



# ThreatConnect® Account Administration Guide

Software Version 7.2

Technical Guide

August 24, 2023

10010-19 EN Rev. A



©2023 ThreatConnect, Inc.

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

Farsight Security® is a registered trademark of DomainTools, LLC.

JavaScript® is a registered trademark of Oracle Corporation.



# Table of Contents

<b>Overview</b> .....	<b>4</b>
<b>Accessing the Account Settings Screen</b> .....	<b>5</b>
<b>Organizations Tab</b> .....	<b>5</b>
Create an Organization .....	5
Configure an Organization Account .....	7
Edit or Delete an Organization .....	11
<b>Communities/Sources Tab</b> .....	<b>12</b>
Community Management .....	12
Create a Community .....	12
Edit or Delete a Community .....	15
Add Accounts to a Community .....	15
Perform Other Community Administrative Tasks .....	16
Source Management .....	18
Create a Source .....	18
Other Source Management Options .....	20
<b>Activity</b> .....	<b>21</b>
<b>Logged In Users</b> .....	<b>21</b>
<b>Owner Roles</b> .....	<b>22</b>
<b>ThreatAssess</b> .....	<b>23</b>
Configure Default ThreatAssess Values .....	23
Analyze Indicators .....	28
Create ThreatAssess Overrides .....	29
Edit ThreatAssess Overrides .....	31
Delete ThreatAssess Overrides .....	31
<b>Deprecation Rules</b> .....	<b>32</b>
Create Indicator Confidence Deprecation Rules .....	33
Edit or Delete Indicator Confidence Deprecation Rules .....	35



# Overview


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

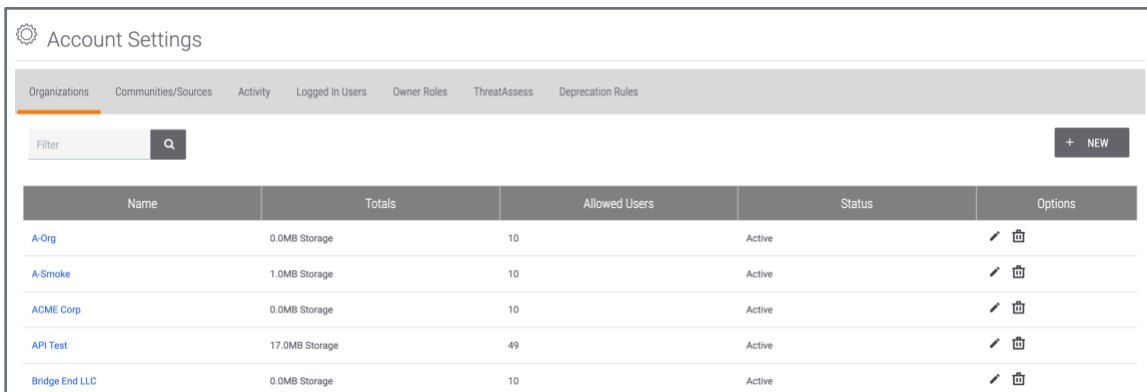
- View, create, modify, and delete Organizations on the ThreatConnect instance
- View, create, modify, and delete Communities and Sources on the ThreatConnect instance
- View and filter all user and data activity on the ThreatConnect instance
- View all users currently logged into the ThreatConnect instance
- 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 **Organizations** tab of the **Account Settings** screen will be displayed (Figure 1).













Name	Totals	Allowed Users	Status	Options
A-Orig	0.0MB Storage	10	Active	 
A-Smoke	1.0MB Storage	10	Active	 
ACME Corp	0.0MB Storage	10	Active	 
API Test	17.0MB Storage	49	Active	 
Bridge End LLC	0.0MB Storage	10	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).

**Important:** 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 features a title bar with the text 'Create Organization' and a close button (X). The form contains the following fields and controls:

- Name \***: A text input field.
- Pseudonym**: A text input field.
- Read-Only**: A checkbox.
- Administrator**: A section header.
- User Name \***: A text input field.
- Password \***: A text input field.
- First Name \***: A text input field.
- Last Name \***: A text input field.

