the checkbox to add all Organizations on the ThreatConnect instance 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 Community role all the accounts within the Organization will be given in the Community.

  ***NOTE: More information about Community and Source roles and default API roles can be found in the* ThreatConnect Community and Source Administration User Guide *and* ThreatConnect Owner Roles and Permissions.**
- **Default API Role**: Select the default Community 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 Organization.

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

Delete a Community

1. Click **Delete** in the **Options** column of the Community to be deleted. The **Delete Community** window will be displayed.
2. Click the **YES** button to delete the Community.

Perform Other Community Administrative Tasks

1. Click a Community name in the **Name** column, and the **Community Info** screen will be displayed (Figure 10).

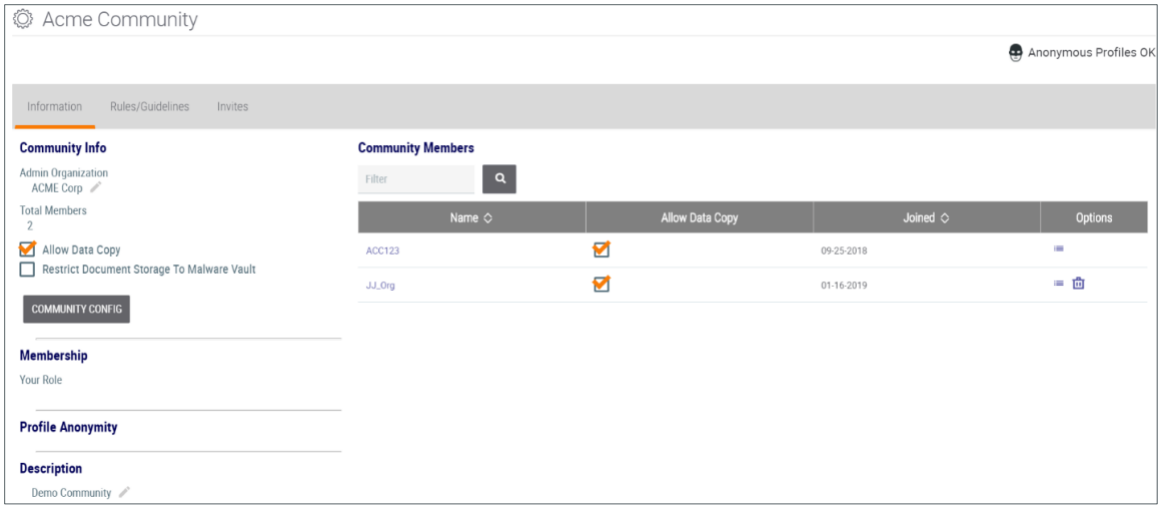

Figure 10

2. The **Community Info** screen allows the Administrator to send Community invites, set specific roles for Organizations and users within the Community, and edit Community rules and guidelines. For instructions on how to perform these tasks, see *ThreatConnect Community and Source Administration User Guide*.

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

1. On the top navigation bar, click **Posts.** The **Posts** screen will be displayed (Figure 11).

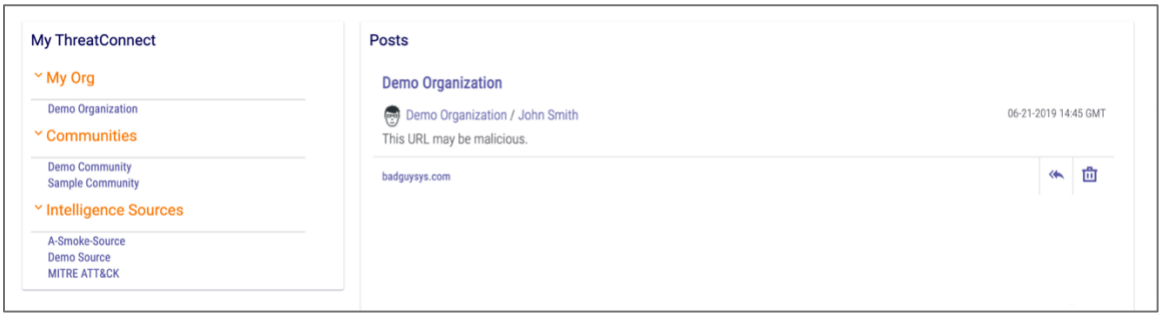

Figure 11

2. Select the desired Community in the **My ThreatConnect** card. The **Posts** screen for the Community will be displayed (Figure 12).

