

# Account Administration

## User Guide

Software Version 6.5

April 5, 2022

10010-13 EN Rev. A



©2022 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.  
TC Exchange™ and CAL™ are trademarks of ThreatConnect, Inc.  
JavaScript® is a registered trademark of the Oracle Corporation



## Table of Contents

OVERVIEW .....	4
ACCESSING THE ACCOUNT SETTINGS SCREEN.....	4
ORGANIZATIONS TAB.....	4
Create an Organization .....	4
Configure an Organization Account.....	5
Delete an Organization .....	9
COMMUNITIES/SOURCES TAB .....	10
Community Management.....	10
Create a Community .....	10
Edit a Community.....	12
Add Accounts to a Community.....	12
Delete a Community .....	13
Perform Other Community Administrative Tasks .....	13
Source Management .....	15
Create a Source .....	15
Other Source Management Options.....	17
ACTIVITY .....	18
LOGGED IN USERS.....	18
OWNER ROLES.....	19
THREATASSESS .....	20
Configure Default ThreatAssess Values .....	20
Analyze Indicators.....	25
Create ThreatAssess Overrides.....	26
Edit ThreatAssess Overrides .....	28
Delete ThreatAssess Overrides .....	28




## Overview

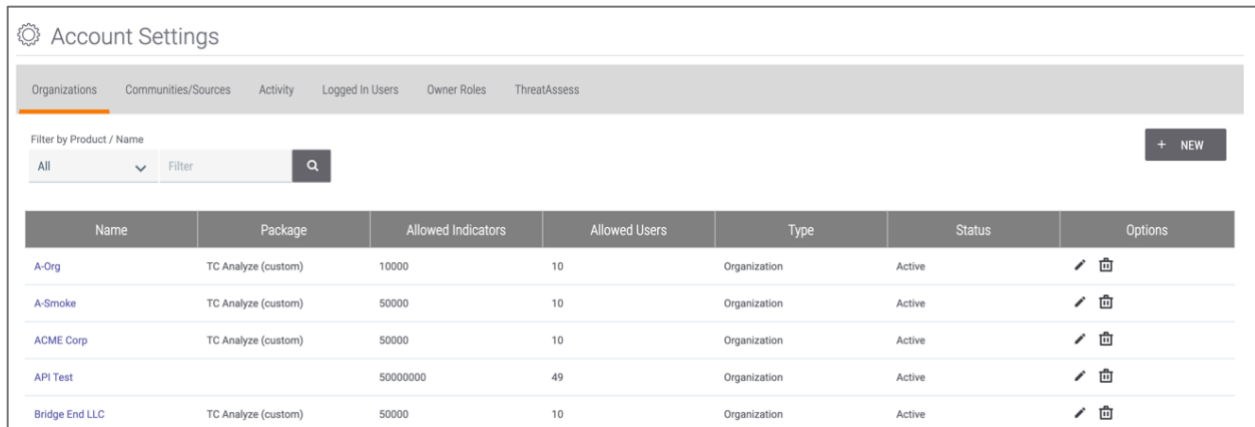
This guide focuses on the capabilities provided on the **Account Settings** screen:

- 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

On the top navigation bar, hover the cursor over **Settings**  and select **Account Settings**. The **Account Settings** screen will be displayed with the **Organizations** tab selected (Figure 1).













Name	Package	Allowed Indicators	Allowed Users	Type	Status	Options
A-Org	TC Analyze (custom)	10000	10	Organization	Active	 
A-Smoke	TC Analyze (custom)	50000	10	Organization	Active	 
ACME Corp	TC Analyze (custom)	50000	10	Organization	Active	 
API Test		50000000	49	Organization	Active	 
Bridge End LLC	TC Analyze (custom)	50000	10	Organization	Active	 

Figure 1

## Organizations Tab

The **Organizations** tab of the **Account Settings** screen (Figure 1) 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 2).



**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.**

The screenshot shows a 'Create Organization' dialog box. It has a title bar with the text 'Create Organization' and a close button (X). Below the title bar are several input fields: 'Name \*', 'Pseudonym', a checkbox labeled 'Read-Only', and an 'Administrator' section. The 'Administrator' section includes 'User Name \*', 'Password \*', 'First Name \*', and 'Last Name \*'. At the bottom right of the form are two buttons: 'CANCEL' and 'SAVE'.

