ThreatConnect® Community and Source Administration Guide

Software Version 7.7

Technical Guide

September 18, 2024

10011-23 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

In ThreatConnect, all threat intelligence data objects have an owner. Owners have full control over their data, and they fall under one of the following three categories: Organization, Community, and Source. Communities and Sources both consist of member Organizations, where the users in a member Organization are also members of the Community or Source.

This guide provides instruction on Community and Source administration and configuration. including the following topics:

- Owner roles:
  - Definitions of the available owner roles in Communities and Sources
  - How to configure default owner roles for member Organizations
  - How to configure owner roles for individual user accounts in a member Organization
- **Community Info** screen and **Source Info** screen
  - How to access the **Community Info** screen and **Source Info** screen
  - How to configure Community and Source information, rules and guidelines, and invitation options
- **Community Config** screen and **Source Config** screen
  - How to access the **Community Config** screen and **Source Config** screen
  - How to configure Attribute Types, Attribute Validation Rules, Attribute Preferences, Indicator Exclusion Lists, and deprecation rules for Indicator Confidence Rating in a Community or Source
  - How to view, download, and delete JavaScript® Object Notation (JSON) files published in a Community or Source
  - How to configure HTTP Feeds and Trusted Automated eXchange of Indicator Information (TAXII™) Exchange Feeds in a Community or Source
  - How to create phishing and feed mailboxes in a Community or Source
  - How to add a DomainTools® API key to enable DomainTools for all Reverse Whois Track queries for a Community or Source

Community and Source Roles

A user's Community role determines the permissions they have within a Community or Source. Table 1 defines each Community role.

Note: Community roles apply to Sources as well, but, for simplicity, the roles for both owner types are collectively referred to as Community roles.

Table 1

Role	Definition
User	Users that can only view existing data in a Community or Source.
Contributor	Users that can view existing data, create and reply to Posts, and create Indicators, Groups, and Tags in a Community or Source.
Commenter	Users that can view existing data and create and reply to Posts in a Community or Source.
Editor	Users that can view, create, and delete data (i.e., Posts and threat intelligence), as well as edit threat intelligence, in a Community or Source. **Important**: Editors in a Source will not be able to update the Threat Rating and Confidence Rating of Indicators in that Source unless they are a member of the Organization that owns the Source.
Director	Users that can view, create, and delete data (i.e., Posts and threat intelligence), edit threat intelligence, and administrate members in a Community or Source.
Banned	Users that have no access at all to a Community or Source.
Subscriber	Users that can only view published data from a Community or Source.

Configure Community and Source Roles

Users with a Community role of Director in a Community or Source can configure the default Community role for all users in member Organizations, as well as configure the Community role for individual users in a member Organization.

> **Note**: Communities are configured as either **ANONYMOUS** (all users are anonymous and are identified by their pseudonym) or **FULL PROFILE** (all users are identified by their full user profile). See the "Community Management" section of *ThreatConnect Account Administration Guide* for more information. Sources do not provide this option, but are configured to have the name of their owner Organization be anonymous or available. See the "Source Management" section of *ThreatConnect Account Administration Guide* for more information.

Follow these steps to configure Community roles for member Organizations and individual users in a member Organization in a Community or Source:

1. Log into ThreatConnect with a user account that has a Community role of Director in the Community or Source.
2. On the top navigation bar, click **Posts** to display the **Posts** screen.
3. Select the Community or Source in the **My ThreatConnect** card on the **Posts** screen to display its **Community** (Figure 1) or **Source** (Figure 2) screen. The **Community** or **Source** card displayed at the upper-left corner of each screen provides information about the selected Community or Source and two icons: **Community** (or **Source**) **Info** and **Community** (or **Source**) **Config** . See the "The Community (or Source) Info Screen" and "The Community (or Source) Config Screen" section, respectively, for more information about these screens.

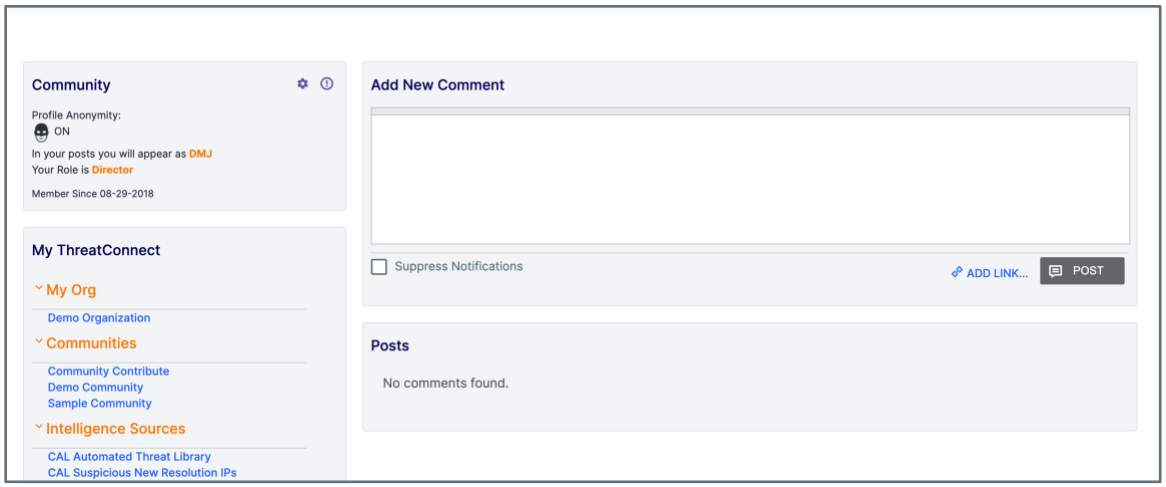

Figure 1

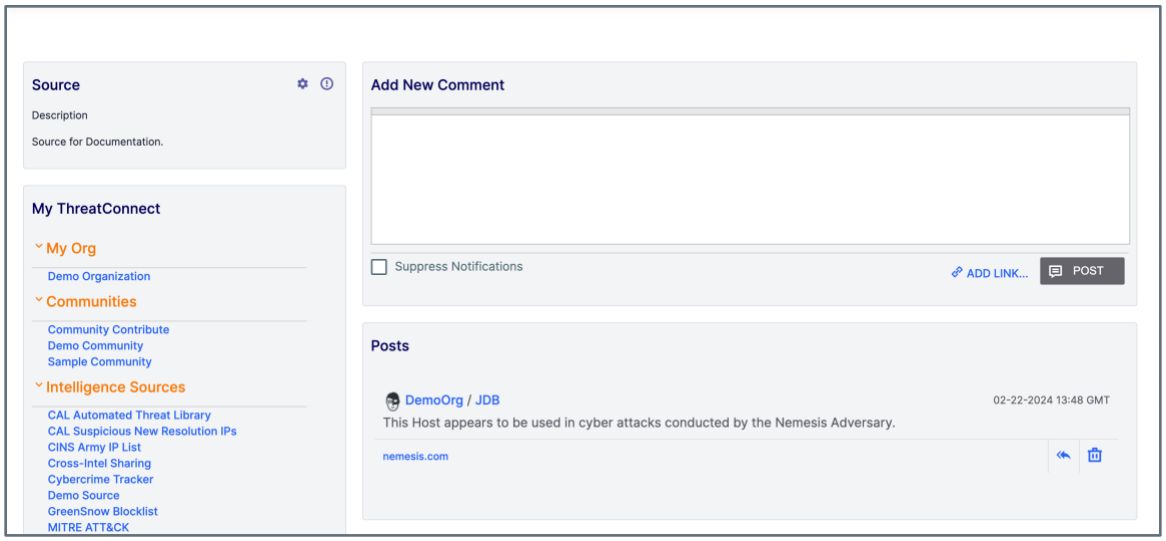

Figure 2

4. Click **Community** (or **Source**) **Info** at the upper-right corner of the **Community** (or **Source**) card to display the **Community Info** (Figure 3) or **Source Info** screen (Figure 4), respectively.

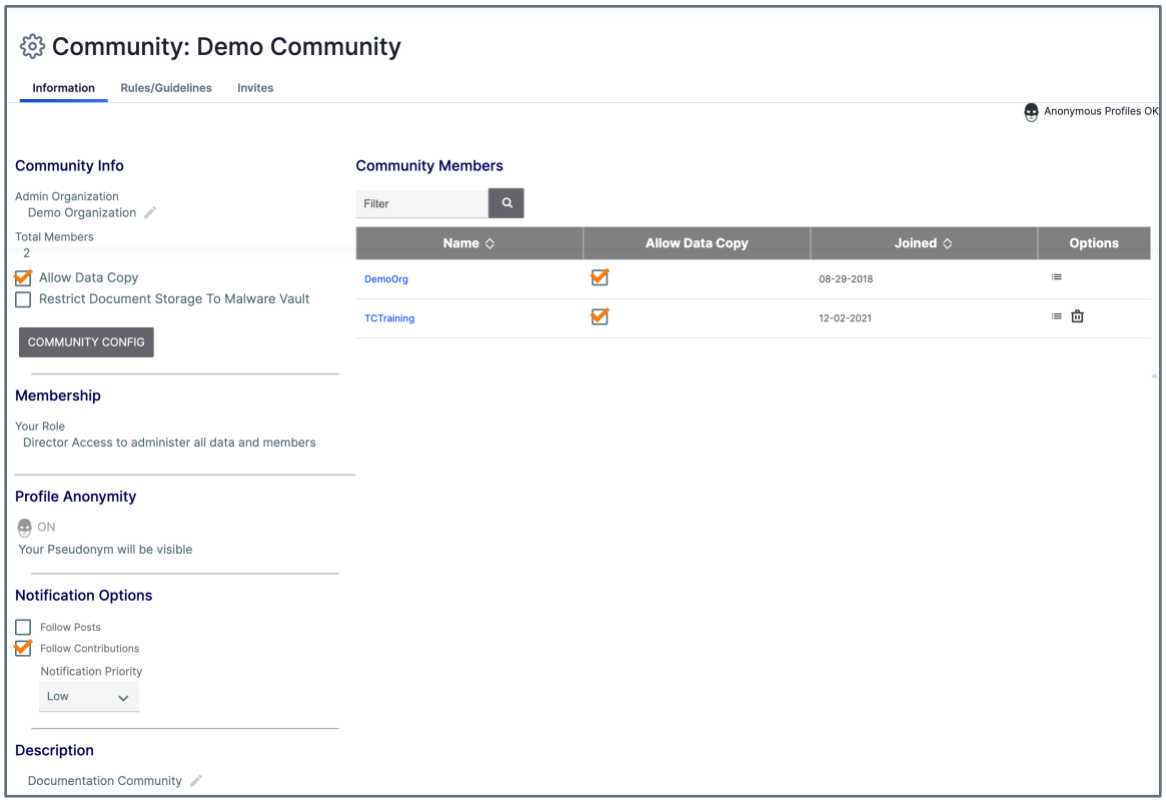

Figure 3

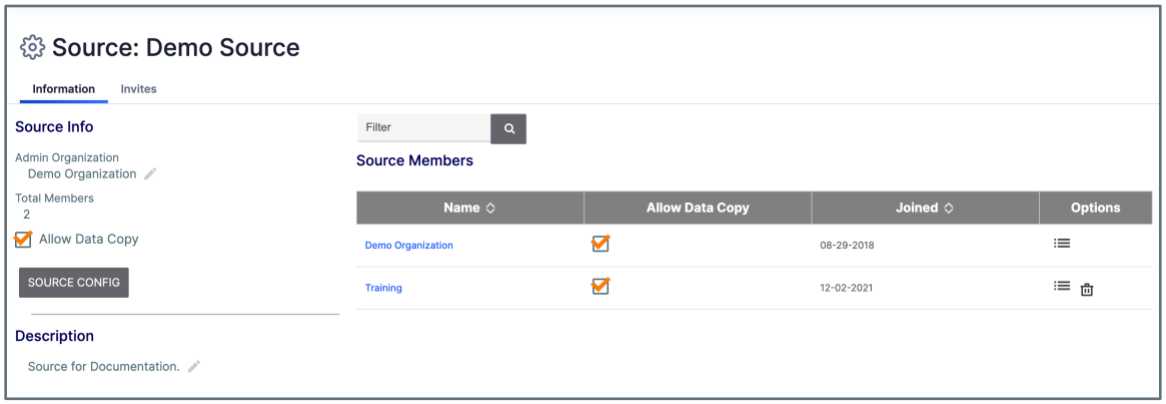

Figure 4

5. Click **Users** ☰ in the **Options** column to display the **Membership** window (Figure 5), which provides options for configuring Community roles for the corresponding member Organization and its users.