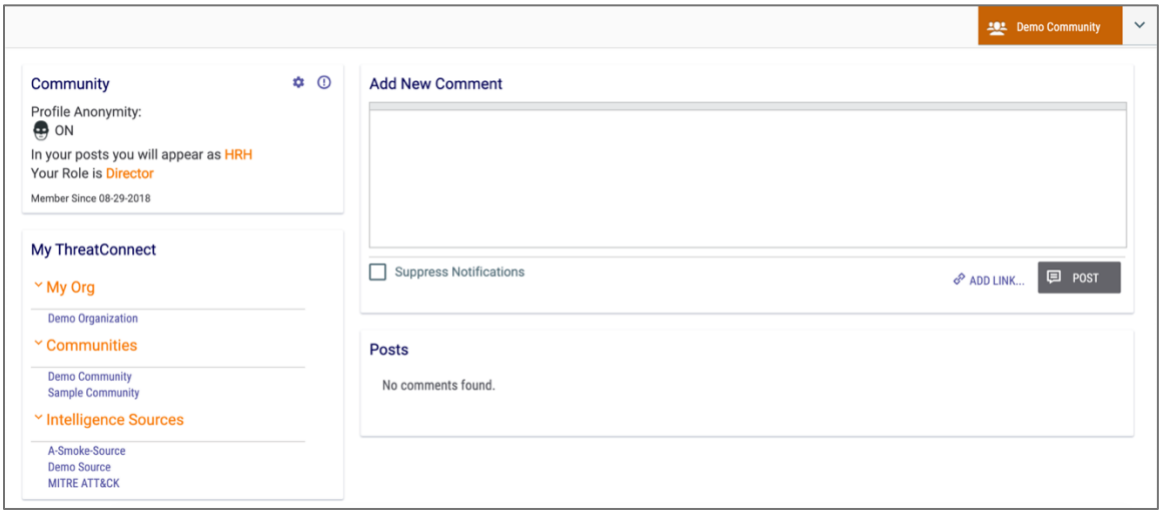

Figure 12

3. Click the **Community Info** icon at the upper right of the **Community** card. The **Community Info** screen will be displayed (Figure 10).

Source Management

Create a Source

NOTE: When creating a new Source, users must log out and log back into ThreatConnect to see the new Source.

1. From the **Communities/Sources** tab of the **Account Settings** screen (Figure 7), click the **+ NEW** button. The **Create Community/Source** window will be displayed with the **Community** option selected by default (Figure 8)
2. Select the **Source** radio button. The **Create Community/Source** window will update with options for creating a Source (Figure 13). Use the scroll bar on the right of the screen to access the **Description** text box.

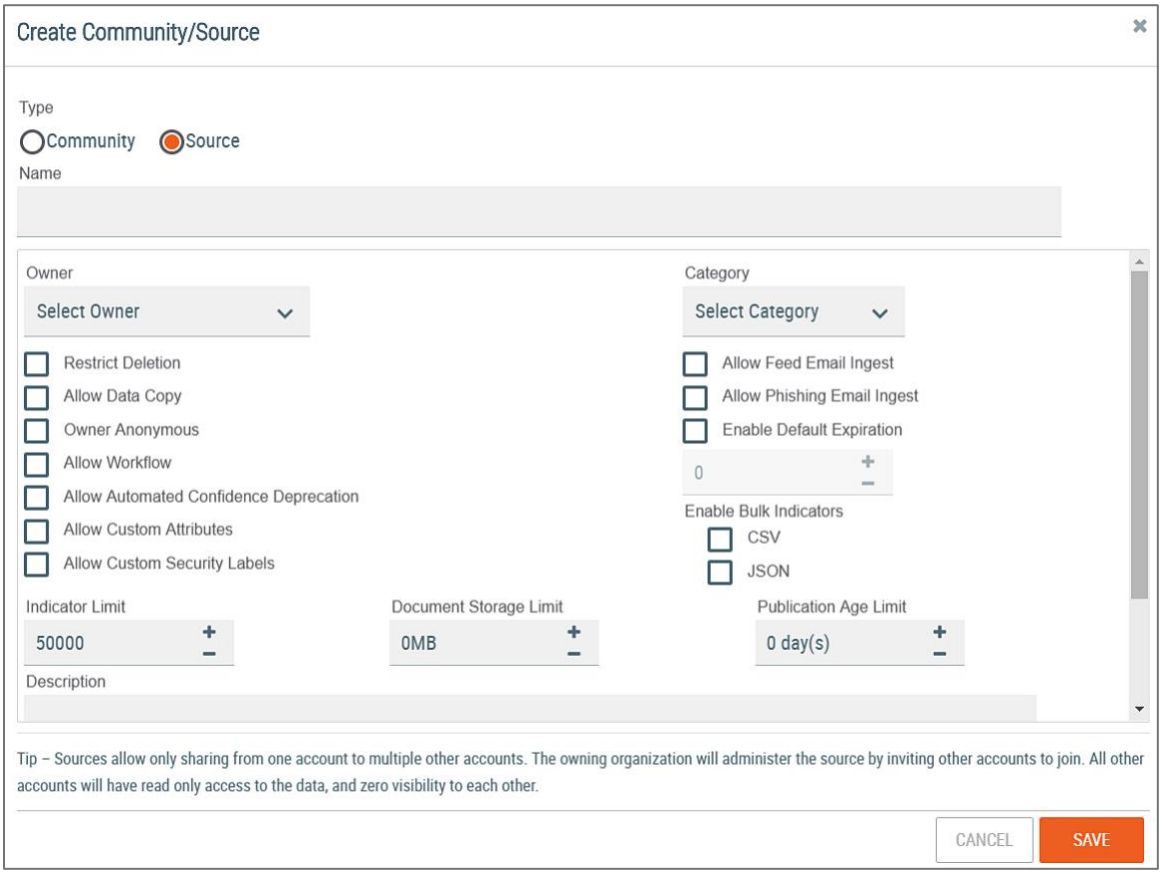

Figure 13

- **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 the 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 Organization.
- **Owner Anonymous**: Select the checkbox to make the Source owner anonymous.
- **Allow Workflow**: Select the checkbox to enable the Source's objects to be available in Worfklow.
- **Allow Automated Confidence Deprecation**: Select the checkbox to create Deprecation Rules for the Source's Indicators.
- **Allow Custom Attributes**: Select the checkbox to allow the creation of custom Attribute Types in the Source.
- **Allow Custom Security Labels**: Select the checkbox to allow the creation of custom Security Labels in the Source.
- **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**: Select the **CSV** or **JSON** checkbox, or both, to enable the Bulk Indicator Export feature.