**Figure 2**

- **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.

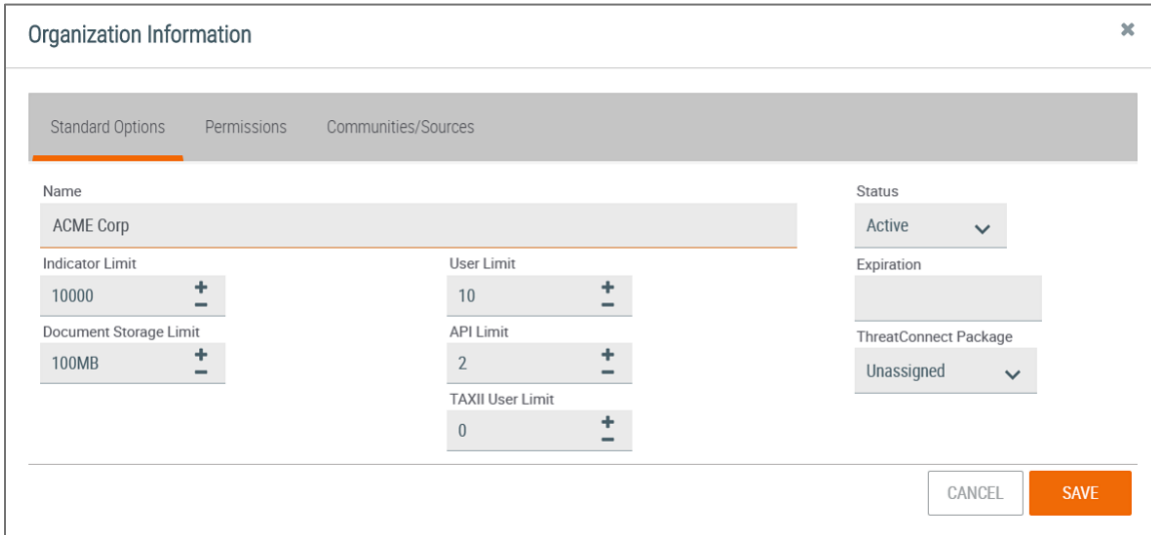
## Configure an Organization Account

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 3).



The screenshot shows the 'Organization Information' window with the 'Standard Options' tab selected. The window contains the following fields and controls:

- Name:** A text input field containing 'ACME Corp'.
- Status:** A dropdown menu set to 'Active'.
- Indicator Limit:** A numeric input field with '10000' and plus/minus buttons.
- User Limit:** A numeric input field with '10' and plus/minus buttons.
- Document Storage Limit:** A numeric input field with '100MB' and plus/minus buttons.
- API Limit:** A numeric input field with '2' and plus/minus buttons.
- TAXII User Limit:** A numeric input field with '0' and plus/minus buttons.
- Expiration:** An empty text input field.
- ThreatConnect Package:** A dropdown menu set to 'Unassigned'.
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom right.

**Figure 3**

- **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 4).

Organization Information

Standard Options | **Permissions** | Communities/Sources

<input checked="" type="checkbox"/> Enable Workflow	<input type="checkbox"/> Enable Pseudonym Change	<input type="checkbox"/> Restrict Deletion
<input checked="" type="checkbox"/> Enable Spaces	<input checked="" type="checkbox"/> Enable Notification Suppression	<input checked="" type="checkbox"/> Enable Org Imports
<input checked="" type="checkbox"/> Enable Custom Attributes	<input checked="" type="checkbox"/> Enable Feed Email Ingest	<input checked="" type="checkbox"/> Enable Org Groups
<input checked="" type="checkbox"/> Enable Custom Security Labels	<input checked="" type="checkbox"/> Enable Phishing Email Ingest	<input type="checkbox"/> Enable Passive DNS
<input type="checkbox"/> Enable Whois	<input checked="" type="checkbox"/> Enable ThreatAssess Details	<input checked="" type="checkbox"/> Enable Custom Dashboards
<input type="checkbox"/> Enable DNS Monitor	<input type="checkbox"/> Enable Automated Confidence Deprecation	<input checked="" type="checkbox"/> Enable App Execute
<input type="checkbox"/> Enable CAL Data	<input type="checkbox"/> Enable Indicator Status Change	<input checked="" type="checkbox"/> Enable App Build
		<input checked="" type="checkbox"/> Enable App Release
		<input checked="" type="checkbox"/> Enable Playbooks

Private Servers

tc-job-2

CentOS Linux | GNU/Linux 7 (Core) build 3.10.0-862.9.1.el7.x86\_64

8 Core | 39GB Mem | 99GB Disk

Enable Bulk Indicators

CSV

JSON

Schedule Time

12:00 AM


CANCEL SAVE

Figure 4

- **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 5). From this screen, an Organization can be added to a Community or Source.