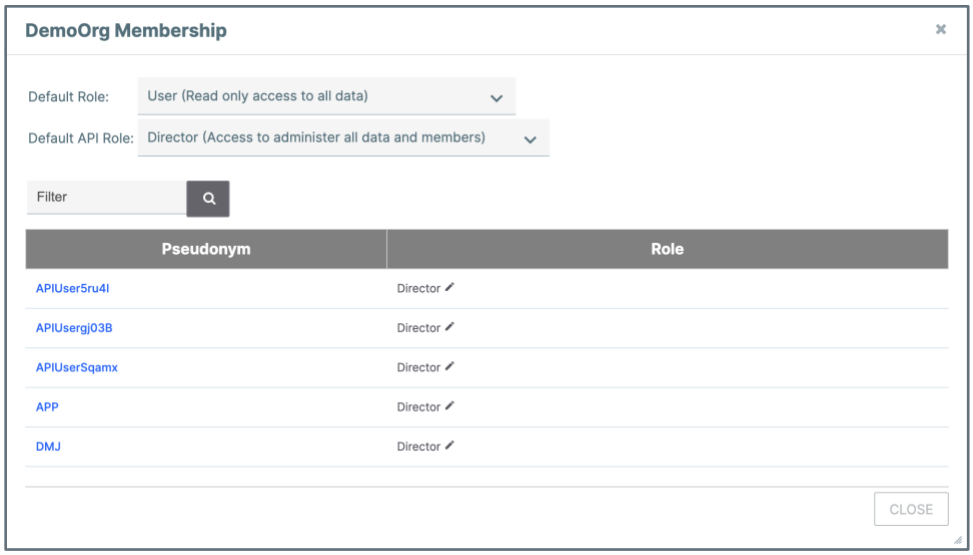

Figure 5

- **Default Role**: Select the default Community role for future users in the member Organization.
- **Default API Role**: Select the default Community role for all future API user accounts created in the member Organization.
- **Role** (of Individual Users): Click **Edit** to the right of a user's role to change their role.
- Click **CLOSE**.

The Community (or Source) Info Screen

The **Community** (or **Source**) **Info** screen is where Community (or Source) Editors and Directors can view and configure information about the Community or Source, including member Organizations, the administrating Organization, and whether member users can copy data from the Community or Source into their Organization; rules and guidelines (for Communities only); and invitations to new users.

Access the Community (or Source) Info Screen from Posts

Follow these steps to access the **Community Info** for a Community or the **Source Info** screen for a Source from the **Posts** screen:

1. Log into ThreatConnect with a user account that has a Community role of Editor or Director in the Community or Source.
2. On the top navigation bar, click **Posts** to display the **Posts** screen.
3. Select the Community or Source in the **My ThreatConnect** card on the **Posts** screen to display its **Community** (Figure 1) or **Source** (Figure 2) screen.
4. Click **Community** (or **Source**) **Info** at the upper-right corner of the **Community** or **Source** card to display the **Community Info** (Figure 6) or **Source Info** screen (Figure 7), respectively. The following features are available on the **Information** tab of the **Community Info** and **Source Info** screen:

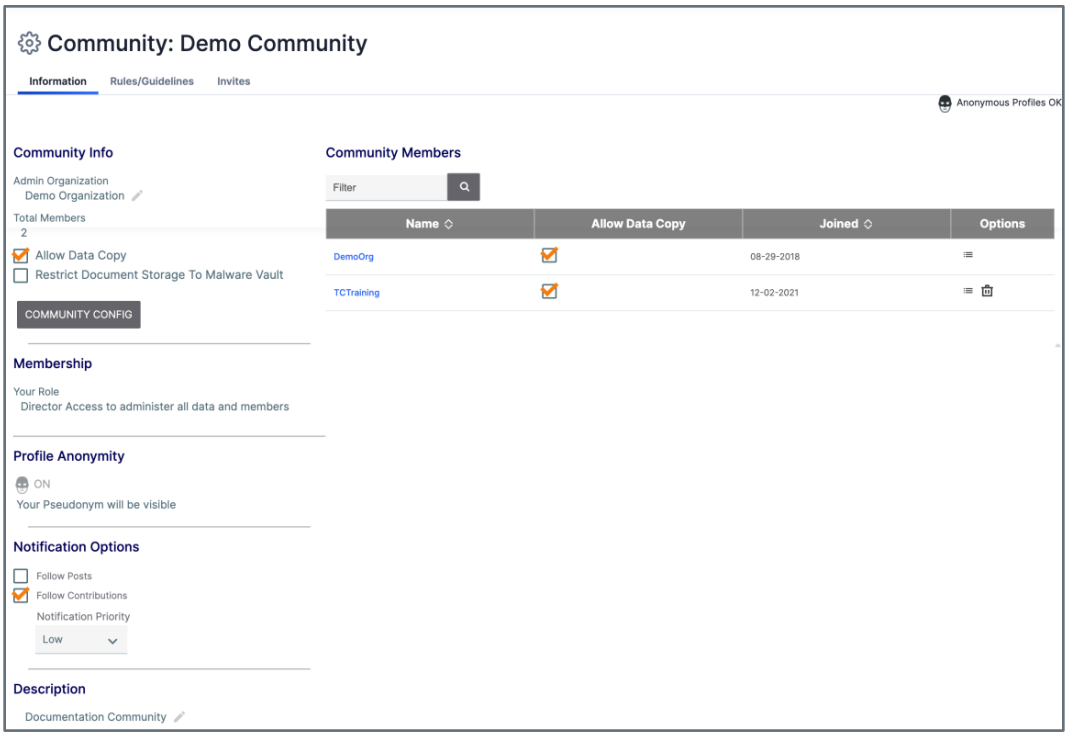

Figure 6

- **Admin Organization**: Click **Edit** to display a dropdown from which you can select the Organization that administrates the Community.
- **Allow Data Copy**: Select this checkbox to allow members of the Community to copy data from the Community into their Organization.
- **Restrict Document Storage to Malware Vault**: Select this checkbox to enforce this restriction in three instances: when uploading a document when creating a Document Group, when uploading a file on the **Document File** card of a Document Group's **Details** screen, and when using the API to upload a document file in a Document Group in a Community.
- **Follow Posts**: Select this checkbox to follow posts in the Community.
- **Follow Contributions**: Select this checkbox to follow contributions to the Community.
- **Notification Priority**: Select the priority for notifications on followed items in the Community.
- **Description**: Click **Edit** to edit the Community's description.

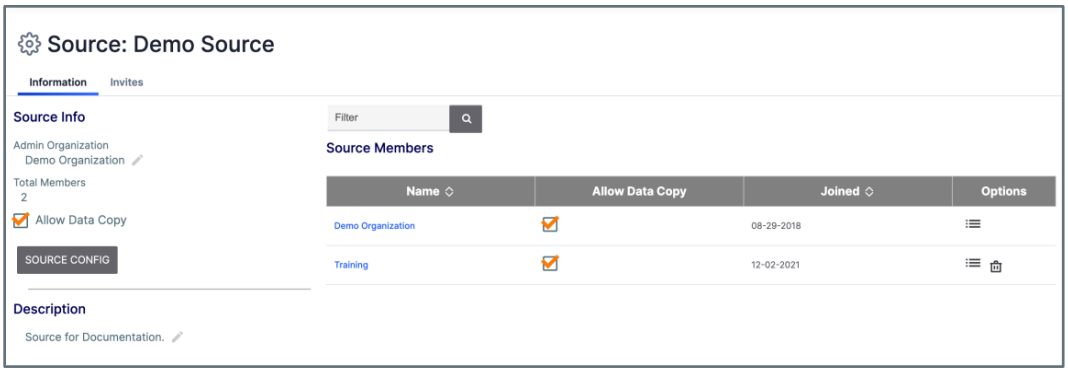

Figure 7

- **Admin Organization**: Click **Edit** to display a dropdown from which you can select the Organization that administrates the Source.
- **Allow Data Copy**: Select this checkbox to allow members of the Source to copy data from the Source into their Organization.
- **Description**: Click **Edit** to edit the Source's description.

Access the Community (or Source) Info Screen from Account Settings

Follow these steps to access the **Community Info** for a Community or the **Source Info** screen for a Source from the **Account Settings** screen:

1. Log into ThreatConnect with a System Administrator, Operations Administrator, or Accounts Administrator account.
2. On the top navigation bar, hover over **Settings** and select **Account Settings** to display the **Account Settings** screen.
3. Select the **Communities/Sources** tab to display the **Communities/Sources** screen (Figure 8).

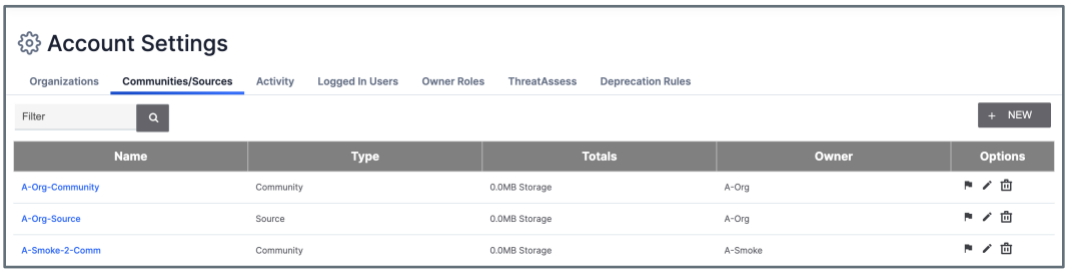

Figure 8

4. Select a Community or Source to display its **Community Info** (Figure 6) or **Source Info** (Figure 7) screen, respectively.