  NOTE: Indicators are retrieved via the API, and** bulkIndicatorEnabled **must be true in** System Settings**, while** bulkIndicatorTempLocation **must be a valid writable directory. If the** JSON **checkbox 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 the** CSV **checkbox 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 the maximum number of Indicators for the Source, or use the plus and minus buttons 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 the Source, or use the plus and minus buttons 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 buttons to add or subtract increments of 1, respectively.
- **Description:** Enter a description for the Source.

3. Click the **SAVE** button to create the Source.
4. Log out and log back into ThreatConnect to see the new Source.

Other Source Management Options

Sources are managed similarly to Communities. Use the information in the “Edit a Community,” “Add Accounts to a Community,” ”Delete a Community,” and “Perform Other Community Administrative Tasks” sections for guidance on the same functionalities for Sources.

Activity

The **Activity** tab of the **Account Settings** screen (Figure 14) displays activity logs within the system, including logins, creations, and deletions.

Figure 14

If desired, filter the table by selecting activities of interest from the dropdown menu above the **Summary** column (Figure 15).

Figure 15

Logged In Users

The **Logged In Users** tab of the **Account Settings** screen (Figure 16) displays a table with the following information for users currently logged into the ThreatConnect instance: **User Name**, **Organization**, and **IP Address** from which the account is logged in.

Figure 16

Owner Roles

The **Owner Roles** tab of the **Account Settings** screen (Figure 17) displays a table of all out-of-the-box and custom Organization and Community roles and a description of their functionality, provides System Administrators with options for viewing the permission settings for each role, and allows System Administrators to create new custom roles.

NOTE: A Community role refers to a user's owner role within a Community or Source.

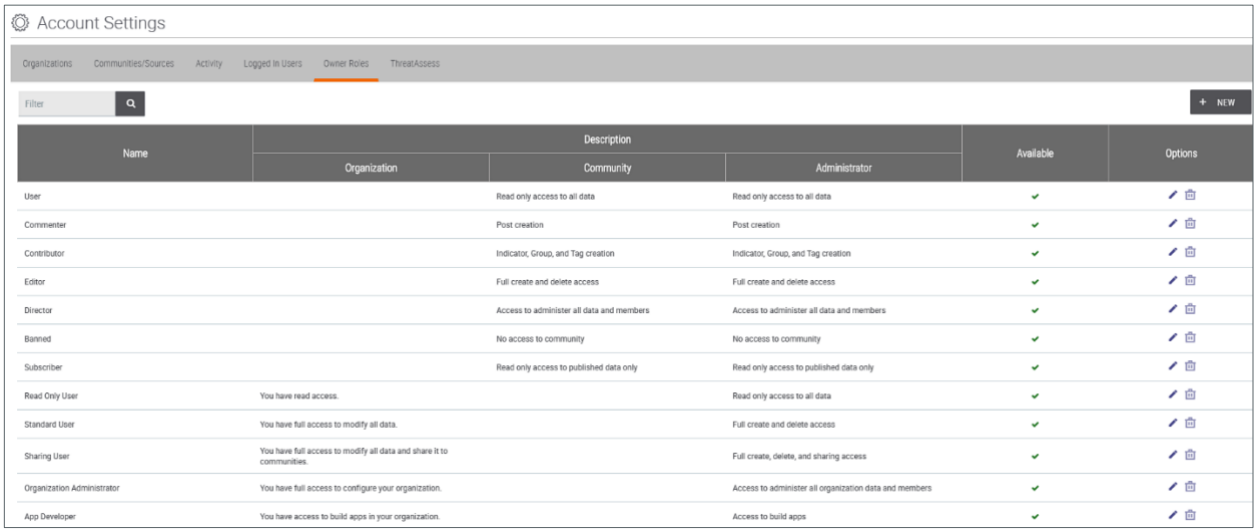

Figure 17

See *ThreatConnect Owner Roles and Permissions* for more information on the following topics:

- Definition of each out-of-the-box Organization role
- Permission settings for each Organization role
- Definition of each out-of-the-box Community role
- Permission settings for each Community role
- Definition of each permission setting
- Creating custom owner roles

ThreatAssess

ThreatAssess gives a basic risk assessment of an Indicator through a single, actionable score. The score, which is found in the **Details** window and on the **Details** screen for an Indicator, among other places, represents the overall potential impact that an Indicator might have to a security organization.

The **ThreatAssess** tab of the **Account Settings** screen (Figure 18) displays the **ThreatAssess Default Organization Overrides** table, which displays the overrides that Administrators have instituted for ThreatAssess settings in specific owners. This screen also provides Administrators with options to configure the default values used to calculate ThreatAssess scores across the ThreatConnect instance and in different owner types, to view ThreatAssess statistics for specific Indicators, and to create and edit default owner overrides.