The screenshot shows a dialog box titled "Organization Information" with a close button (X) in the top right corner. Below the title bar are three tabs: "Standard Options", "Permissions", and "Communities/Sources", with the latter being selected and underlined. The main content area is divided into two columns. The left column contains a "Name" field with the value "ACME Corp" and a "Communities/Sources" field which is currently empty. Below these is a checkbox labeled "Enable Data Copy" which is unchecked. The right column contains two dropdown menus: "Default Role" and "Default API Role", both set to "User (Read only access to all data)". At the bottom right of the dialog are two buttons: "CANCEL" and "SAVE".

**Figure 5**


- **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 6) provides options for viewing, creating, editing, and deleting Communities and Sources on the ThreatConnect instance.

Name	Type	Category	Totals	Allowed Indicators	Owner	Options
A-Org-Community	Community		0.0MB Storage	50000	A-Org	
A-Org-Source	Source		0.0MB Storage	50000	A-Org	
A-Smoke-2-Comm	Community	Premium	0.0MB Storage	50000	A-Smoke	

Figure 6

## 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 7). Use the scroll bar on the right side of the window to access the full **Description** text box.

**Create Community/Source**

Type  
 Community  Source

Name

Owner  
Select Owner

Category  
Select Category

Restrict Deletion  
 Allow Data Copy  
 Anonymous Profiles  
 Allow Workflow  
 Allow Automated Confidence Deprecation  
 Allow Custom Attributes  
 Allow Custom Security Labels

Allow Feed Email Ingest  
 Allow Phishing Email Ingest  
 Enable Default Expiration

0  + -

Enable Bulk Indicators  
 CSV  
 JSON


Indicator Limit: 50000  + -  
Document Storage Limit: 0MB  + -  
Publication Age Limit: 0 day(s)  + -

Description

Tip – Communities allow interaction and sharing between many accounts. The owning organization will be the director of the community and can administer the community by inviting other accounts to join, set user privileges, delete posts, and remove accounts.

Figure 7



- **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.**




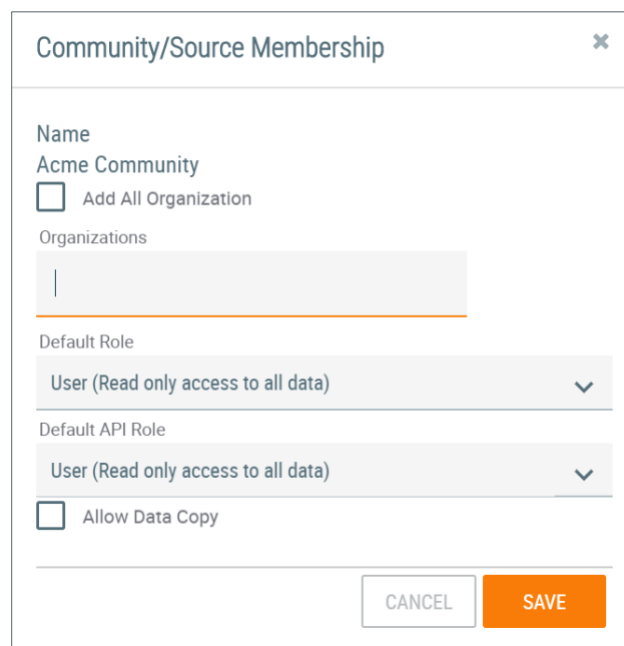
- **Indicator Limit:** Enter maximum number of Indicators for the Community, or use the plus and minus buttons to add or subtract increments of 1, respectively.
  - **Document Storage Limit:** Enter the amount of document storage space available to the Community, or use the plus and minus buttons to 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 7).
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 8).