Rules/Guidelines

Follow these steps to view and manage the rules and guidelines for a Community:

1. Navigate to the **Community Info** screen (Figure 6).
2. Click the **Rules/Guidelines** tab (Figure 9).

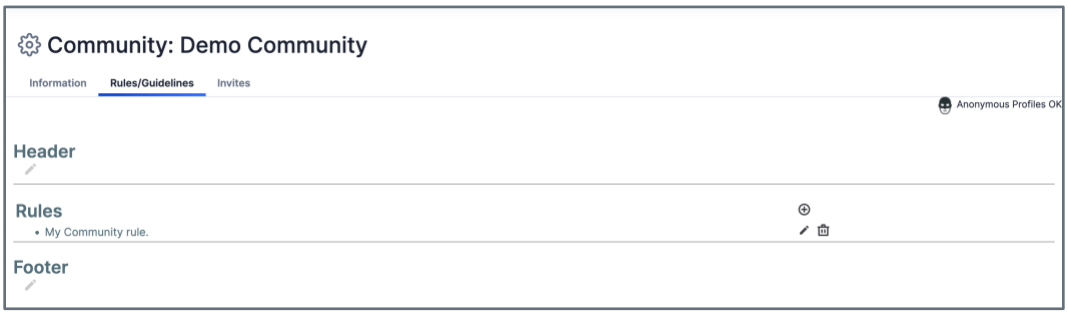

Figure 9

- **Header**: Click **Edit** to create or edit a header for the Community rules and guidelines.
- **Rules:** For existing rules, click **Edit** or **Delete** to edit or delete a rule, respectively. To add a new rule to the Community, click **New Rule**. The **Create Community Rule** window will be displayed (Figure 10).

Figure 10

- **Order:** Community rules are displayed in numerical order. Enter a number for the rule's place in the order.
- **Text:** Enter the contents of the Community rule.

- Click **SAVE**.

- **Footer**: Click **Edit** to create or edit a footer for the Community rules and guidelines.

Invites

In order for an Organization and its members to join a Community or Source, an Organization Administrator for the Organization must receive and accept an invitation from a user with a Community role of Director in the Community or Source. Organization Administrators may view and accept Community and Source invitations on the **Invitations** tab of the **Organization Settings** screen. See the "Invitations" section of *ThreatConnect Organization Administration Guide* for more information. Once an Organization Administrator has accepted an invitation, the Organization will be a member of the Community or Source, and all members of the Organization will automatically become members of the Community or Source.

Invite Users to a Community

Follow these steps to invite an Organization to become a member of a Community:

1. Navigate to the **Community Info** screen (Figure 6).
2. Click the **Invites** tab (Figure 11).

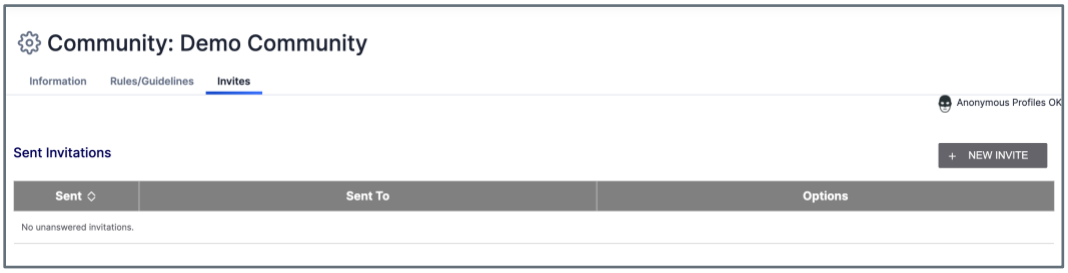

Figure 11

3. Click **+ NEW INVITE** to display the **Send Community Invite** window (Figure 12).

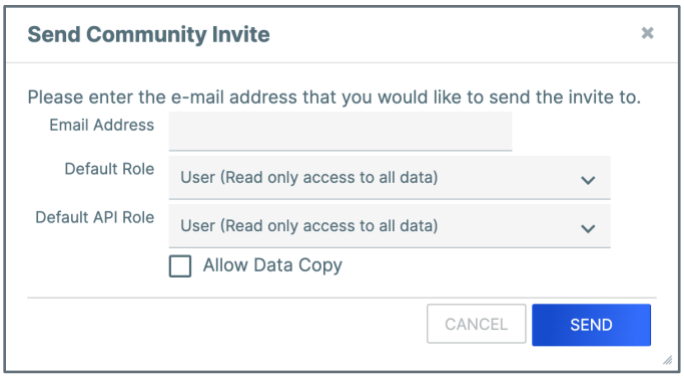

Figure 12

- **Email Address**: Enter the email address for an Organization Administrator in the Organization.

  Important: If the email address is not currently associated with a ThreatConnect user account, the recipient will be able to use the invite code provided in the email to join the Community after a user account with an Organization role of Organization Administrator on the instance has been created for them.

- **Default Role**: Select the default Community role for members of the Organization.
- **Default API Role:** Select the default Community role for API users in the Organization.
- **Allow Data Copy**: Select this checkbox to allow members of the Organization to copy data from the Community into the Organization.
- Click **SEND**.

Invite Users to a Source

Follow these steps to invite an Organization to become a member of a Source:

1. Navigate to the **Source Info** screen (Figure 7).
2. Click the **Invites** tab (Figure 13).

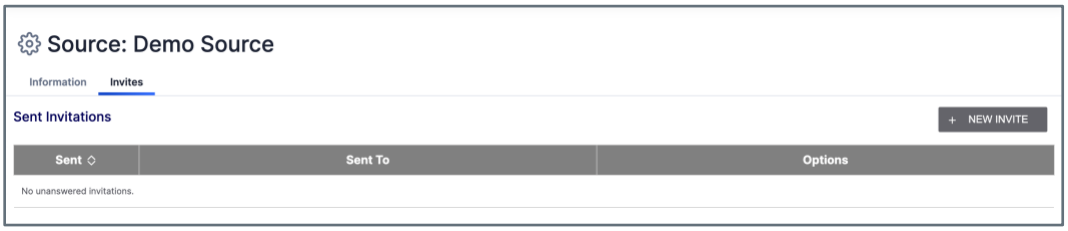

Figure 13

3. Click **+ NEW INVITE** to display the **Send Source Invite** window (Figure 14).

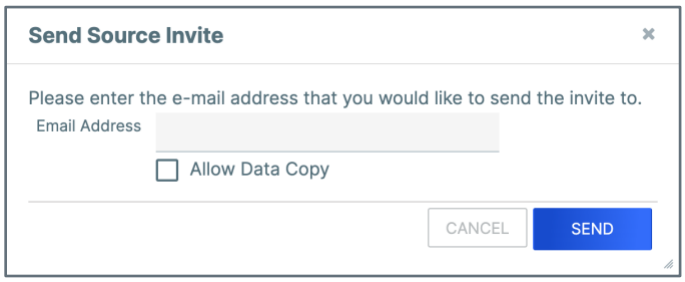

Figure 14

- **Email Address**: Enter the email address for an Organization Administrator in the Organization.

  Important: If the email address is not currently associated with a ThreatConnect user account, the recipient will be able to use the invite code provided in the email to join the Source after a user account with an Organization role of Organization Administrator on the instance has been created for them.

- **Allow Data Copy**: Select this checkbox to allow members of the Organization to copy data from the Source into the Organization.
- Click **SEND**.

The Community (or Source) Config Screen

The **Community** (or **Source**) **Config** screen is where Community (or Source) Editors and Directors can customize how data in the Community or Source are labeled and acted upon.

Access the Community (or Source) Config Screen

Follow these steps to view the **Community** (or **Source**) **Config** screen:

1. Log into ThreatConnect with a user account that has a Community role of Editor or Director in the Community or Source.
2. On the top navigation bar, click **Posts** to display the **Posts** screen.
3. Select the Community or Source in the **My ThreatConnect** card on the **Posts** screen to display its **Community** (Figure 1) or **Source** (Figure 2) screen.
4. Click **Community** (or **Source**) **Config** at the upper-right corner of the **Community** or **Source** card to display the **Community Config** (Figure 15) or **Source Config** screen (Figure 16), respectively.

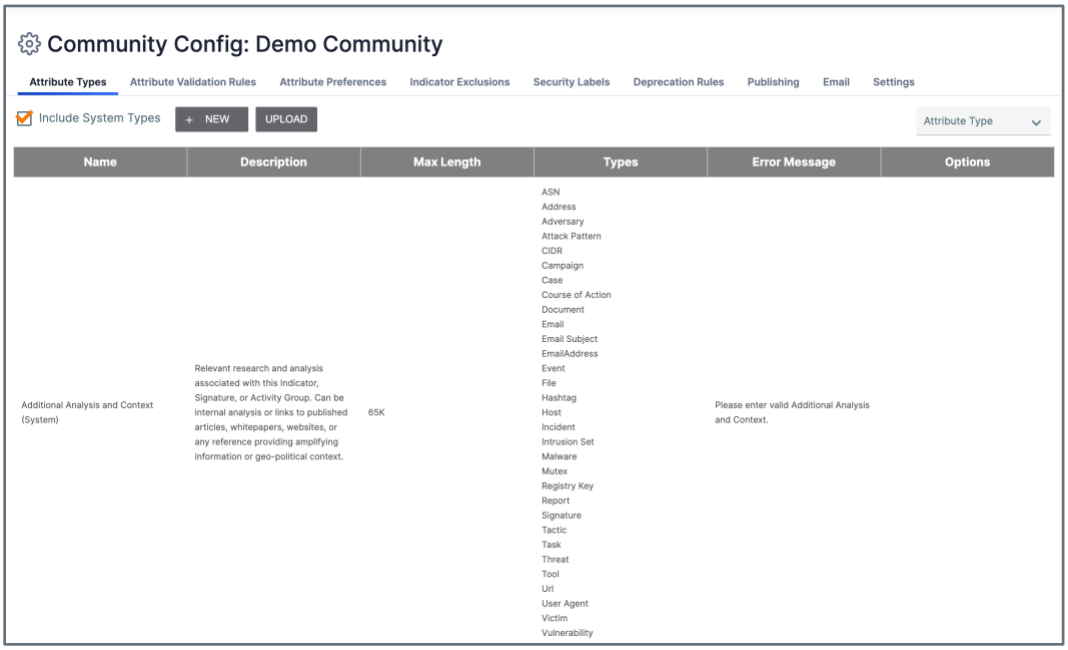

Figure 15

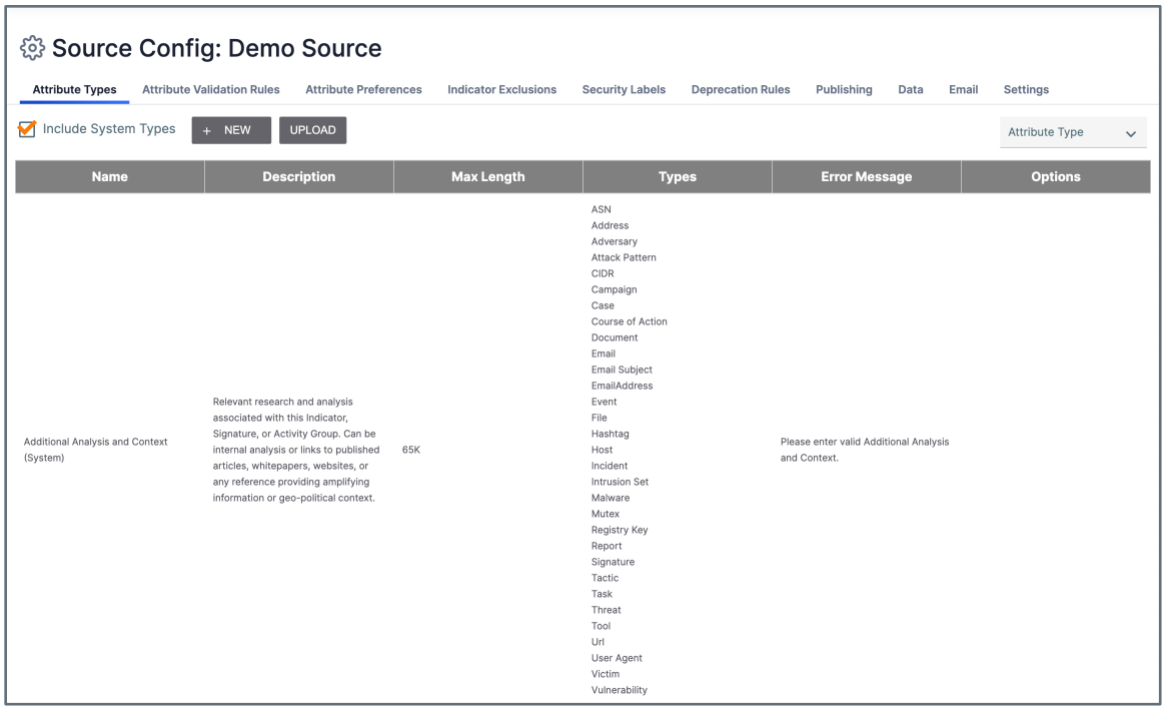

Figure 16

Important: The **Deprecation Rules** tab will be displayed only if the **Allow Automated Confidence Deprecation** option was selected when creating the Community or Source. Similarly, the **Email** tab will be displayed only if the **Allow Feed Email Ingest or Allow Phishing Email Ingest** option was selected when creating the Community or Source. For more information about these options, see the "Community/Sources Tab" section of *ThreatConnect Account Administration Guide*.