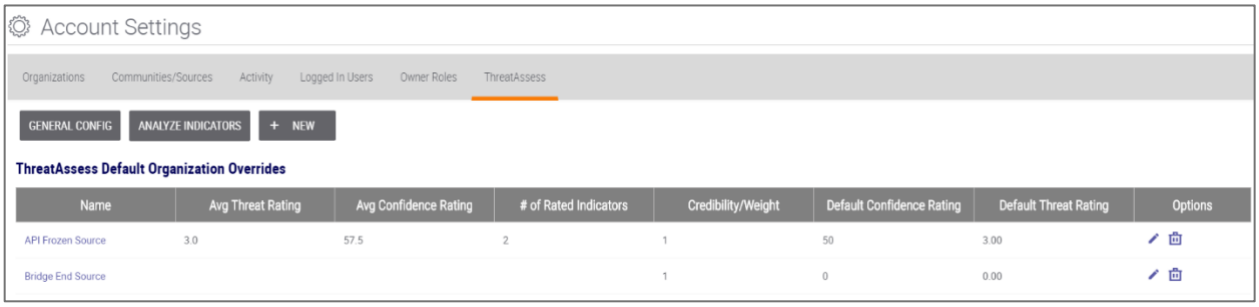

Figure 18

Configure Default ThreatAssess Values

1. Click the **GENERAL CONFIG** button to configure the default parameters used to calculate ThreatAssess scores. The **Default ThreatAssess Values** window will be displayed with the **General** tab selected (Figure 19). On this screen, the following options can be configured: **Use All False Positives**, **Exclude False Positives after (days)**, **Offset for False Positives**, **Weight for CAL Score**, **Weight for Instance Score**, and **Baseline Score**. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

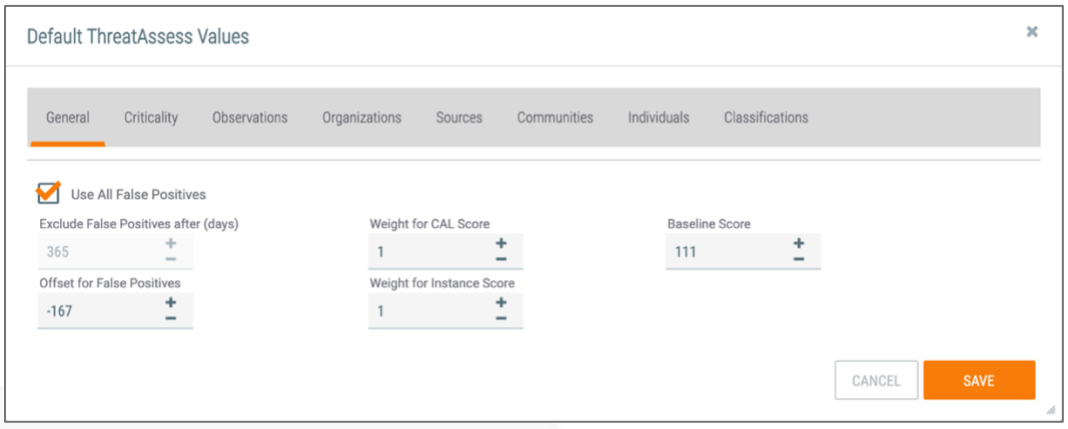

Figure 19

2. Select the **Criticality** tab (Figure 20) to configure the **Criticality Base Coefficient**, **Criticality Linear Coefficient**, **Criticality Quadratic Coefficient**, **Minimum Score Contribution from Criticality**, and **Maximum Score Contribution from Criticality** options. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

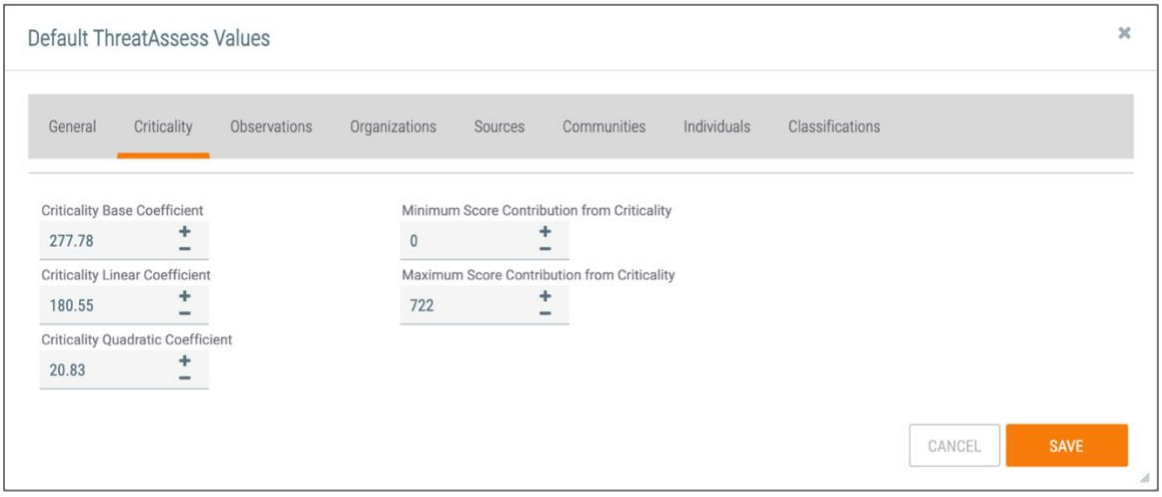

Figure 20

3. Select the **Observations** tab (Figure 21) 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** options. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

Figure 21

4. Select the **Organizations** tab (Figure 22) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for Organizations. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