The screenshot shows a window titled "Community/Source Membership" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Name:** "Acme Community"
- Add All Organization**
- Organizations:** A text input field with a vertical cursor.
- Default Role:** A dropdown menu showing "User (Read only access to all data)" with a downward arrow.
- Default API Role:** A dropdown menu showing "User (Read only access to all data)" with a downward arrow.
- Allow Data Copy**

At the bottom right of the window are two buttons: "CANCEL" and "SAVE".

**Figure 8**




- **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](#).

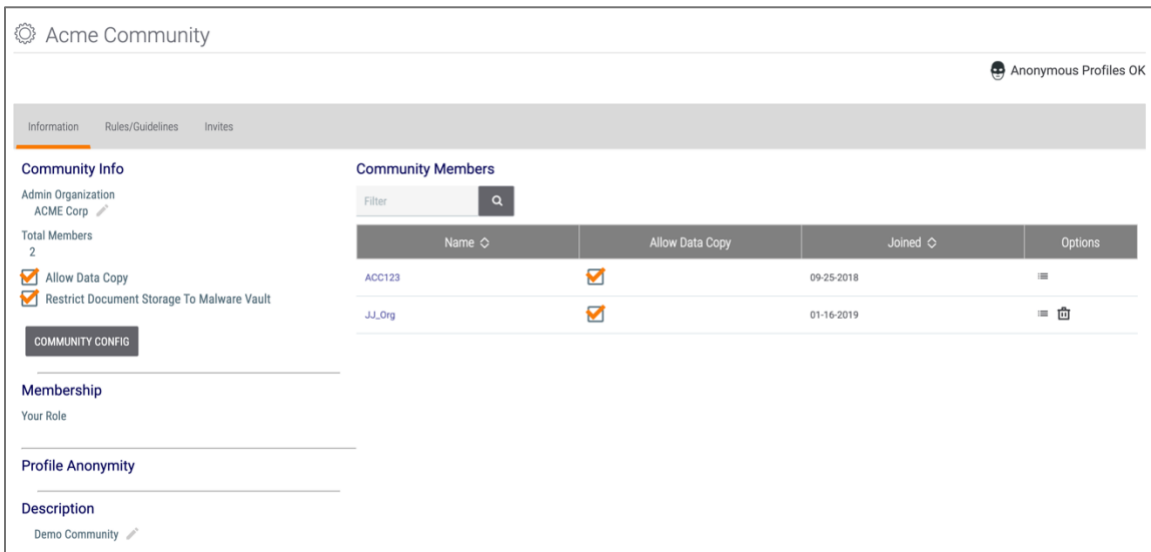
2. Click the **SAVE** button to add the Organizations to the Community.

## 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 9).



Name	Allow Data Copy	Joined	Options
ACC123	<input checked="" type="checkbox"/>	09-25-2018	
JJ_Org	<input checked="" type="checkbox"/>	01-16-2019	

**Figure 9**



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 10).

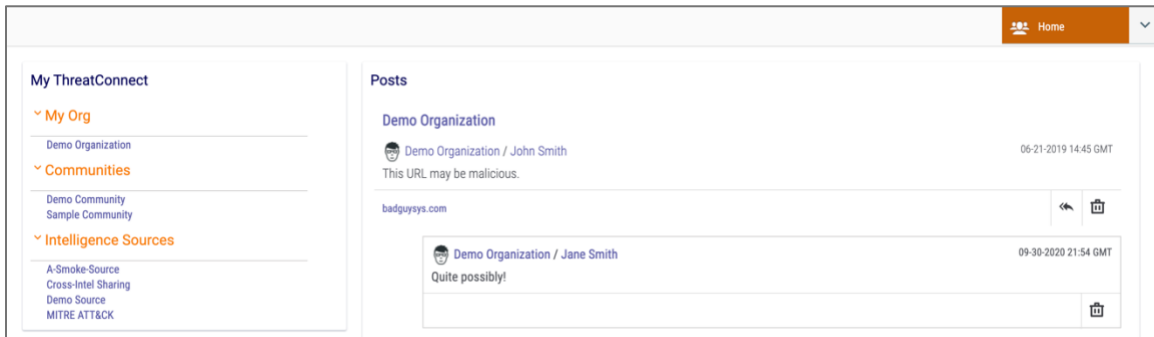


Figure 10

2. Select the desired Community in the **My ThreatConnect** card. The **Posts** screen for the Community will be displayed (Figure 11).