At the bottom right of the form are two buttons: a grey 'CANCEL' button and an orange 'SAVE' button.


**Figure 2**

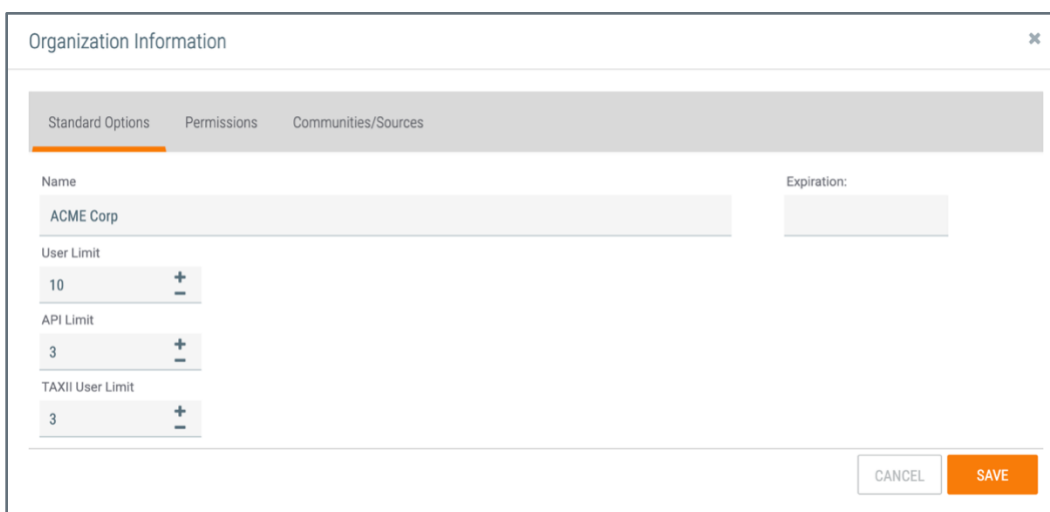
- **Name**: Enter the name of the Organization.
  - **Pseudonym**: Enter a pseudonym for the Organization.
  - **Read-Only**: Select this checkbox to restrict the permissions to read-only status.
  - **User Name**: Enter the User Name for the initial Administrator account. It is recommended that all 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 *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).



**Figure 3**

- **Name:** Modify the Organization account name if desired.
- **User Limit:** Enter the maximum number of users that can exist in an Organization.

**Note:** The default value is 1.

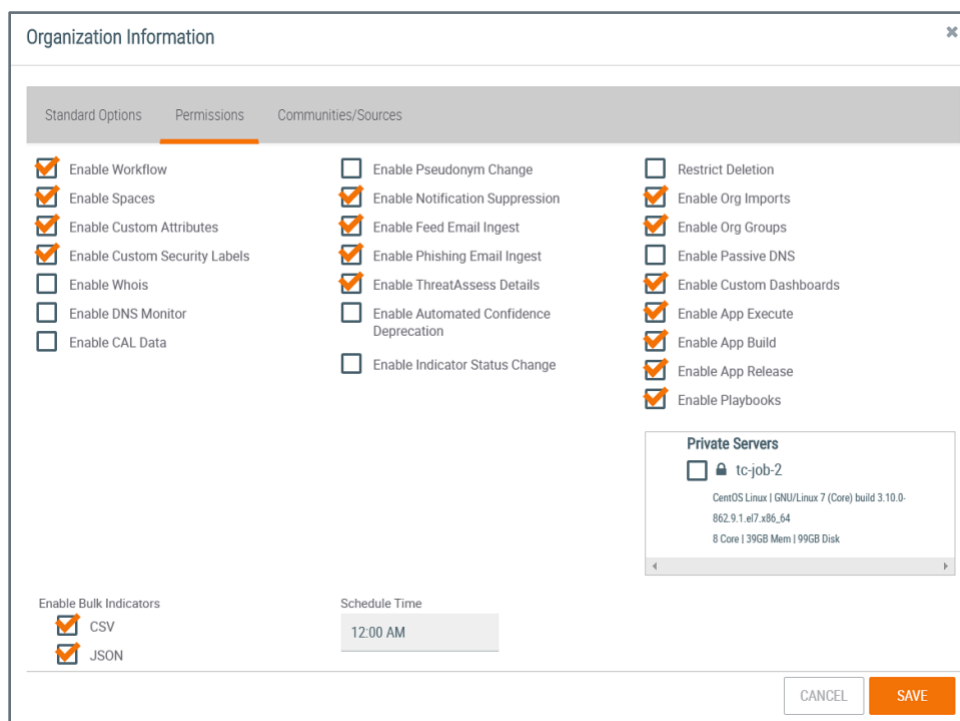
- **API Limit:** Enter the number of API users that can exist within an Organization.
- **TAXII User Limit:** Enter the number of TAXII users that can exist within an Organization.
- **Status:** If an Organization is expired, the **Status** dropdown will be displayed. Select whether the status of the 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.