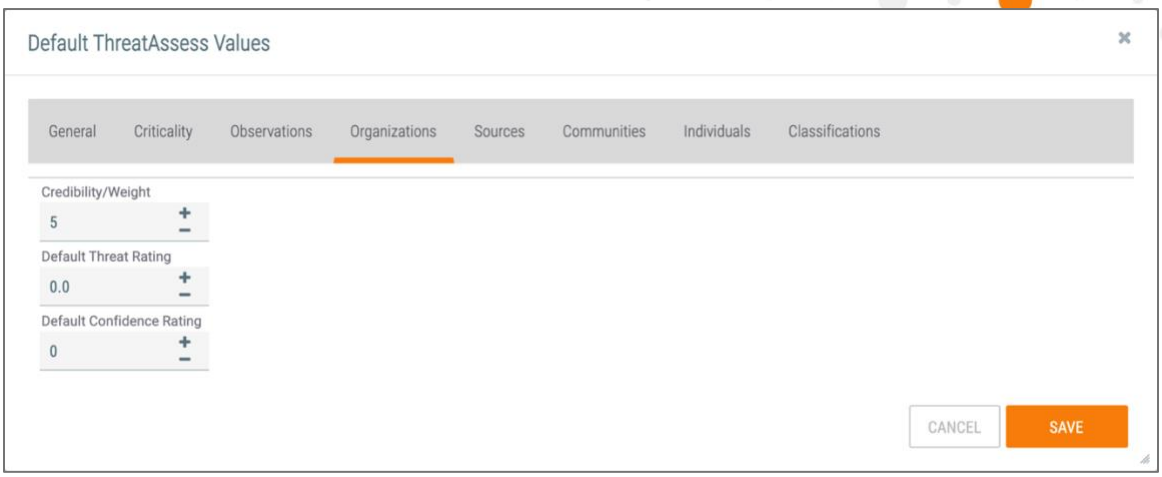

Figure 22

5. Select the **Sources** tab (Figure 23) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for Sources. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively. To exclude Indicators from Sources in ThreatAssess calculations, select the **Exclude Sources** checkbox.

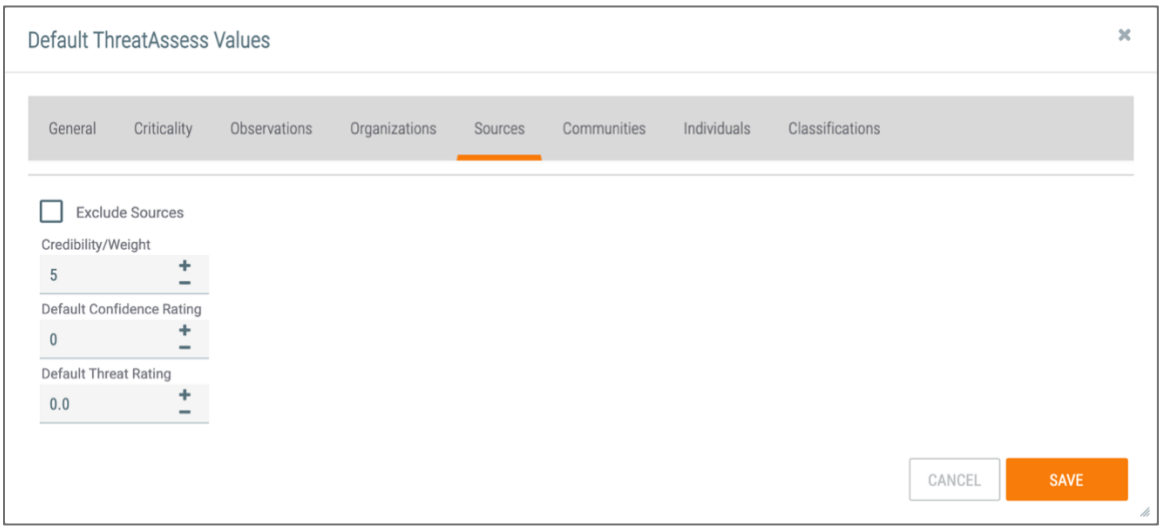

Figure 23

6. Select the **Communities** tab (Figure 24) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for Communities. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

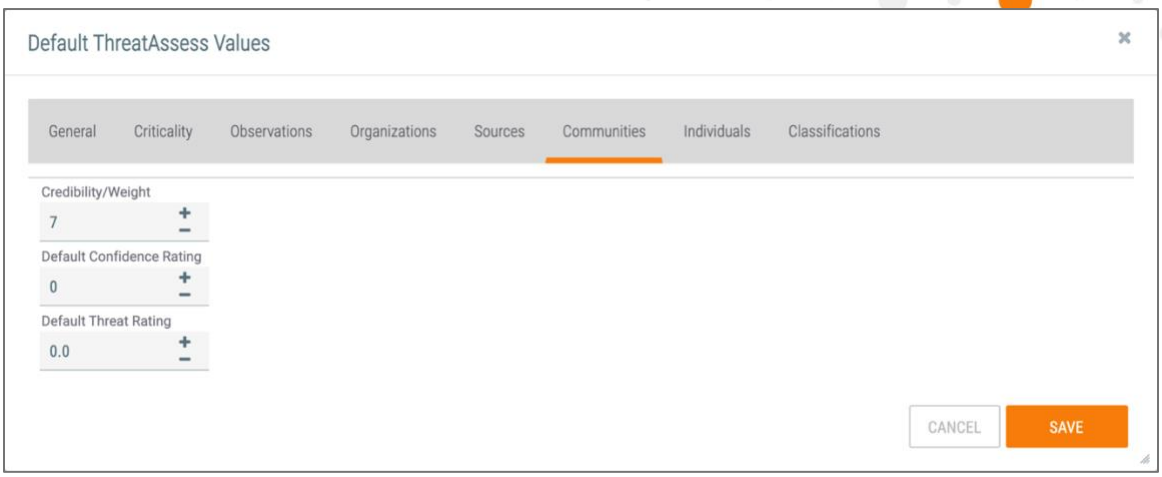

Figure 24

7. Select the **Individuals** tab (Figure 25) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for individuals. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