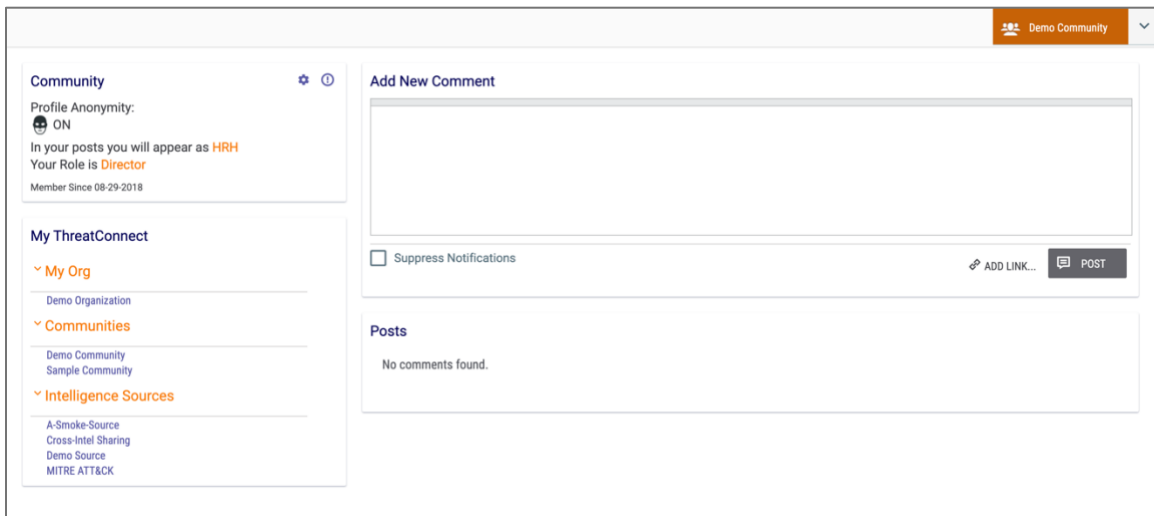



Figure 11

3. Click the **Community Info**  icon at the upper right of the **Community** card. The **Community Info** screen will be displayed (Figure 9).



# 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 6), click the **+ NEW** button. The **Create Community/Source** window will be displayed with the **Community** option selected by default (Figure 7)
2. Select the **Source** radio button. The **Create Community/Source** window will update with options for creating a Source (Figure 12). Use the scroll bar on the right of the screen to access the **Description** text box.

**Create Community/Source**

Type  
 Community  Source

Name

Owner  
Select Owner

Category  
Select Category

Restrict Deletion  
 Allow Data Copy  
 Owner Anonymous  
 Allow Workflow  
 Allow Automated Confidence Deprecation  
 Allow Custom Attributes  
 Allow Custom Security Labels

Allow Feed Email Ingest  
 Allow Phishing Email Ingest  
 Enable Default Expiration

0

Enable Bulk Indicators  
 CSV  
 JSON

Indicator Limit: 50000  
Document Storage Limit: OMB  
Publication Age Limit: 0 day(s)

Description

Tip – Sources allow only sharing from one account to multiple other accounts. The owning organization will administer the source by inviting other accounts to join. All other accounts will have read only access to the data, and zero visibility to each other.

CANCEL SAVE

Figure 12

- **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 [Workflow](#).
- **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 13) displays activity logs within the system, including logins, creations, and deletions.

The screenshot shows the 'Account Settings' page with the 'Activity' tab selected. A dropdown menu is set to 'All'. The table below shows activity logs with columns for 'Summary' and 'Date Added'.

Summary	Date Added
Host catv-80-98-190-53.catv.broadband.hu was deleted by automatic confidence deprecation	08-16-2019 14:11 UTC
Host catv-80-98-18-62.catv.broadband.hu was deleted by automatic confidence deprecation	08-16-2019 14:11 UTC
Host bzzq-79-180-128-146.red.bezeqint.net was deleted by automatic confidence deprecation	08-16-2019 14:11 UTC
Host bypassit.net was deleted by automatic confidence deprecation	08-16-2019 14:11 UTC

Figure 13

If desired, filter the table by selecting activities of interest from the dropdown menu above the **Summary** column (Figure 14).