**Note:** The **ThreatConnect Package** dropdown will not be displayed on Dedicated Cloud and On-Premises ThreatConnect instances.

2. Click the **Permissions** tab to view the **Permissions** screen (Figure 4).




**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 [Domain Name System \(DNS\) 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.

**Important:** 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 [confidence deprecation](#).
- **Enable Indicator Status Change:** Select the checkbox to allow users in the Organization to change the [Indicator Status](#) for an Indicator.
- **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 DNS data service](#). A Farsight Security® API key is required for this feature to work.

**Note:** The visibility of the **Enable Passive DNS** checkbox depends on the configuration of a user's ThreatConnect license.

- **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 the active tab. 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. The right column contains two dropdown menus: "Default Role" and "Default API Role", both set to "Banned (No access to community)". At the bottom left, there is a checkbox labeled "Enable Data Copy" which is currently unchecked. At the bottom right, there 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. See *ThreatConnect Community and Source Administration Guide* and *ThreatConnect Owner Roles and Permissions* for more information about Community and Source roles.
- **Default API Role:** Select the default role that all API accounts in the Organization will be given in the Community or Source.
- **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.

## Edit or Delete an Organization

Click **Edit**  or **Delete**  in the **Options** column to edit or delete an Organization, respectively.



# 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.

The screenshot shows the 'Account Settings' interface with the 'Communities/Sources' tab selected. The table below lists the existing Communities and Sources.

Name	Type	Totals	Owner	Options
<a href="#">A-Org-Community</a>	Community	0.0MB Storage	A-Org	
<a href="#">A-Org-Source</a>	Source	0.0MB Storage	A-Org	
<a href="#">A-Smoke-2-Comm</a>	Community	0.0MB Storage	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). If necessary, scroll down in the window to access the full **Description** text box.



**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.

**Note:** The **Category** dropdown will not be displayed on Dedicated Cloud and On-Premises ThreatConnect instances.

- **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.
- **Allow Feed Email Ingest:** Select the checkbox to allow the Feed Email Ingest feature for the Community.
- **Allow 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 the number of days until 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.

- **Publication Age Limit:** Enter the number of days after which a publication created using the [Publish feature](#) within the Community will be aged off.
- **Description:** Enter an initial description for the Community.




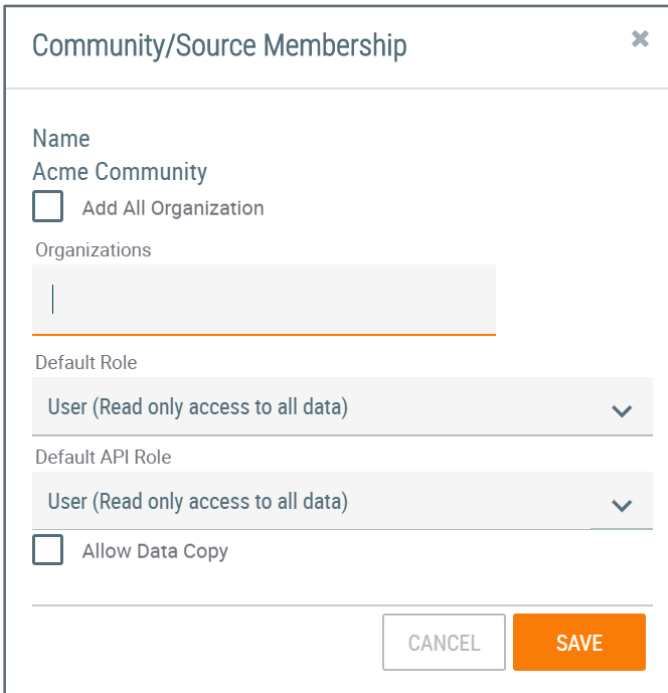
2. Click the **SAVE** button to create the Community. If the new Community is not displayed on the **Communities/Sources** screen, log out and log back into ThreatConnect to refresh the screen.

