ThreatConnect® Community and Source Administration Guide

Software Version 7.0

Technical Guide

January 18, 2023

10011-16 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

The purpose of this guide is to instruct users in the different components of Community and Source administration and configuration. Among the topics discussed are **Roles** and **Access**, **Attribute Types**, **Indicator Exclusion Lists**, **Security Labels**, **Deprecation Rules**, **Email Ingestion**, and **Feeds**. These features reside, primarily, on the **Community Config** or **Source Config** screen.

Community and Source Roles and Access

Table 1 defines each Community and Source role.

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.
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.

Important: Editors in a Source will not be able to update the Threat Rating and Confidence Rating unless they are a member of the Organization that owns the Source, but they can delete and update Attribute Types.

Configure Community and Source Roles

In ThreatConnect, profiles for Communities can either be **ANONYMOUS** or **FULL PROFILE** where all users in a Community are anonymous and able to use their pseudonym or, based on the setting of the Community, able to use their full profile.

1. Log into ThreatConnect with a Director account for the desired Community or Source.
2. On the top navigation bar, click **Posts**. The **Posts screen** will be displayed (Figure 1).

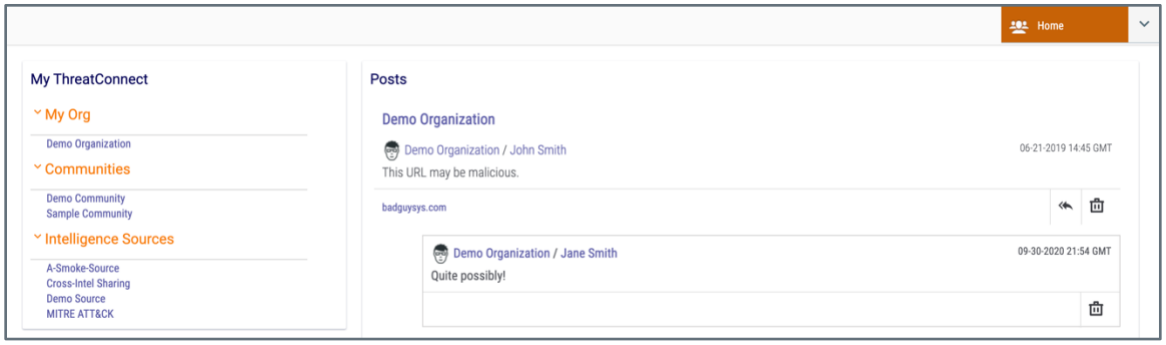

Figure 1

3. Select the desired Community or Source in the **My ThreatConnect** card to display its **Community** (Figure 2) or **Source** (Figure 3) screen. A **Community** or **Source** card is located at the upper-left corner of each screen, which includes information about the selected Community or Source and two icons: **Community** (or **Source**) **Info** and **Community** (or **Source**) **Config** . See the "The Community (and Source) Info Screen" and "The Community (and Source) Config Screen" sections for more information about the screens associated with these icons.