Hint: You can also click the **COMMUNITY CONFIG** or **SOURCE CONFIG** button on the left side of the **Information** tab of the **Community Info** screen (Figure 6) or **Source Info** screen (Figure 7) to navigate to the **Community Config** or **Source Config** screen, respectively.

Attribute Types

Attributes are key/value sets that can be added to any Indicator, Group, Case, or Victim, based on the information defined in the Attribute Type for a given Attribute. Attribute Types can be defined for data in all owners on a ThreatConnect instance (System Attribute Type), data in an Organization (Organization Attribute Type), or data in a Community or Source (Community or Source Attribute Types). Community and Source Editors and Directors can create and edit Attribute Types in their Community or Source.

The **Attribute Types** tab of the **Community Config** screen (Figure 15) and **Source Config** screen (Figure 16) displays Attribute Types that have been created for the Community or Source, as well as System Attribute Types if the **Include System Rules** checkbox is selected.

Create Attribute Types

Attribute Types can be created directly in the ThreatConnect UI. Follow these steps to create a new Attribute Type in a Community or Source via the ThreatConnect UI:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Retain the default tab selection of **Attribute Types** (Figure 15, Figure 16).
3. Click **+ NEW** to display the **Configure Attribute Type** window (Figure 17).

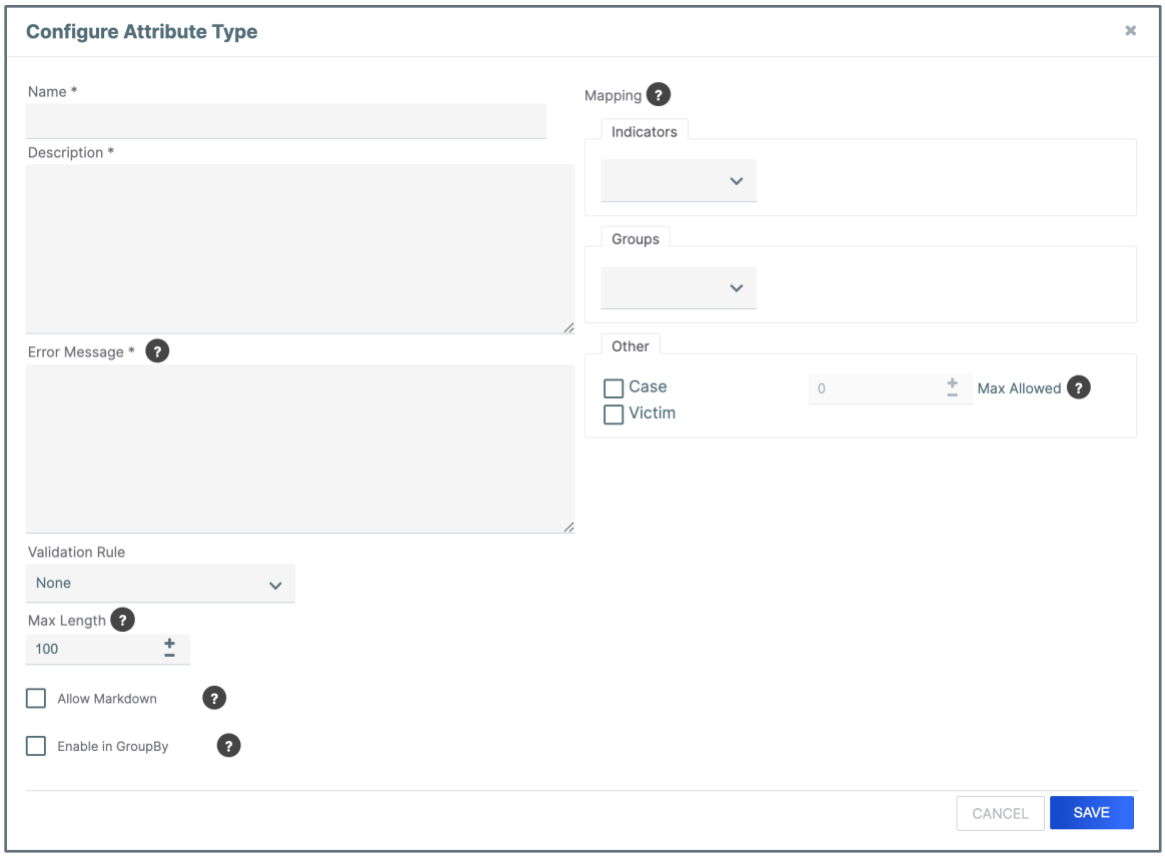

Figure 17

- **Name**: Enter a name for the Attribute Type.
- **Description**: Enter a description for the Attribute Type..
- **Error Message**: Enter the message displayed when users try to input a value for an Attribute that does not meet the Attribute Type's Validation Rule.
- **Validation Rule**: Select the schema that determines whether a user's input is valid when entering an Attribute of this Attribute Type. ThreatConnect provides a variety of Validation Rules, but you can also define their own Attribute Type Validation Rules on the **Attribute Validation Rules** .
- **Max Length**: Enter the maximum character length of the Attribute Type, if applicable, based on the Attribute Type's Validation Rule.
- **Allow Markdown**: Select the checkbox to allow Markdown to be used when configuring an Attribute Type.

> **Note**: Markdown is a plaintext formatting language that can be used to add formatting elements to a number of Attribute Types, including Description and Source. See the

"Enabling and Using Markdown in Attributes" section of *Creating Attributes* for more information.

- **Enable in GroupBy**: Select this checkbox to allow the Attribute Type to be grouped or queried by in dashboard query cards.

  Important: If an Attribute Type's maximum length is greater than 500 characters, the **Enable in GroupBy** checkbox will be disabled.

- **Mapping**:
  - **Indicators**: Click the dropdown to display a scrollable multi-select list of Indicators, and select the checkboxes to specify the types of Indicators to which the Attribute Type can apply. For example, it may make sense to track a "work-hours" Attribute Type against an Incident or File, but not against a URL.
  - **Groups**: Click the dropdown to display a scrollable multi-select list of Groups, and select the checkboxes to specify the types of Indicators to which the Attribute Type can apply.
  - **Case**: This checkbox is used when the Attribute Type should apply to a Case. However, Case Attribute Types do not apply to Communities and Sources, so it is recommended that they are not created here.
  - **Max Allowed**: If the **Case** checkbox is selected, the **Max Allowed** option will be enabled. This option allows you to enter the maximum number of times that the Attribute Type can be added to a single Case. However, Case Attribute Types do not apply to Communities and Sources, so it is recommended that they are not created here and that this option not be configured here.
  - **Victim**: Select this checkbox if the Attribute Type should apply to a Victim.
- Click **SAVE**.

Upload Attribute Types

Attribute Types can be uploaded directly into ThreatConnect from a text or JSON file. Follow these steps to create a new Attribute Type in a Community or Source via upload:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Retain the default tab selection of **Attribute Types** (Figure 15, Figure 16).
3. Click **UPLOAD** button to display the **Upload Attributes** window (Figure 18).

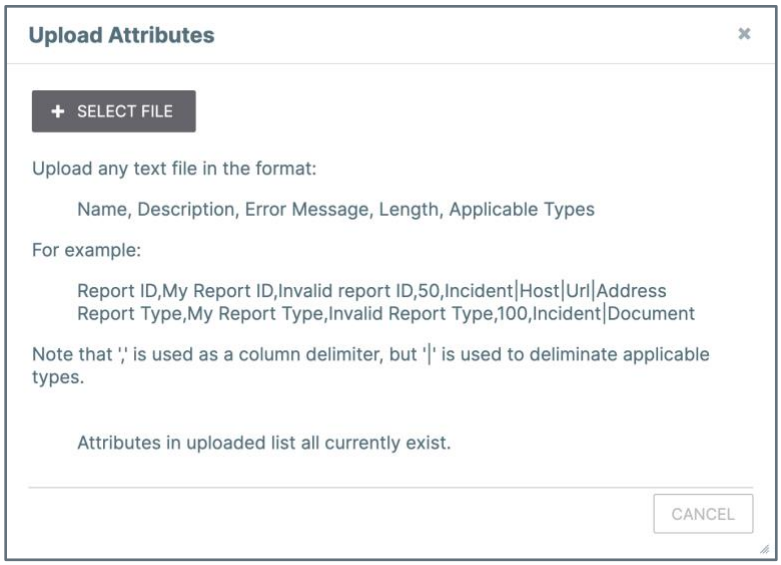

Figure 18

- Click **+ SELECT FILE** to locate and select a file to upload.
- Click **SAVE**.

If uploading Attribute Types in a text file, use the following format: **Name**, **Description**, **Error Message**, **Length**, **Applicable Types**.

> **Note**: In text files, columns are delimited by the comma character (,). Applicable Types are delimited by the pipe character (|).

If uploading Attribute Types via a JSON file, refer to the following schema and example for the fields that can be included in the file.

> **Note**: To update an existing Attribute Type, the `name` field's value must be the name of the Attribute Type being updated, and the `version` field's value must be incremented from the previous value by at least 1.

Schema

- `types`: <*Array of Objects*> **REQUIRED** The details of the Attribute Type(s) to create or update:
  - `allowMarkdown`: <*Boolean*> Specifies whether Markdown may be used when entering values for Attributes of this Attribute Type.
  - `description`: <*String*> **REQUIRED** The Attribute Type's description.