## Edit or Delete a Community

Click **Edit**  or **Delete**  in the **Options** column to edit or delete a Community, respectively.

## 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).



Community/Source Membership

Name  
Acme Community

Add All Organization

Organizations

Default Role  
User (Read only access to all data)

Default API Role  
User (Read only access to all data)

Allow Data Copy

CANCEL 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. See *ThreatConnect Community and Source Administration Guide* and *ThreatConnect Owner Roles and Permissions* for more information about Community and Source roles and default API roles.
  - **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.

## 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	⋮

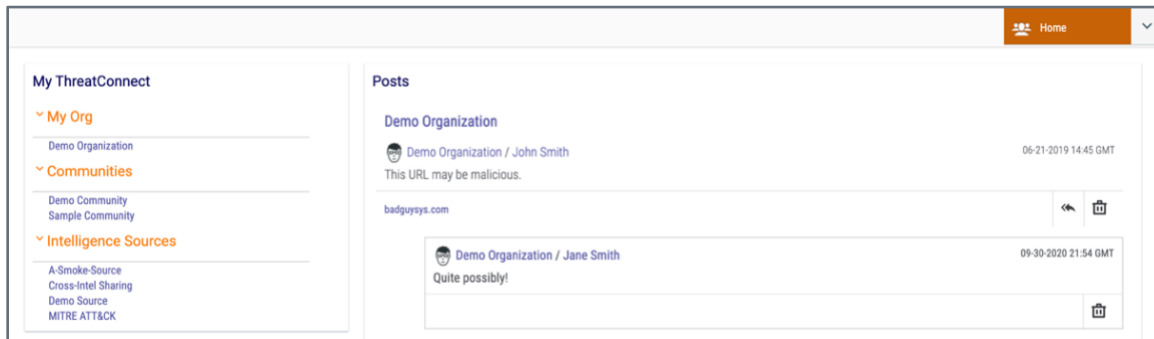
**Figure 9**

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 Guide*.