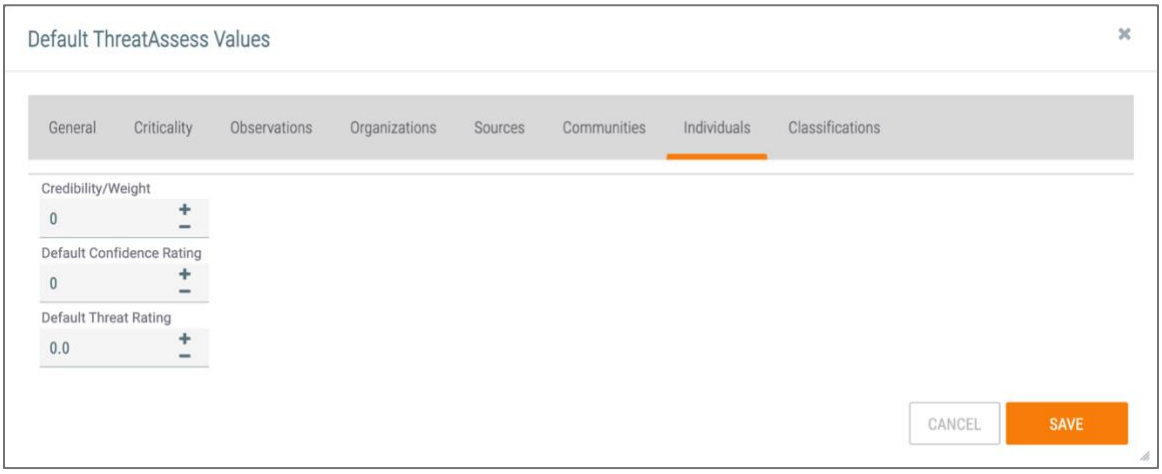

Figure 25

8. Select the **Classifications** tab (Figure 26) to configure the four ThreatAssess Assessments (**Low**, **Medium**, **High**, and **Critical**) and their corresponding **Threshold**, which are displayed on the **Indicator Analytics** card of the **Details** window and the **Details** screen for an Indicator. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

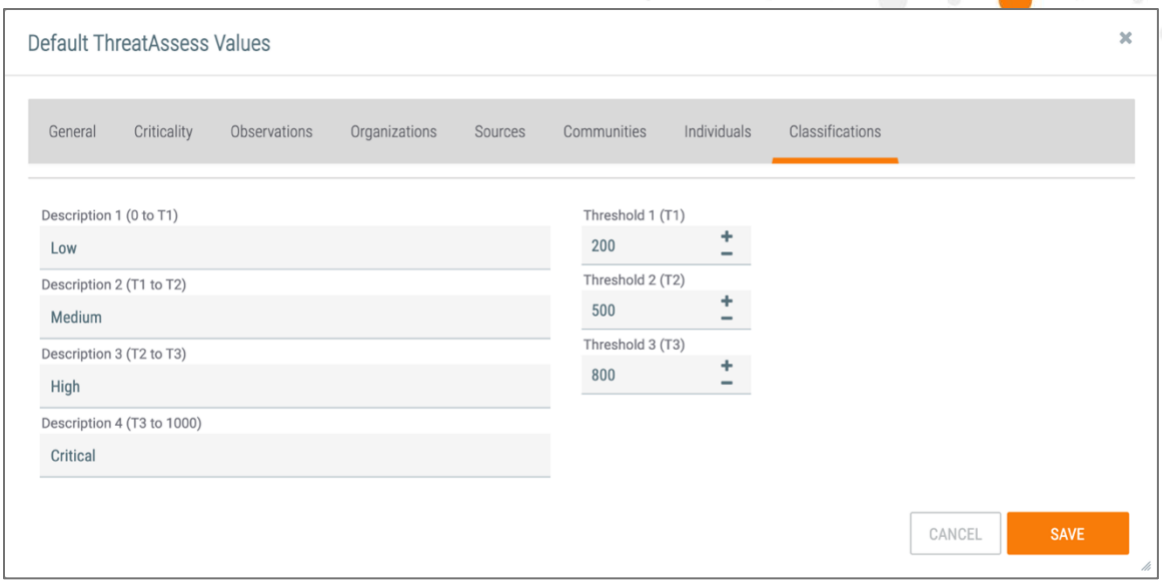

Figure 26

Analyze Indicators

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 18), click the **ANALYZE INDICATORS** button to get current systemwide and owner-specific statistics on an Indicator. The **ThreatAssess/Statistics** screen will be displayed (Figure 27).

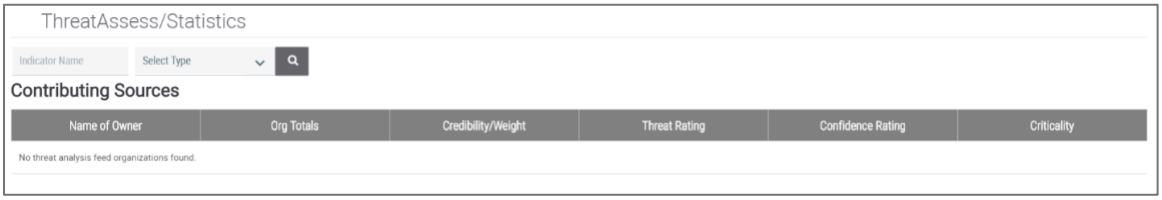

Figure 27

2. Enter the name of an Indicator in the **Indicator Name** box, and select an Indicator type from the **Select Type** dropdown menu. The screen will now display the latest statistics for that Indicator in each of its owners and across the ThreatConnect instance (Figure 28).