- `errorMessage`: <*String*> **REQUIRED** The error message that is presented to users when they try to enter an invalid value for Attributes of this Attribute Type (i.e., a value that does not meet the Attribute Type's Validation Rule, if one is applied).
- `groups`: <*Array of Strings*> The Group type(s) that can use the Attribute Type.
- `indicators`: <*Array of Strings*> The Indicator type(s) that can use the Attribute Type.
- `maxLength`: <*Integer*> **REQUIRED** The maximum number of characters that may be used when entering values for Attributes of this Attribute Type. (Minimum value: **1**; Maximum value: **512000**)
- `name`: <*String*> **REQUIRED** The Attribute Type's name.
- `system`: <*Boolean*> Specifies whether to create the Attribute Type at the System level. If uploading the JSON file on the **System Settings** screen, this field will be ignored.
- `validationRule`: <*Object*> The details of the Validation Rule to apply to the Attribute Type. If applying a Validation Rule to an Attribute Type, the `validationRules` field must be included in the JSON file.
  - `name`: <*String*> The Validation Rule's name.
- `version`: <*Integer*> The Attribute Type's version number. Upon creation of a new Attribute Type, the `version` field is assigned a value of **1** automatically.

- `validationRules`: <*Array of Objects*>The details of the Validation Rule(s) to apply to the Attribute Type(s). If this field is included, each object in the array must include all of the following fields marked as required at a minimum:
  - `data`: <*String*> The contents of the Validation Rule. This field is required unless the `type` field's value is **DATE** or **DATE_TIME**. If the `type` field's value is **SELECT_ONE_PICKLIST**, **SELECT_ONE_RADIO**, or **INTEGER**, then the value for the `data` field must be a semicolon-delimited string.
  - `description`: <*String*> **REQUIRED** The Validation Rule's description.
  - `name`: <*String*> **REQUIRED** The Validation Rule's name.
  - `type`: <*String*> **REQUIRED** The Validation Rule's type. (Acceptable values: **REGEX**, **XSD**, **SELECT_ONE_PICKLIST**, **SELECT_ONE_RADIO**, **DATE**, **DATE_TIME**, **INTEGER**)
  - `version`: <*Integer*> The Validation Rule's version number.

Example

```
{
    "types": [
        {
            "allowMarkdown": <boolean>,
            "description": "<string>",
            "errorMessage": "<string>",
            "groups": [
                "<string>"
            ],
            "indicators": [
                "<string>"
            ],
            "maxLength": <int>,
            "name": "<string>",
            "system": <boolean>,
            "validationRule": {
                "name": "<string>"
            },
            "version": <int>
        }
    ],
    "validationRules": [
        {
            "data": "<string>",
            "description": "<string>",
            "name": "<string>",
            "type": "<string>",
            "version": <int>
        }
    ]
}
```

Edit Attribute Types

Follow these steps to edit an Attribute Type in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Retain the default tab selection of **Attribute Types** (Figure 15, Figure 16).

3. Click **Edit** in the **Options** column for the Attribute Type to display the **Configure Attribute Type** window (Figure 17).

> **Note**: You cannot edit System Attribute Types from this screen. To filter the screen to Attribute Types for only the Community or Source, clear the **Include System Types** checkbox at the upper left.

> **Note**: You can use the dropdown at the top right of the **Attribute Types** screen to filter the displayed Attribute Types by object. For example, selecting **Host** will display only Attribute Types that map to the **Host** Indicator.

4. Configure the fields for the Attribute Type. See the "Create Attribute Types" section for more detail.
5. Click **SAVE** .

Delete Attribute Types

Follow these steps to delete an Attribute Type in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Retain the default tab selection of **Attribute Types** (Figure 15, Figure 16).
3. Click **Delete** in the **Options** column for the Attribute Type to display the **Delete Attribute Type** window.

> **Note**: You cannot delete System Attribute Types from this screen. To filter the screen to Attribute Types for only the Community or Source, clear the **Include System Types** checkbox at the upper left.

> **Note**: You can use the dropdown at the top right of the **Attribute Types** screen to filter the displayed Attribute Types by object. For example, selecting **Host** will display only Attribute Types that map to the **Host** Indicator.

4. Click **YES**.

Attribute Validation Rules

Attribute Validation Rules ensure that Attribute Types conform to a valid input range and format. The **Attribute Validation Rules** tab of the **Community Config** and **Source Config** screen (Figure 19) displays the Attribute Validation Rules that have been created for the Community or Source, respectively, as well as the System Attribute Validation Rules if the **Include System Rules** checkbox is selected.

Figure 19

Create Attribute Validation Rules

Follow these steps to create a new Attribute Validation Rule in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Attribute Validation Rules** tab (Figure 19).
3. Click **+ NEW** to display the **Create Attribute Validation Rule** window (Figure 20).

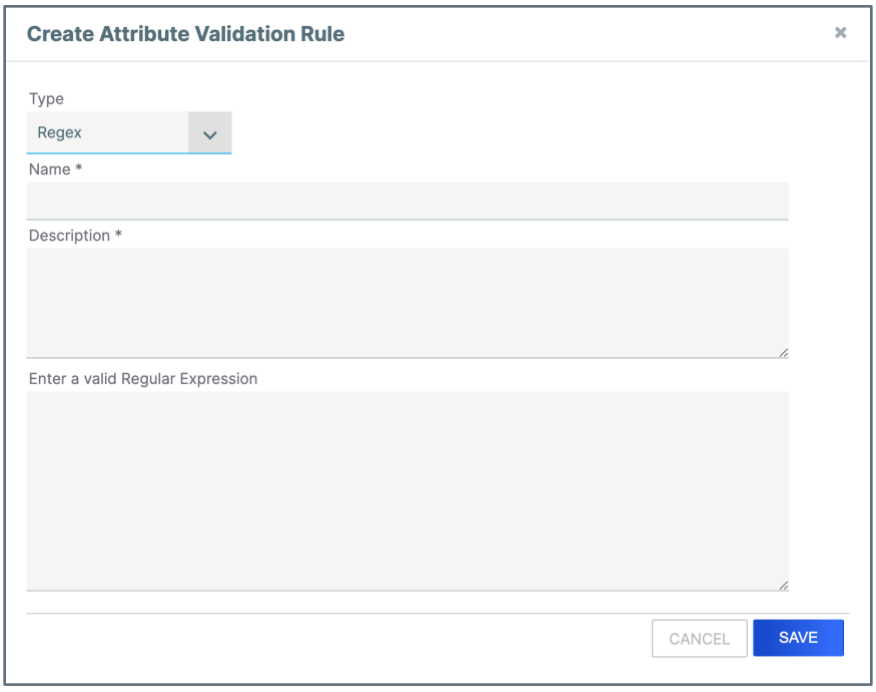

Figure 20

- **Type**: Select the schema to use for the Validation Rule. Each option offers the flexibility to determine the valid domain for each Attribute Type.
  - **Regex:** A regular expression that considers only matching inputs to be valid (e.g., an IP address or email address on a certain domain).
  - **Xsd**: An XML Schema Definition used to validate input (useful for attaching logs from a vendor product).
  - **Select One Picklist**: A dropdown menu of options from which users may select only one value (e.g., high, medium, or low priorities).
  - **Select One Radio**: A series of radio buttons from which users may select only one value.
  - **Date**: A date in YYYY/MM/DD format.
  - **Date/Time**: A date and time in YYYY-MM-DD HH:MM UTC format.
  - **Integer:** A whole number, valid in a specified range (e.g., 0:1440 for "minutes worked").
- **Name**: Enter the name of the Validation Rule. This name will be displayed in the **Validation Rule** dropdown in the **Configure Attribute Type** window (Figure 17).
- **Description**: Enter a description for the Validation Rule.

- **Enter a …:** If the selected **Type** is **Regex**, **Xsd**, **Select One Picklist**, **Select One Radio**, or **Integer**, enter the parameters for the Validation Rule as specified by the text above the field (e.g., **Enter a valid Regular Expression**, **Enter a semicolon-delimited list of options**).
- Click **SAVE**.

> **Important**: The Attribute Validation Rule must be assigned to an Attribute Type in order to validate user input.

Edit Attribute Validation Rules

Follow these steps to edit an Attribute Validation Rule in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Attribute Validation Rules** tab (Figure 19).
3. Click **Edit** in the **Options** column for the Attribute Validation Rule to display the **Create Attribute Validation Rule** window (Figure 20).

> **Note**: You cannot edit System Attribute Validation Rules from this screen. To filter the screen to Validation Rules for only the Community or Source, clear the **Include System Rules** checkbox at the upper left.

4. Configure the fields for the Attribute Validation Rule. See the "Create Attribute Validation Rules" section for more detail.
5. Click **SAVE**.

Delete Attribute Validation Rules

Follow these steps to delete an Attribute Validation Rule in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Attribute Validation Rules** tab (Figure 19).
3. Click **Delete** in the **Options** column for the Attribute Validation Rule to display the **Delete Attribute Validation Rule** window.

> **Note**: You cannot delete System Attribute Validation Rules from this screen. To filter the screen to Validation Rules for only the Community or Source, clear the **Include System Rules** checkbox at the upper left.

4. Click **YES**.

Attribute Preferences

Attribute Preferences allow you to configure an Attribute Type as a default, pinned, or association Attribute Type in a Community or Source for selected object type(s). The **Attribute Preferences** tab of the **Community Config** and **Source Config** screen (Figure 21) displays the Attribute Types to which you have added an Attribute Preference.

Figure 21

Create Attribute Preferences

Follow these steps to create an Attribute Preference in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Attribute Preferences** tab (Figure 21).
3. Click **+ NEW** to display the **Add Attribute Preference** window (Figure 22).

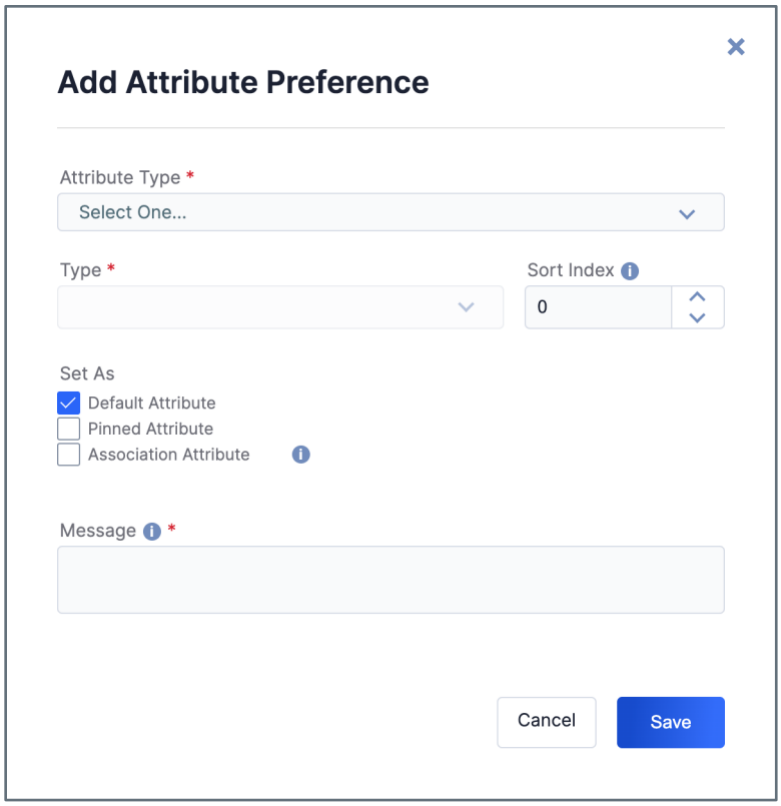

Figure 22

- **Attribute Type**: Select the Attribute Type to which the Attribute Preference will be added. Note that you can filter Attribute Types in the dropdown menu by name.
- **Type**: Select one or more object types to which the Attribute Preference will apply. Only object types to which the Attribute Type can be added will be listed in the dropdown menu.
- **Sort Index**: Enter the index used to arrange Attributes of the selected Attribute Type on the **Attributes** card. Indices are set in ascending order, meaning that the Attribute Type ranked **0** will be at the top of the **Attributes** card, and the Attribute Type ranked with the highest number will be at the bottom.
- **Default Attribute**: Select this checkbox to display the Attribute Type as a placeholder default Attribute on the **Attributes** card on the **Details** screen for objects of the selected type(s).
- **Pinned Attribute**: Select this checkbox to configure the Attribute Type as a pinned Attribute Type for the selected object type(s). When this setting is enabled, Attributes of the selected Attribute Type that are added to objects of the selected type(s) will be displayed in the **Pinned Attributes** section of the **Attributes** card

automatically, regardless of whether the user selected the **Pinned Attribute** checkbox when creating the Attribute.