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

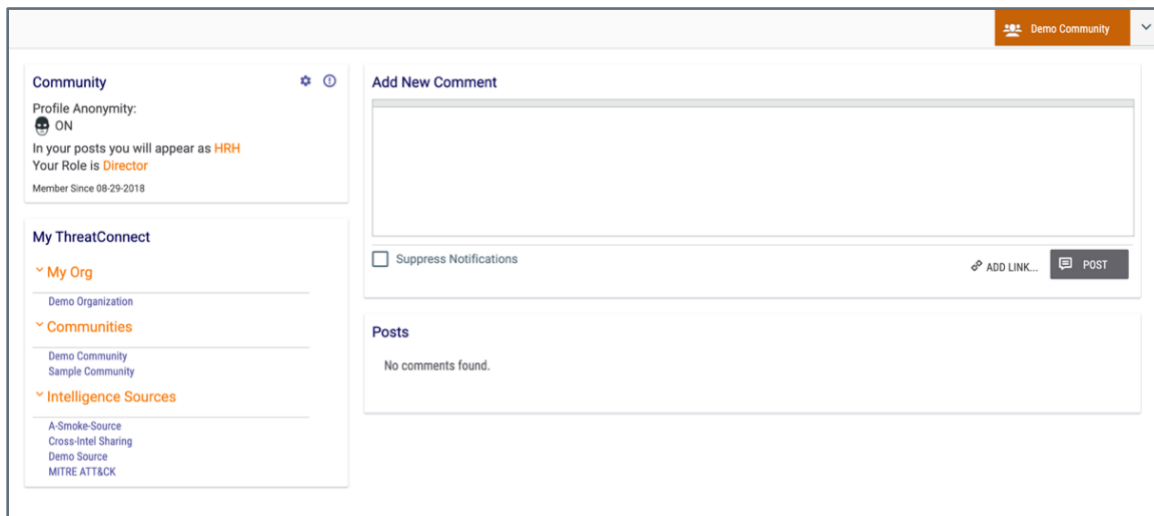


1. On the top navigation bar, click **Posts**. The **Posts** screen will be displayed (Figure 10).




**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

**Important:** 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** [x]

Type  
 Community  Source

Name \*

Owner \*

Select Owner [v]

Restrict Deletion  Allow Feed Email Ingest  
 Allow Data Copy  Allow Phishing Email Ingest  
 Owner Anonymous  Enable Default Expiration  
 Allow Workflow  +  
 Allow Automated Confidence Deprecation  
 Allow Custom Attributes Enable Bulk Indicators  
 Allow Custom Security Labels  CSV  
 JSON

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.



**Note:** The **Category** dropdown will not be displayed on Dedicated Cloud and On-Premises ThreatConnect instances.

- **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 the number of days until 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 Community and their Indicator types. The report will also include each Indicator's Threat Rating and Confidence Rating values, if set, or null otherwise.



- **Publication Age Limit:** Enter the number of days after which a publication created using the [Publish feature](#) within the Source will be aged off.
  - **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 or Delete a Community,” “Add Accounts to 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' interface with the 'Activity' tab selected. A dropdown menu is set to 'All'. Below is a table with two columns: 'Summary' and 'Date Added'.

Summary	Date Added
User Douglas Jones logged in 171.12.0.5	06-29-2022 11:54 UTC
Host karenbrownrx.com had a DNS Change to 63.141.242.45	06-29-2022 11:47 UTC
Host neobake.com had a DNS Change to 52.86.6.113	06-29-2022 11:45 UTC
Host neobake.com had a DNS Change to 3.94.41.167	06-29-2022 11:45 UTC

**Figure 13**

If desired, filter the table by selecting activities of interest from the dropdown menu displayed above the **Summary** column.

# Logged In Users

The **Logged In Users** tab of the **Account Settings** screen (Figure 14) 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' interface with the 'Logged In Users' tab selected. Below is a table with three columns: 'User Name', 'Organization', and 'IP'.

User Name	Organization	IP
djones	Demo Organization	171.12.0.5
jsmith	ACME Corp	19.0.8.1

**Figure 14**



# Owner Roles

The **Owner Roles** tab of the **Account Settings** screen (Figure 15) 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.

Name	Description		Available	Options	
	Organization	Community			
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 15**

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 (i.e., a user's owner role within a Community or Source)
- 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 on the [Details drawer](#) and [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 16) 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' page with the 'ThreatAssess' tab selected. Below the navigation bar are buttons for 'GENERAL CONFIG', 'ANALYZE INDICATORS', and '+ NEW'. The main content is 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	[Edit] [Delete]
Bridge End Source				1	0	0.00	[Edit] [Delete]

Figure 16

## 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 17). 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.



The screenshot shows the 'Default ThreatAssess Values' configuration window with the 'General' tab selected. The window has a title bar with a close button (X) and a tabbed interface with the following tabs: General, Criticality, Observations, Organizations, Sources, Communities, Individuals, and Classifications. The 'General' tab is active and contains the following settings:

- Use All False Positives
- Exclude False Positives after (days): 365
- Offset for False Positives: -167
- Weight for CAL Score: 1
- Weight for Instance Score: 1
- Baseline Score: 111

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

Figure 17

2. Select the **Criticality** tab (Figure 18) 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.

The screenshot shows the 'Default ThreatAssess Values' configuration window with the 'Criticality' tab selected. The window has a title bar with a close button (X) and a tabbed interface with the following tabs: General, Criticality, Observations, Organizations, Sources, Communities, Individuals, and Classifications. The 'Criticality' tab is active and contains the following settings:

- 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

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

Figure 18

3. Select the **Observations** tab (Figure 19) 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.



The screenshot shows the 'Default ThreatAssess Values' dialog box with the 'Observations' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: General, Criticality, Observations (selected), Organizations, Sources, Communities, Individuals, and Classifications. The 'Observations' tab contains the following settings:

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 two buttons: 'CANCEL' and 'SAVE'.