The screenshot shows the 'Account Settings' page with the 'Activity' tab selected. A dropdown menu is open, showing filter options. The table below shows activity logs with columns for 'Summary' and 'Date Added'.

Summary	Date Added
automatic confidence deprecation	08-16-2019 14:11 UTC
automatic confidence deprecation	08-16-2019 14:11 UTC
automatic confidence deprecation	08-16-2019 14:11 UTC
recation	08-16-2019 14:11 UTC
Host catv-80-98-152-2.catv.broadband.hu was deleted by automatic confidence deprecation	08-16-2019 14:11 UTC

Figure 14

## Logged In Users

The **Logged In Users** tab of the **Account Settings** screen (Figure 15) 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.

The screenshot shows the 'Account Settings' page with the 'Logged In Users' tab selected. The table below shows logged in users with columns for 'User Name', 'Organization', and 'IP'.

User Name	Organization	IP
b@threatconnect.com	BOrg	19.0.0
uatadmin	System	19.0.0

Figure 15



## Owner Roles

The **Owner Roles** tab of the **Account Settings** screen (Figure 16) 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.**

Name	Description			Available	Options
	Organization	Community	Administrator		
User		Read only access to all data	Read only access to all data	✓	✎ 🗑
Commenter		Post creation	Post creation	✓	✎ 🗑
Contributor		Indicator, Group, and Tag creation	Indicator, Group, and Tag creation	✓	✎ 🗑
Editor		Full create and delete access	Full create and delete access	✓	✎ 🗑
Director		Access to administer all data and members	Access to administer all data and members	✓	✎ 🗑
Banned		No access to community	No access to community	✓	✎ 🗑
Subscriber		Read only access to published data only	Read only access to published data only	✓	✎ 🗑
Read Only User	You have read access.		Read only access to all data	✓	✎ 🗑
Standard User	You have full access to modify all data.		Full create and delete access	✓	✎ 🗑
Sharing User	You have full access to modify all data and share it to communities.		Full create, delete, and sharing access	✓	✎ 🗑
Organization Administrator	You have full access to configure your organization.		Access to administer all organization data and members	✓	✎ 🗑
App Developer	You have access to build apps in your organization.		Access to build apps	✓	✎ 🗑
Read Only Commenter	You have read access and can create posts.		Read only access to all data with commenting	✓	✎ 🗑

Figure 16

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 17) 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.

The screenshot shows the 'Account Settings' interface with the 'ThreatAssess' tab selected. Below the navigation tabs, there are buttons for 'GENERAL CONFIG', 'ANALYZE INDICATORS', and '+ NEW'. The main content area displays a table titled 'ThreatAssess Default Organization Overrides' with the following data:

Name	Avg Threat Rating	Avg Confidence Rating	# of Rated Indicators	Credibility/Weight	Default Confidence Rating	Default Threat Rating	Options
API Frozen Source	3.0	57.5	2	1	50	3.00	
Bridge End Source				1	0	0.00	

Figure 17

## 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 18). 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.



Default ThreatAssess Values

General Criticality Observations Organizations Sources Communities Individuals Classifications

Use All False Positives

Exclude False Positives after (days): 365

Weight for CAL Score: 1

Baseline Score: 111

Offset for False Positives: -167

Weight for Instance Score: 1

CANCEL SAVE

Figure 18

2. Select the **Criticality** tab (Figure 19) 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.

Default ThreatAssess Values

General Criticality Observations Organizations Sources Communities Individuals Classifications

Criticality Base Coefficient: 277.78

Criticality Linear Coefficient: 180.55

Criticality Quadratic Coefficient: 20.83

Minimum Score Contribution from Criticality: 0

Maximum Score Contribution from Criticality: 722

CANCEL SAVE

Figure 19

3. Select the **Observations** tab (Figure 20) 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.



The screenshot shows the 'Default ThreatAssess Values' dialog box with the 'Observations' tab selected. The dialog has a close button (X) in the top right corner. Below the title bar is a tabbed interface with tabs for General, Criticality, Observations (selected), Organizations, Sources, Communities, Individuals, and Classifications. The main content area contains several input fields with plus and minus buttons for adjustment:

- Exclude Observations after (days): 365
- Base Coefficient for Observation Points: 55.50
- Linear Coefficient for Observation Points: 55.50
- Minimum Score Contribution from Observations: 0
- Maximum Score Contribution from Observations: 167

At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

Figure 20

4. Select the **Organizations** tab (Figure 21) 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.

The screenshot shows the 'Default ThreatAssess Values' dialog box with the 'Organizations' tab selected. The dialog has a close button (X) in the top right corner. Below the title bar is a tabbed interface with tabs for General, Criticality, Observations, Organizations (selected), Sources, Communities, Individuals, and Classifications. The main content area contains three input fields with plus and minus buttons for adjustment:

- Credibility/Weight: 5
- Default Threat Rating: 0.0
- Default Confidence Rating: 0

At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

Figure 21

5. Select the **Sources** tab (Figure 22) 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.



The screenshot shows a dialog box titled "Default ThreatAssess Values" with a close button (X) in the top right corner. Below the title bar is a horizontal menu with tabs: "General", "Criticality", "Observations", "Organizations", "Sources", "Communities", "Individuals", and "Classifications". The "Sources" tab is currently selected and highlighted with an orange underline. Below the menu, there is a checkbox labeled "Exclude Sources" which is unchecked. Underneath are three input fields, each with a plus (+) and minus (-) button to its right: "Credibility/Weight" with a value of 5, "Default Confidence Rating" with a value of 0, and "Default Threat Rating" with a value of 0.0. At the bottom right of the dialog are two buttons: "CANCEL" and "SAVE".

Figure 22

6. Select the **Communities** tab (Figure 23) 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.

The screenshot shows the same "Default ThreatAssess Values" dialog box, but now the "Communities" tab is selected and highlighted with an orange underline. The "Exclude Sources" checkbox remains unchecked. The input fields are: "Credibility/Weight" with a value of 7, "Default Confidence Rating" with a value of 0, and "Default Threat Rating" with a value of 0.0. The "CANCEL" and "SAVE" buttons are still present at the bottom right.

Figure 23

7. Select the **Individuals** tab (Figure 24) 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.



The screenshot shows a window titled "Default ThreatAssess Values" with a close button (X) in the top right corner. Below the title bar is a horizontal menu with tabs: General, Criticality, Observations, Organizations, Sources, Communities, Individuals, and Classifications. The "Individuals" tab is selected and highlighted with an orange underline. Below the menu, there are three input fields, each with a plus (+) and minus (-) button to its right:

- Credibility/Weight: 0
- Default Confidence Rating: 0
- Default Threat Rating: 0.0

At the bottom right of the window are two buttons: "CANCEL" (white) and "SAVE" (orange).

Figure 24

8. Select the **Classifications** tab (Figure 25) 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.

The screenshot shows the same "Default ThreatAssess Values" window, but with the "Classifications" tab selected and highlighted with an orange underline. The content area is divided into two columns:

Description	Threshold
Description 1 (0 to T1) Low	Threshold 1 (T1) 200
Description 2 (T1 to T2) Medium	Threshold 2 (T2) 500
Description 3 (T2 to T3) High	Threshold 3 (T3) 800
Description 4 (T3 to 1000) Critical	

Each threshold value (200, 500, 800) has a plus (+) and minus (-) button to its right. At the bottom right of the window are two buttons: "CANCEL" (white) and "SAVE" (orange).

Figure 25



## Analyze Indicators

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 17), click the **ANALYZE INDICATORS** button to get current systemwide and owner-specific statistics on an Indicator. The **ThreatAssess/Statistics** screen will be displayed (Figure 26).

ThreatAssess/Statistics

Indicator Name:  Select Type:

**Contributing Sources**

Name of Owner	Org Totals	Credibility/Weight	Threat Rating	Confidence Rating	Criticality
No threat analysis feed organizations found.					

Figure 26

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 27).