> **Note**: Pinned Attributes are not available on the legacy **Details** screen.

- **Association Attribute**: Select this checkbox to configure the Attribute Type as an association Attribute Type for the selected object type(s). If a user adds an Attribute to a Group and this setting is enabled for its Attribute Type and the Group's type, then the Attribute will be displayed on the **Pinned Association Attributes** card for Indicators and Groups associated to that Group.

> **Note**: Association Attributes are not available on the legacy **Details** screen.

> **Note**: The **Pinned Association Attributes** card only displays association Attributes added to Groups that are associated to the Indicator or Group you are viewing.

- **Message**: Enter text prompting users to populate the placeholder default Attribute in the **Attributes** card on the **Details** screen.
- Click **Save** to save the Attribute Preference for the selected Attribute Type and object type(s).

Edit Attribute Preferences

Follow these steps to edit an Attribute Preference in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Attribute Preferences** tab (Figure 21).
3. Click **Edit** in the **Options** column for the Attribute Preference to display the **Add Attribute Preference** window (Figure 22).
4. Configure the fields for the Attribute Preference. See "Create Attribute Preferences" for more detail.
5. Click **SAVE**.

Delete Attribute Preferences

Follow these steps to delete an Attribute Preference in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Attribute Preferences** tab (Figure 21).
3. Click **Delete** in the **Options** column for the Attribute Preference to display the **Delete Default Attribute Type** window.
4. Click **YES**.

Indicator Exclusions

Indicator Exclusion Lists are created to prevent the import of Indicators that may be deemed legitimate or non-hostile to an organization. When a user tries to create an Indicator that is on an Indicator Exclusion List, the Indicator will not be created, and a message explaining that the Indicator is contained on an Indicator Exclusion List will be displayed.

The **Indicator Exclusions** tab of the **Community Config** and **Source Config** screen (Figure 23) displays the number of items on each Indicator type's Indicator Exclusion List for the Community or Source, respectively.

Figure 23

Edit Indicator Exclusion Lists

Follow these steps to edit an Indicator Exclusion List in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Indicator Exclusions** tab (Figure 23).

3. Click **Edit** in the **Options** column for an Indicator type to display the **Exclusion Details** window (Figure 24).

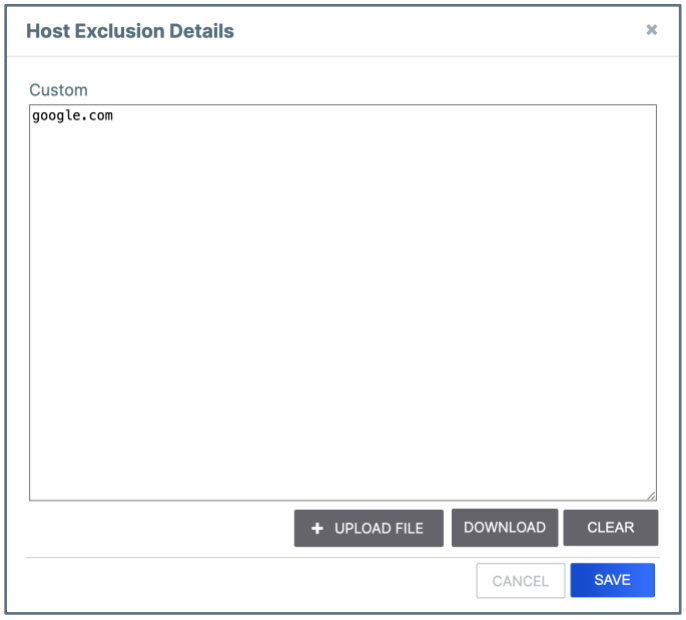

Figure 24

- **Custom**: Enter Indicators of the selected type into the text box.

  Hint: Place an asterisk (*) at the beginning and end of an Indicator to include all results containing the enclosed text in the Indicator Exclusion List. For example, ***xyz.com*** in the Exclusion List for the URL Indicator type would exclude any URL that contains the string **xyz.com**.

- **+ UPLOAD FILE**: Click this button to locate and upload a **.tx**t file containing a list of Indicators. After the upload is complete, the Indicators will be listed in the **Custom** text box.
- **DOWNLOAD**: This option will be displayed when editing an Indicator Exclusion List that has at least one value. Click this button to download the current Indicator Exclusion List into a **.txt** file.
- **CLEAR**: This option will be displayed when editing an Indicator Exclusion List that has at least one value. Click this button to clear all values from the list.
- Click **SAVE**.

Security Labels

Security Labels are a powerful way to label, track, and limit information shared across data owners in ThreatConnect. ThreatConnect uses the Traffic Light Protocol (TLP) system published by the Forum of Incident Response and Security Teams™ (FIRST). You can define Security Labels for use by all member Organizations in a Community or Source. When users share or contribute data within ThreatConnect, they can use Security Labels to determine whether a piece of information is withheld or provided according to their organization's policies.

Security Labels can be applied to Indicators, Groups, and Victims. In addition, separate Security Labels can be applied to Attributes. For example, an Address Indicator may have a Security Label of **TLP:GREEN** (i.e., peers and partner organizations may see it). However, its Source Attribute may be a sensitive system log that pinpoints a system vulnerability and thus has a Security Label of **TLP:RED** (i.e., not to be shared). Community and Source Editors and Directors are encouraged to familiarize their users with their Community's or Source's sharing policies and the Security Labels used to enact them.

The **Security Labels** tab of the **Community Config** and **Source Config** screen (Figure 25) displays existing Security Labels that have been created for the Community or Source, as well as System Security Labels if the **Include System Labels** checkbox is selected.

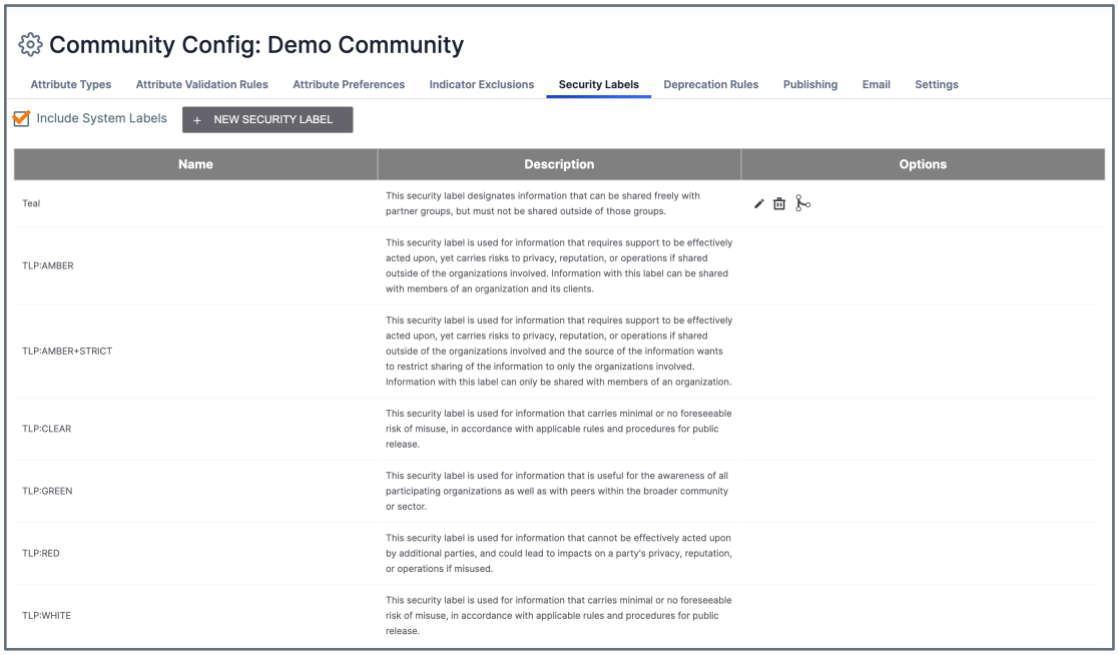

Figure 25

Create Security Labels

Follow these steps to create a new Security Label in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Security Labels** tab (Figure 25).
3. Click **+ NEW SECURITY LABEL** to display the **Create Security Label** window (Figure 26).

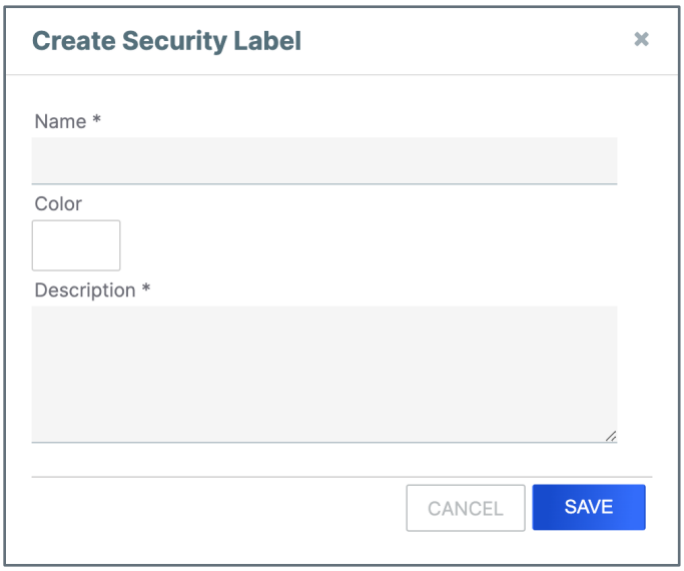

Figure 26

- **Name**: Enter a name for the Security Label.
- **Color**: Click in the box to select a color using the color picker, or enter a color code in RGB or hexadecimal format.
- **Description**: Enter a description for the Security Label.

> **Note**: These fields are provided solely for user and Administrator readability, as no policy enforcement is derived from this screen.

- Click **SAVE**.

Edit Security Labels

Follow these steps to edit a Security Label in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Security Labels** tab (Figure 25).
3. Click **Edit** in the **Options** column for the Security Label to display the **Create Security Label** window (Figure 26).

   Note: You cannot edit System Security Labels from this screen. To filter the screen to Security Labels for only the Community or Source, clear the **Include System Labels** checkbox at the upper left.

4. Configure the fields for the Security Label. See the "Create Security Labels" section for more detail.
5. Click **SAVE**.