**Figure 19**

4. Select the **Organizations** tab (Figure 20) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for Organizations. Enter the desired value for each option.

The screenshot shows the 'Default ThreatAssess Values' dialog box with the 'Organizations' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: General, Criticality, Observations, Organizations (selected), Sources, Communities, Individuals, and Classifications. The 'Organizations' tab contains the following settings:

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

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

**Figure 20**

5. Select the **Sources** tab (Figure 21) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for Sources. Enter the desired value for each option. 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 tabbed interface with the following tabs: General, Criticality, Observations, Organizations, Sources, Communities, Individuals, and Classifications. The "Sources" tab is currently selected and highlighted with an orange underline. Below the tabs, there is a checkbox labeled "Exclude Sources" which is unchecked. Underneath, there are three numerical 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 box are two buttons: "CANCEL" and "SAVE".

**Figure 21**

6. Select the **Communities** tab (Figure 22) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for Communities. Enter the desired value for each option.

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 numerical 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 22**

7. Select the **Individuals** tab (Figure 23) to configure the **Credibility/Weight**, **Default Threat Rating**, and **Default Confidence Rating** options for individuals. Enter the desired value for each option.



The screenshot shows the 'Default ThreatAssess Values' dialog box with the 'Individuals' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: General, Criticality, Observations, Organizations, Sources, Communities, Individuals (selected), and Classifications. Below the tabs, there are three input fields, each with a '+' and '-' button:

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

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

**Figure 23**

8. Select the **Classifications** tab (Figure 24) 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.

The screenshot shows the 'Default ThreatAssess Values' dialog box with the 'Classifications' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: General, Criticality, Observations, Organizations, Sources, Communities, Individuals, and Classifications (selected). Below the tabs, there are four rows, each with a description and a threshold value:

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	

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

**Figure 24**



# Analyze Indicators

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 16), click the **ANALYZE INDICATORS** button to get current systemwide and owner-specific statistics on an Indicator. The **ThreatAssess/Statistics** screen will be displayed (Figure 25).

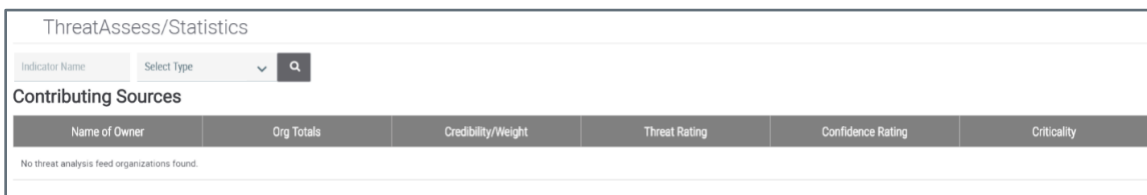


Figure 25

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 26).