ThreatAssess/Statistics

bad.com Host

**Contributing Sources**

Name of Owner	Org Totals	Credibility/Weight	Threat Rating	Confidence Rating	Criticality
Demo Community	0.0MB Storage	7	3.00	95	2.0
Demo Organization	1.0MB Storage	5	3.00	94	2.0
System	5.0MB Storage	5	0.0	0	0.0

Weighted Average Threat Rating: 2.12  
Weighted Average Confidence Rating: 66.76  
Weighted Average Criticality Rating: 1.41  
Overall Score: 431  
Instance Score: 685  
CAL Score: 177  
Score From Criticality: 574  
Score From False Positives: 0  
Score From Observations: 0  
Base Score: 111

Figure 27



## Create ThreatAssess Overrides

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 17), 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 28). 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.

Create ThreatAssess Overrides

Add for a Single Organization Advanced Search

Data Owner  
A-Org

Credibility/Weight  
1

Default Confidence Rating  
0

Default Threat Rating  
0.0

CANCEL SAVE

Figure 28

2. Select the **Advanced Search** tab (Figure 29) to search for data owners that meet the desired criteria for feeds.



Create ThreatAssess Overrides ✕

?

Add for a Single Organization   **Advanced Search**

Minimum Average Threat Rating: 0.00 + -      Type: All ▼ 🔍

Minimum Average Confidence Rating: 0 + -

Minimum Total Rated Indicators: 0 + -

<input type="checkbox"/>	Owner Name	Average Threat Rating	Average Confidence Rating	Total Number of Rated Indicators
--------------------------	------------	-----------------------	---------------------------	----------------------------------

Find organizations for customized ThreatAssess behavior.

i Modify default values for the selected owners.

Credibility/Weight: 1 + -      Default Confidence Rating: 0 + -      Default Threat Rating: 0.0 + -

CANCEL SAVE


Figure 29

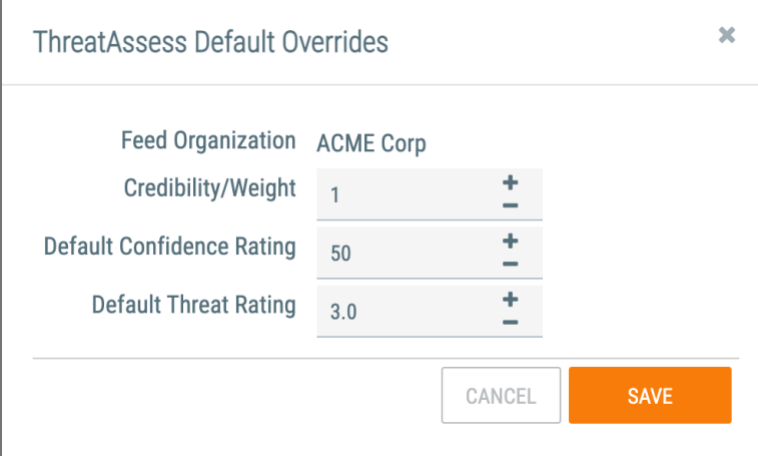
3. Click the **SAVE** button.





## Edit ThreatAssess Overrides

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 17), 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 30).




ThreatAssess Default Overrides		
Feed Organization	ACME Corp	
Credibility/Weight	1	+ -
Default Confidence Rating	50	+ -
Default Threat Rating	3.0	+ -

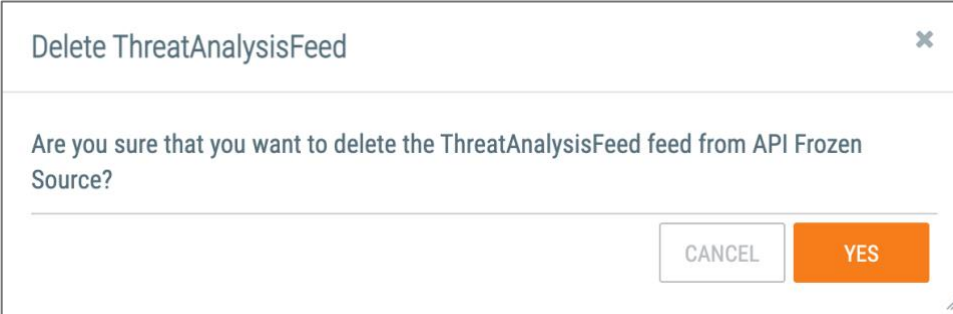
CANCEL SAVE

Figure 30

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 17), 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 31).



Delete ThreatAnalysisFeed

Are you sure that you want to delete the ThreatAnalysisFeed feed from API Frozen Source?

CANCEL YES

Figure 31

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