Delete Security Labels

Follow these steps to delete a Security Label in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Security Labels** tab (Figure 25).
3. Click **Delete** in the **Options** column for the Security Label to display the **Delete Security Label** window.

   Note: You cannot delete System Security Labels from this screen. To filter the screen to Security Labels for only the Community or Source, clear the **Include System Labels** checkbox at the upper left.

4. Click **YES**.

Consolidate Security Labels

A Security Label in a Community or Source can be consolidated with a System Security Label, causing all data objects that have the Community or Source Security Label to be re-labeled with the System Security Label.

Follow these steps to consolidate a Security Label in a Community or Source with a System Security Label:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Security Labels** tab (Figure 25).
3. Click **Consolidate** in the **Options** column for the Security Label to display the **Consolidate Security Label** window (Figure 27).

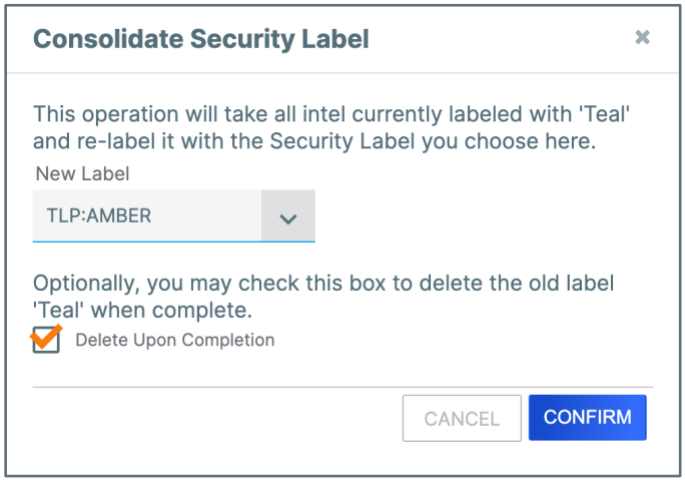

Figure 27

- **New Label**: Select the System Security Label that will be applied to all data objects currently labeled with the Community or Source Security Label.

  Important: The **Include System Labels** checkbox on the **Security Labels** tab must be selected for options to be provided in the **New Label** dropdown.

- **Delete Upon Completion**: Select this checkbox to delete the Community or Source Security Label after consolidation is complete.
- Click **CONFIRM**.

Deprecation Rules

Indicator confidence deprecation is a great way to allow Indicators to drop in Confidence Rating over time or be set as inactive or deleted if the Confidence Rating is not being maintained and updated. Confidence deprecation is a way to determine that an Indicator is no longer being used for any malicious activity for a certain amount of time. Depending on the configuration of the confidence deprecation rule for an Indicator's type, ThreatConnect will drop the Confidence Rating for the Indicator. Once the Confidence Rating reaches the minimum value in the deprecation rule's configuration, it may set the Indicator's status as inactive or delete the Indicator, assuming that the Indicator is dormant or that the threat actor has ceased using it.

The **Deprecation Rules** tab of the **Community Config** or **Source Config** screen (Figure 28) displays the confidence deprecation rules that have been created for Indicator types in the Community or Source, respectively.

Important: The **Deprecation Rules** tab will be displayed only if the **Allow Automated Confidence Deprecation** option was selected when creating the Community or Source. See the "Community/Sources Tab" section of *ThreatConnect Account Administration Guide* for more information.

Figure 28

Create Deprecation Rules

See *Configuring Indicator Confidence Deprecation* for instruction on how to create a new confidence deprecation rule for the Community or Source.

Edit Deprecation Rules

See *Configuring Indicator Confidence Deprecation* for instruction on how to edit a confidence deprecation rule for the Community or Source.

Delete Deprecation Rules

Follow these steps to delete a deprecation rule in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Deprecation Rules** tab (Figure 28).
3. Click **Delete** in the **Options** column for the deprecation rule to display the **Delete Deprecation Rule** window.
4. Click **YES**.

Publishing

The Publish feature packages intelligence in the form of Group data objects and writes it to a JSON file. It is a necessary step in the process of sharing the data with users on other ThreatConnect instances. Once a Group has been published, it can be shared across instances via the Cross-Intel Sharing App.

All types of Group data objects except Task can be published. In order to publish a Group, it must first exist in, or be contributed to, a Community or Source. The Publish feature is accessed from the **Sharing** tab of a Group's legacy **Details** screen.

The **Publishing** tab of the **Community Config** and **Source Config** screen (Figure 29) allows you to view, download, and delete JSON files published in a Community or Source, respectively.

Figure 29

View and Download Published Files

You can determine which types of published files to display on the **Publishing** tab by selecting the **Active**, **Superseded**, or **Deleted** checkboxes at the top left of the screen. To download a file, click **Download** in the **Options** column for a published file.

Delete Published Files

Follow these steps to delete a published file in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Publishing** tab (Figure 29).
3. Click **Delete** in the **Options** column for the file to display the **Delete Publication** window.
4. Click **YES**.

Data

The **Data** tab of the **Source Config** screen (Figure 30) allows you to create feeds in a Source, including HTTP Feeds and inbound and outbound TAXII Exchange Feeds.

Important: The **Data** tab is available only for Sources. It is not available for Communities.

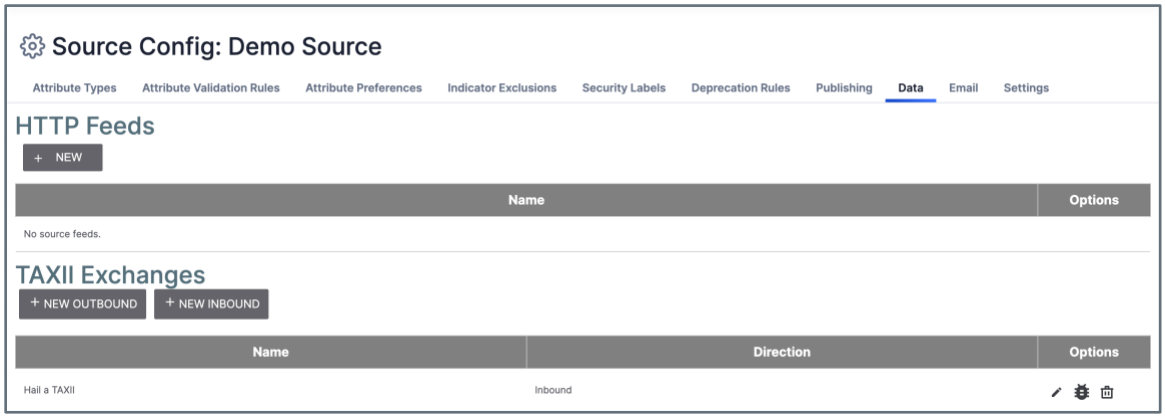

Figure 30

HTTP Feeds

You can set up an ad hoc HTTP Feed (also known as a "screen scrape") for sources of information in ThreatConnect. This ability is particularly useful when a more in-depth feed integration with ThreatConnect does not exist. In order for this feature to work adequately, the source of information should be updated with some regularity. When the Feed Monitor finds Indicators at the designated URL, it will import the Indicators according to the configuration. For instruction on creating an HTTP Feed, see *Creating an HTTP Feed*.

TAXII Exchanges

An Inbound Trusted Automated eXchange of Indicator Information (TAXII) Exchange Feed ingests Structured Threat Information eXpression (STIX™) formatted data from a TAXII server. For instruction on creating an Inbound TAXII Exchange Feed, see *Creating an Inbound TAXII Exchange Feed*.

An Outbound TAXII Exchange Feed pushes STIX-formatted data to a TAXII server via a mailbox. For instruction on creating an Inbound TAXII Exchange Feed, see *Creating an Outbound TAXII Exchange Feed*.

Email

Email ingestion allows users to send cyberthreat-related emails to ThreatConnect, where they will be parsed and imported for further analysis. In order for a ThreatConnect instance to receive phishing or feed emails, a System Administrator must configure ThreatConnect as follows:

- Enable the **mailInboundEnabled** system setting.
- Set a firewall rule on the ThreatConnect server redirecting **port 25** to **port 2500**.

Furthermore, assuming that the domain name for ThreatConnect is **tip.lab.domain.com**, the following is also needed:

- Mail-exchanger record set up for **tip.lab.domain.com.**
- Firewall rules to allow this traffic to traverse the network.

The **Email** tab of the **Community Config** and **Source Config** screen (Figure 31) allows you to create phishing and feed mailboxes in the Community and Source, respectively.

Important: The **Email** tab will be displayed only if the **Allow Feed Email Ingest or Allow Phishing Email Ingest** option was selected when creating the Community or Source. See the "Community/Sources Tab" section of *ThreatConnect Account Administration Guide* for more information.

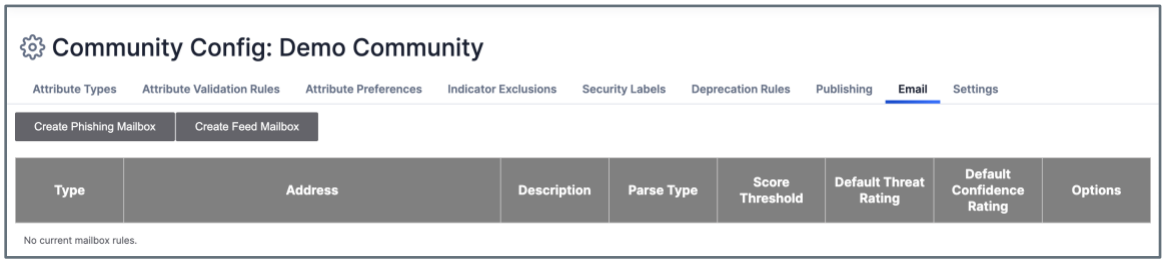

Figure 31

Create a Phishing Mailbox

Phishing mailboxes receive malicious or suspicious emails that are flagged by the Email Security Gateway, or emails in .msg or .eml format that have been flagged by a security analyst. When creating a phishing mailbox in a Community or Source, the Director specifies whether the mailbox will be configured to receive emails directly from network devices or email headers in the form of attachments. After the phishing mailbox has been created, ThreatConnect parses the emails the mailbox receives, and if an email meets the minimum score threshold specified in the mailbox's configuration, an Email Group object and Task Group object are created, and Indicators found in the header or body of the email are associated to the Email Group if those Indicators already exist in the Community or Source. See *Creating a Phishing Mailbox* for further instruction.

Create a Feed Mailbox

Feed mailboxes receive mail from cyber-intel sources, which release information periodically as an RSS feed in an email-type format. Emails sent to the feed mailbox have only their bodies parsed for Indicators. ThreatConnect then creates a Document Group object with the email's body, creates Indicators that matched the regular expressions defined in the feed mailbox's configuration, and associates the Indicators to the Document.

Follow these steps to create a feed mailbox in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Email** tab (Figure 31).

3. Click **Create Feed Mailbox** on the **Email** screen to display the **Mailbox** tab of the **Feed Mailbox Administration** window (Figure 32).