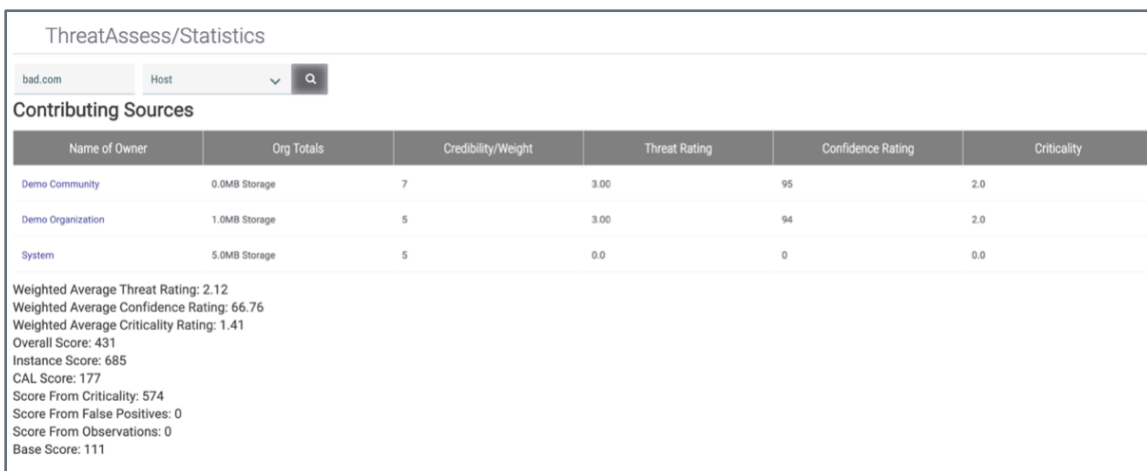


Figure 26



## Create ThreatAssess Overrides

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 16), 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 27). 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.

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 27**

2. Select the **Advanced Search** tab (Figure 28) 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

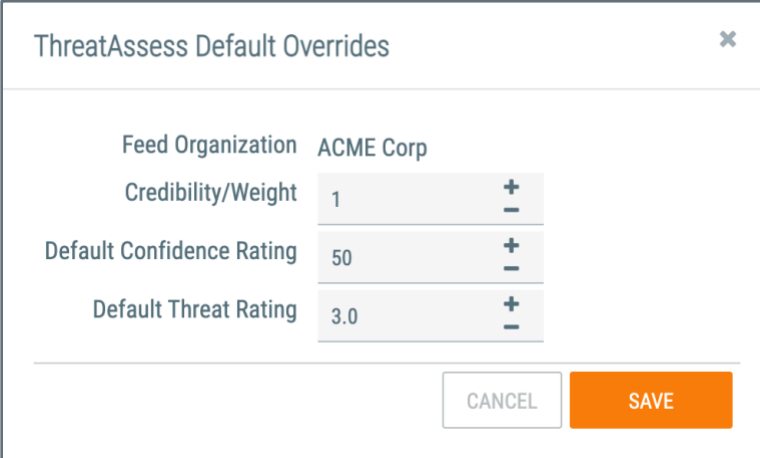
Figure 28

3. Click the **SAVE** button.



## Edit ThreatAssess Overrides

1. From the **ThreatAssess** tab of the **Account Settings** screen (Figure 16), 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 29).




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

CANCEL SAVE

**Figure 29**

2. The following values may be edited: **Credibility/Weight**, **Default Confidence Rating**, and **Default Threat Rating**. Enter the desired value for each option.
3. Click the **SAVE** button.

## Delete ThreatAssess Overrides

From the **ThreatAssess** tab of the **Account Settings** screen (Figure 16), click **Delete**  for an entry in the table to delete the ThreatAssess default overrides for that owner. The **Delete ThreatAnalysisFeed** window will be displayed. Click **YES** to delete the overrides for the selected owner.



# Deprecation Rules

Indicator confidence deprecation is a great way to allow Indicators to drop in [Confidence Rating](#) over time or be deleted if the Confidence Rating is not being maintained and updated. Confidence deprecation is used in the case of an Indicator, such as an IP Address, that is no longer being used for any malicious activity for a certain amount of time. Depending on the confidence deprecation rule, ThreatConnect will drop the Confidence Rating or delete the Indicator, assuming that the Indicator is dormant or that the threat actor has ceased using it. ThreatConnect allows the creation of confidence deprecation rules at the System, Organization, Community, and Source levels.

The **Deprecation Rules** tab of the **Account Settings** screen (Figure 30) allows System Administrators and Operations Administrators to configure System-wide confidence deprecation rules for Indicators. When configuring a System-wide confidence deprecation rule, users can choose which owner types (i.e., Organizations, Communities, or Sources) the rule will be applied to automatically when an owner of the selected type(s) is created, as well as whether to begin confidence deprecation for Indicators of a selected type from the time the rule is saved or from the date when Indicators were [last modified](#).