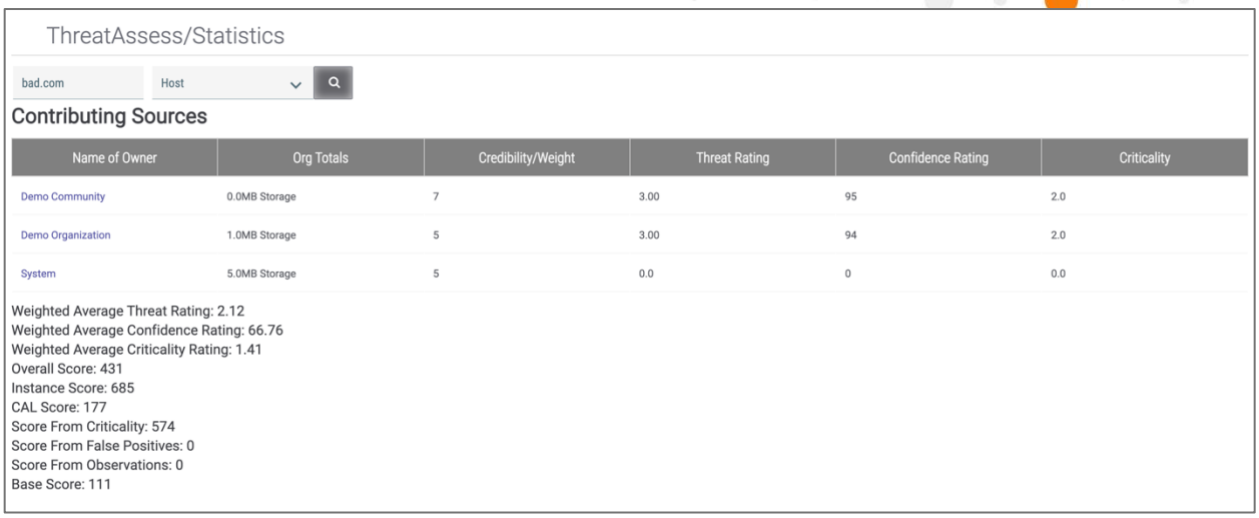

Figure 28

Create ThreatAssess Overrides

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 18), click the **+ NEW** button to create new ThreatAssess default overrides for a data owner (Organization, Community, or Source) or in multiple owners. The **Create ThreatAssess Overrides** window will be displayed with the **Add for a Single Organization** tab selected (Figure 29). Use the **Data Owner** dropdown menu to select the owner in which to create overrides of the default ThreatAssess values, and then modify the following options: **Credibility/Weight**, **Default Confidence Rating**, **Default Threat Rating**. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.