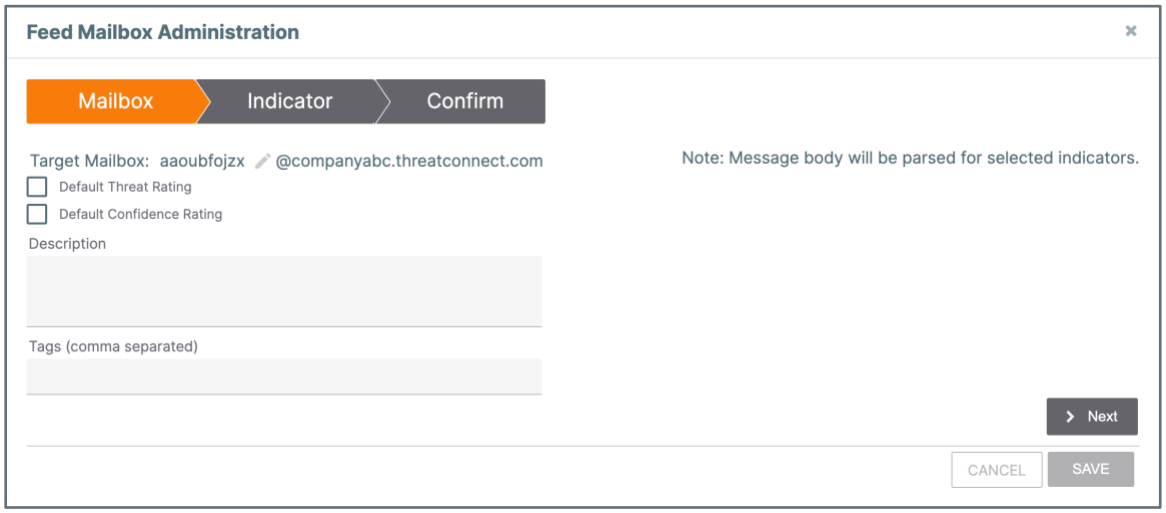

Figure 32

- **Default Threat Rating**: Select the checkbox to assign a default Threat Rating to any found Indicators, and then click on the appropriate skull (1–5) to set the Threat Rating.
- **Default Confidence Rating**: Select this checkbox to assign a default Confidence Rating to any found Indicators, and then enter the Confidence Rating.
- **Description**: Enter a description for the feed mailbox.
- **Tags**: Enter Tags, separated by commas, for the feed mailbox.
- Click **Next**.

4. The **Indicator** tab will be displayed (Figure 33).

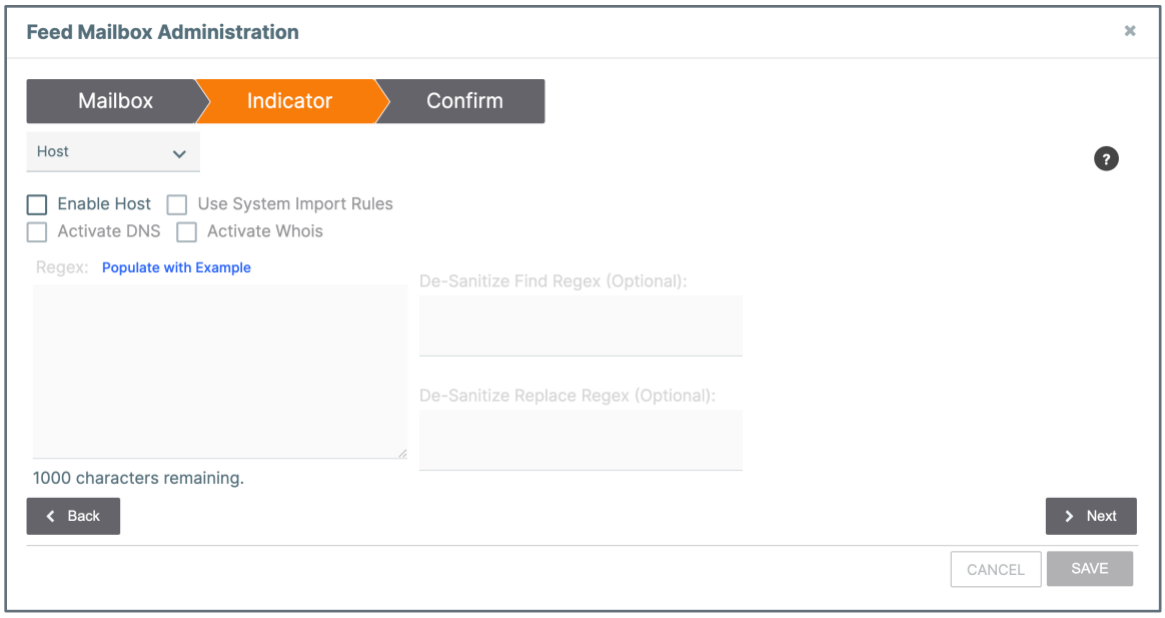

Figure 33

- ‹ ***Indicator Type***›: Select an Indicator type from the dropdown.

  Note: The following Indicator types are not available in the dropdown: Email Subject, Hashtag, Mutex, Registry Key, User Agent.

- **Enable ‹ *Indicator Type*›**: Select this checkbox to enable detection of sanitized Indicators of the selected type.
- **Use System Import Rules**: Select this checkbox to use the standard ThreatConnect import rules for the selected Indicator type. See the "Indicator Import Rules" section of *ThreatConnect System Administration Guide* for more information.
- **Activate DNS**: (Host Indicator type only) Select this checkbox to activate DNS tracking on Host Indicators.
- **Activate Whois**: (Host Indicator type only) Select this checkbox to activate Whois tracking on Host Indicators.
- **Regex**: If the **Enable ‹ *Indicator Type*›** checkbox is selected, you can enter regular expressions to run against the text in an email. The regular expressions should handle sanitized Indicators. If there is no text entered in the **Regex** text box, you can click **Populate with Example** to populate the text box with an example regex.
- **De-Sanitize Find Regex**: (Optional) Enter regular expressions to find sanitized Indicator text. This text box will also populate with an example when you click **Populate with Example**.

- **De-Sanitize Replace Regex (Optional)**: Enter regular expressions to replace sanitized Indicator text.

> **Note**: You can hover over the **Question Mark** at the upper-right corner of the window to display explanations and examples to help define the criteria for each Indicator type.

> **Note**: Indicators that were sanitized within a Document Group can be de-sanitized after the main regex finds them.

5. Repeat Step 4 for each Indicator type that you want to configure the feed mailbox to parse, starting by selecting the Indicator type from the dropdown at the upper left and clicking the **Enable** *‹Indicator Type›* checkbox. When you have finished adding configurations for all of the Indicator types you want the feed mailbox to parse, click **Next**.
6. The **Confirm** tab will be displayed, showing a summary of the feed mailbox's configuration (Figure 34).

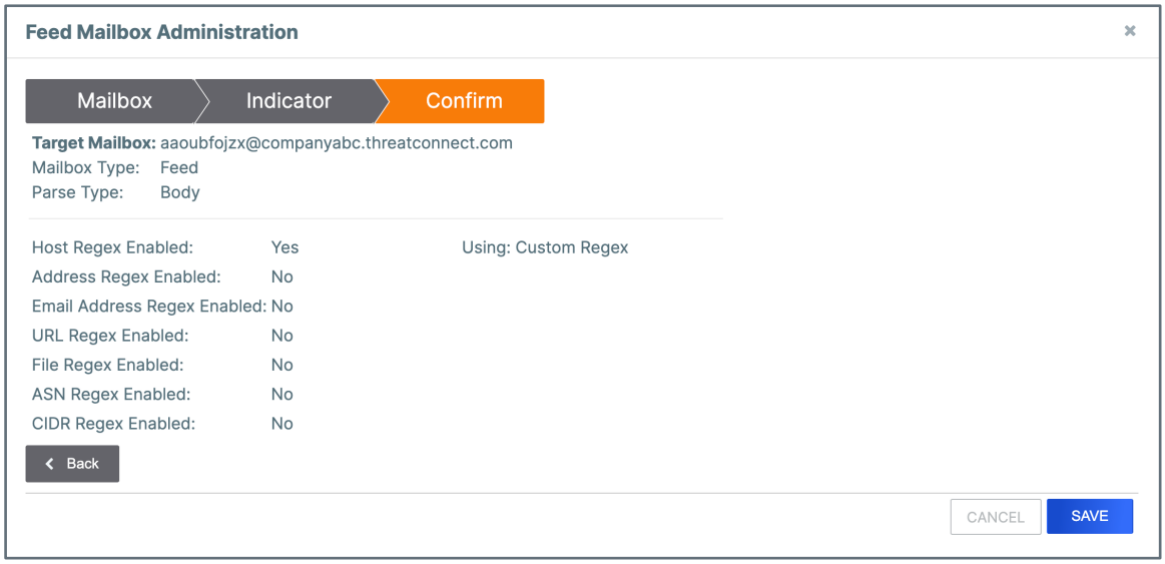

Figure 34

- Review the summary.
- Click **SAVE**.

Settings

The **Settings** tab of the **Community Config** and **Source Config** screen (Figure 35) allows you to add a DomainTools API key in order to enable DomainTools for all Reverse Whois Track queries for a Community or Source, respectively.

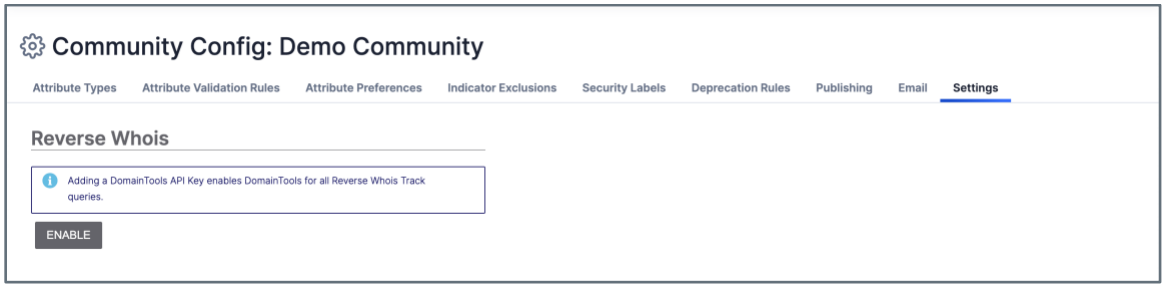

Figure 35

Enable DomainTools

Follow these steps to enable DomainTools in a Community or Source:

1. Navigate to the **Community** (or **Source**) **Config** screen.
2. Select the **Settings** tab (Figure 35).
3. Click **ENABLE** on the **Settings** screen to display the **Setup DomainTools** window (Figure 36).

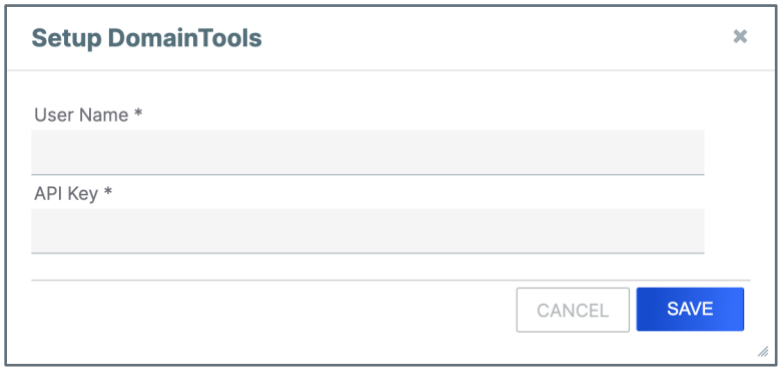

Figure 36

- **User Name**: Enter the username for the DomainTools account.
- **API Key**: Enter the API key for the DomainTools account.
- Click **SAVE**.