**Important:** System-wide confidence deprecation rules for a given Indicator type that are applied to an owner type will be overridden if a confidence deprecation rule for that same Indicator type is created in an owner of that type. See [Configuring Indicator Confidence Deprecation](#) for more information on creating confidence deprecation rules in Organizations, Communities, and Sources.

Name	Applies to Community	Applies to Source	Applies to Org	Indicator Type	Interval	Amount	Percentage	Recurring	Action At Minimum	Options
Address Deprecation Rule	true	true	true	Address	2 days	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inactive	
Host Deprecation Rule	true	true	false	Host	3 days	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete	
URL Deprecation Rule	false	false	true	Host	2 days	5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	None	

Figure 30



## Create Indicator Confidence Deprecation Rules

Click the + **NEW** button on the **Deprecation Rules** screen (Figure 30). The **Create/Edit System Deprecation Rule** window will be displayed (Figure 31).

**Figure 31**

- **Name:** Enter a name for the deprecation rule. Note that this is a required field.
- **Description:** Enter a description of the deprecation rule. Note that this is a required field.
- **Indicator Type:** Select the type of Indicator to which the deprecation rule is to apply.
- **Confidence:** Enter the amount by which the Confidence Rating for Indicators of the selected type should decrease if not updated by a ThreatConnect user.
- **Percentage:** Select this checkbox to use the value entered in the **Confidence** box as a percentage instead of a numerical value. For example, if the **Confidence** is 5 and the **Percentage** checkbox is cleared, the Confidence Rating will drop by a value of 5



(e.g., from 60 to 55) when it is deprecated. If the **Confidence** is 5 and the **Percentage** checkbox is selected, the Confidence Rating will drop by 5% (e.g., from 60 to 57).

- **Action at Minimum:** Select the action to take when the Confidence Rating for an Indicator of the selected type drops to 0. Available options include the following:
  - **None:** Select this option to take no action when the Confidence Rating for an Indicator of the selected type drops to 0.
  - **Set Inactive:** Select this option to set the [Indicator Status](#) for an Indicator of the selected type to inactive when its Confidence Rating drops to 0. When this option is selected, a **CAL Status Lock** checkbox will be displayed. Select this checkbox to prevent CAL from changing the Indicator Status for an Indicator back to active.
  - **Delete:** Select this option to delete an Indicator of the selected type when its Confidence Rating drops to 0.
- **Interval:** Enter the number of days after which the Confidence Rating should decrease if not updated by a ThreatConnect user (i.e., the number of days after the date when the Indicator was [last modified](#)).
- **Recurring:** Select this checkbox for the deprecation rule to be applied on a recurring basis instead of just once.
- **Initialize Deprecation from:** Select when to initialize the confidence deprecation rule. Available options include the following:
  - **Last Modified Date:** Select this option to initialize confidence deprecation from the date when Indicators of the selected type were [last modified](#). For existing Indicators, confidence deprecation will occur retroactively from that date.
  - **Time of Save:** Select this option to initialize confidence deprecation from the time the rule is saved. For existing Indicators, confidence deprecation will occur from that time.
- **Apply to New:** Select the type of owner(s) to which the deprecation rule should be applied automatically when an owner of the selected type(s) is created.
- Click the **SAVE** button.

**Note:** System-wide deprecation rules created on the **Deprecation Rules** tab of the **Account Settings** screen will be applied only to newly created owners of type(s) selected in the **Apply to New** section of the **Create/Edit System Deprecation Rule** window. For instructions on using a



System-wide deprecation rule as a template when creating an owner-level rule, see [Configuring Indicator Confidence Deprecation](#).

**Important:** Only one confidence deprecation rule for an Indicator type that applies to the owner type(s) selected in the **Apply to New** section of the **Create/Edit System Deprecation Rule** window can be created. Attempts to create a second rule for an Indicator type that applies to the same owner type(s) selected in the **Apply to New** section of the **Create/Edit System Deprecation Rule** window will result in an error.

## Edit or Delete Indicator Confidence Deprecation Rules

Click **Edit**  or **Delete**  in the **Options** column to edit or delete a confidence deprecation rule, respectively.