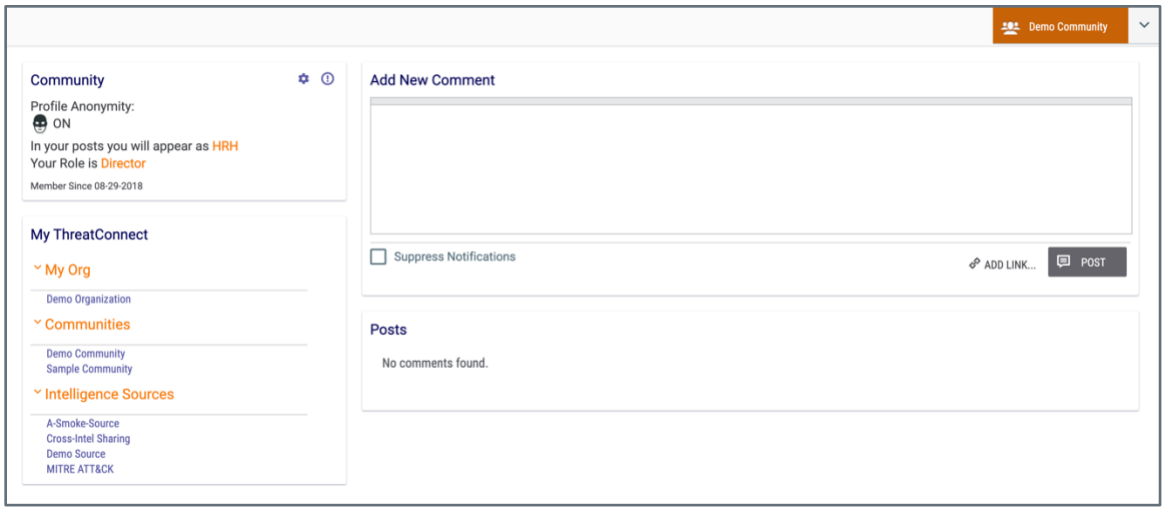

Figure 2

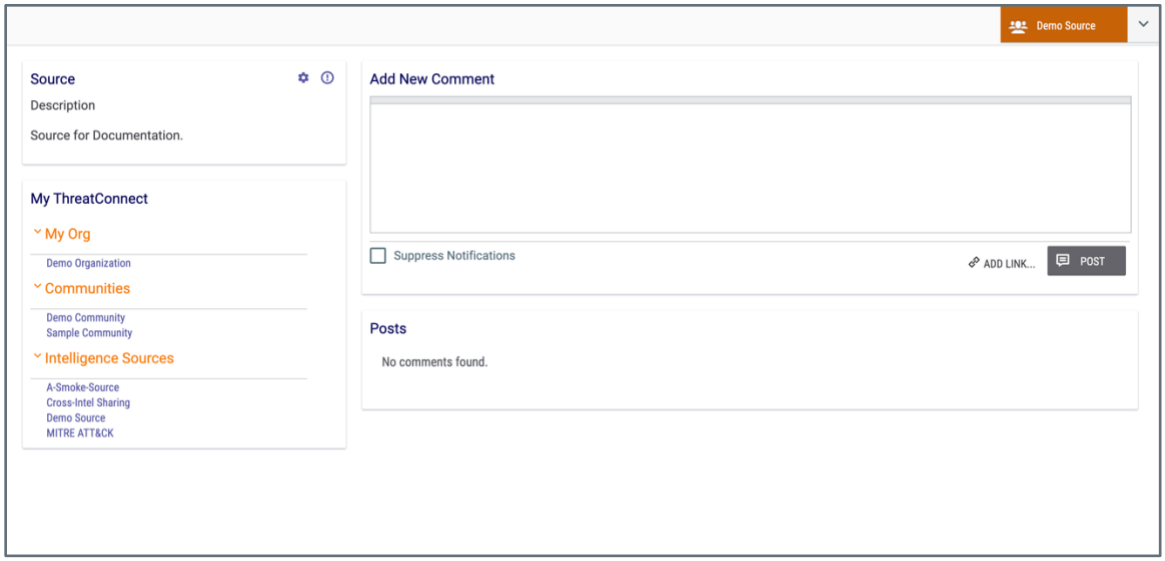

Figure 3

4. Click **Community** (or **Source**) **Info** at the upper-right corner of the **Community** (or **Source**) card. The **Community Info** (Figure 4) or **Source Info** screen (Figure 5) will be displayed.