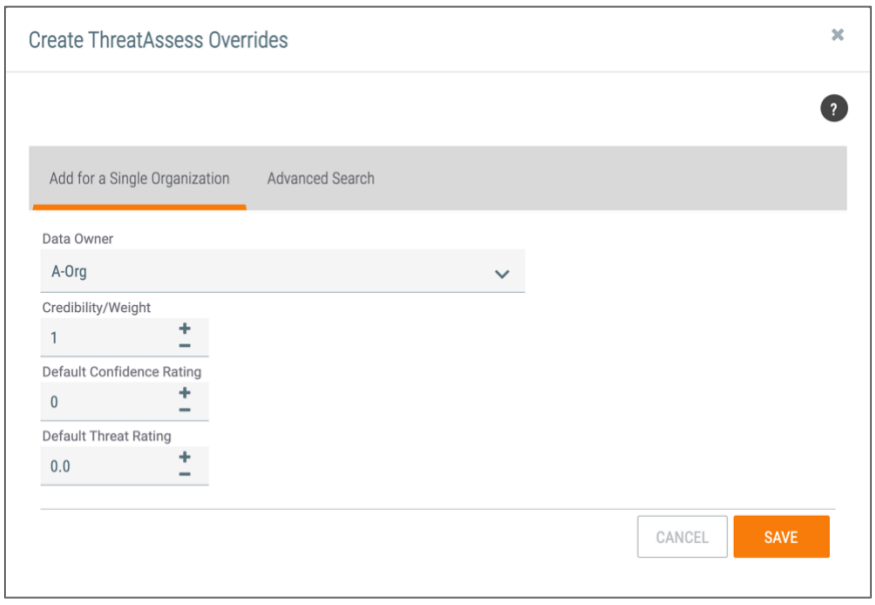

Figure 29

2. Select the **Advanced Search** tab (Figure 30) to search for data owners that meet the desired criteria for feeds.

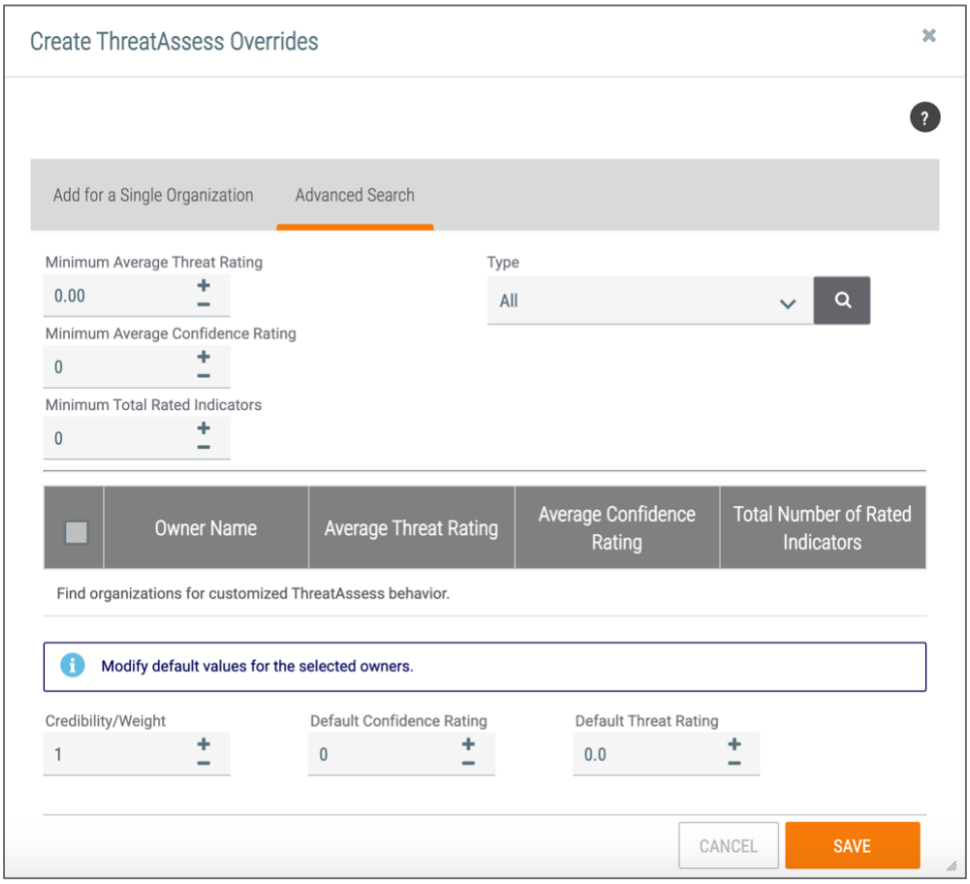

Figure 30

3. Click the **SAVE** button.

Edit ThreatAssess Overrides

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 18), click **Edit** for an entry in the table to edit the ThreatAssess default overrides for that owner. The **ThreatAssess Default Overrides** window will be displayed (Figure 31).

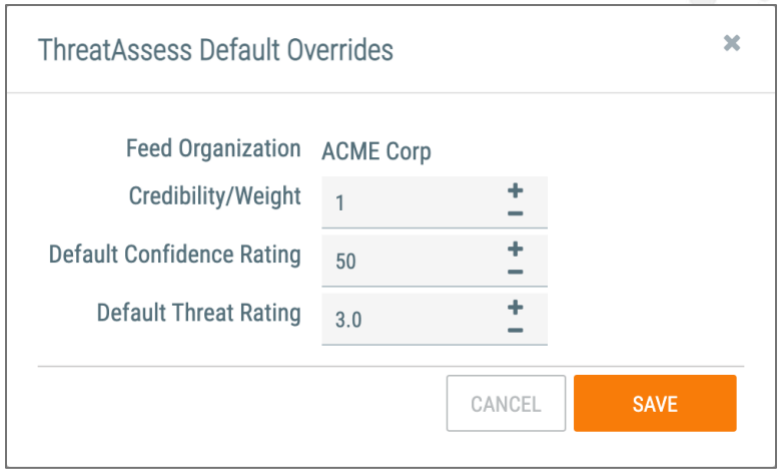

Figure 31

2. The following values may be edited: Credibility/Weight, Default Confidence Rating, and Default Threat Rating. Enter the desired value for each option manually, or use the plus and minus buttons to add or subtract increments of 1, respectively.
3. Click the **SAVE** button.

Delete ThreatAssess Overrides

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 18), click **Delete** for an entry in the table to delete the ThreatAssess default overrides for that owner. The **Delete ThreatAnalysisFeed** window will be displayed (Figure 32).

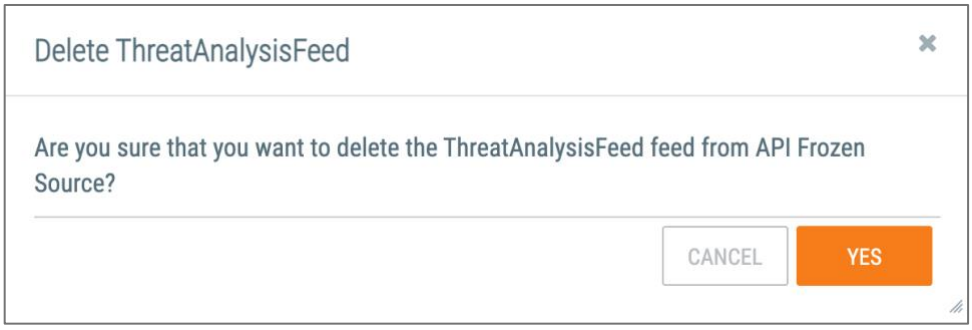

Figure 32

2. Click **YES** to delete the overrides for the selected owner.