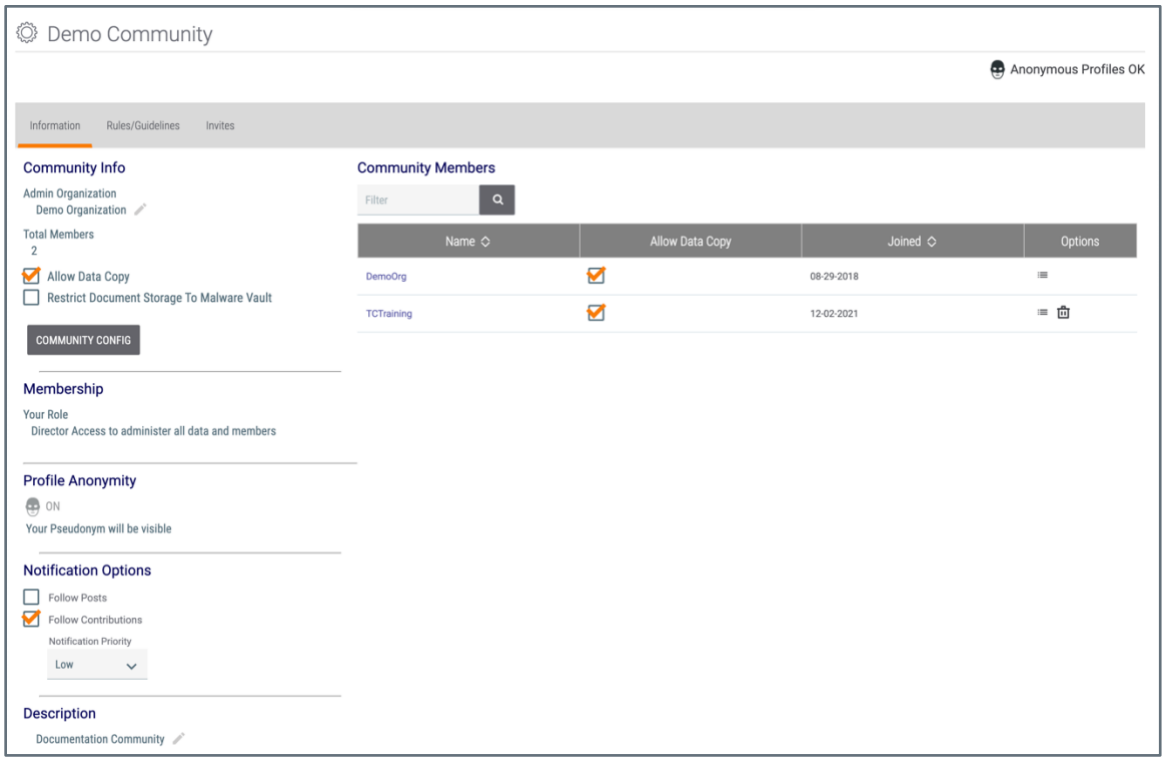

Figure 4

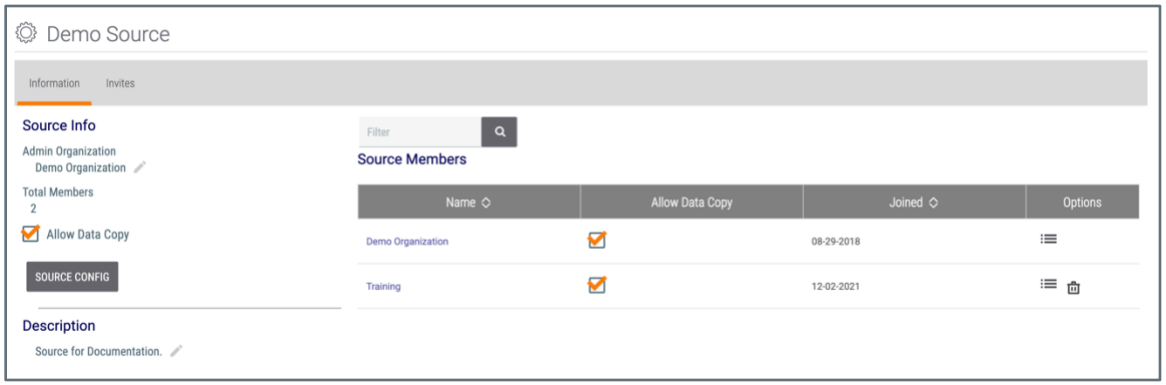

Figure 5

5. Click the corresponding **Users** icon displayed in the **Options** column to configure the Community Member. The **Membership** window will be displayed (Figure 6).

Figure 6

- **Default Role**: Select the default role for all future Org members created under this Organization.
- **Default API Role**: Select the default API role for all future API accounts created under this Organization.
- **Role** (of Individual Users): Click **Edit** to the right of a user's role to change their role. All changes are applied immediately.
- Click the **CLOSE** button when done.

The Community (and Source) Info Screen

Access the Community (or Source) Info Screen

1. Log into ThreatConnect with an Editor or Director account for the desired Community or Source.
2. On the top navigation bar, click **Posts**. The **Posts** screen will be displayed (Figure 1).
3. Select the desired Community or Source in the **My ThreatConnect** card to display its **Community** (Figure 2) or **Source** (Figure 3) screen.
4. Click **Community** (or **Source**) **Info** at the upper-right corner of the **Community** or **Source** card. The **Community Info** (Figure 7) or **Source Info** screen (Figure 8) will be displayed with the **Information** tab selected.

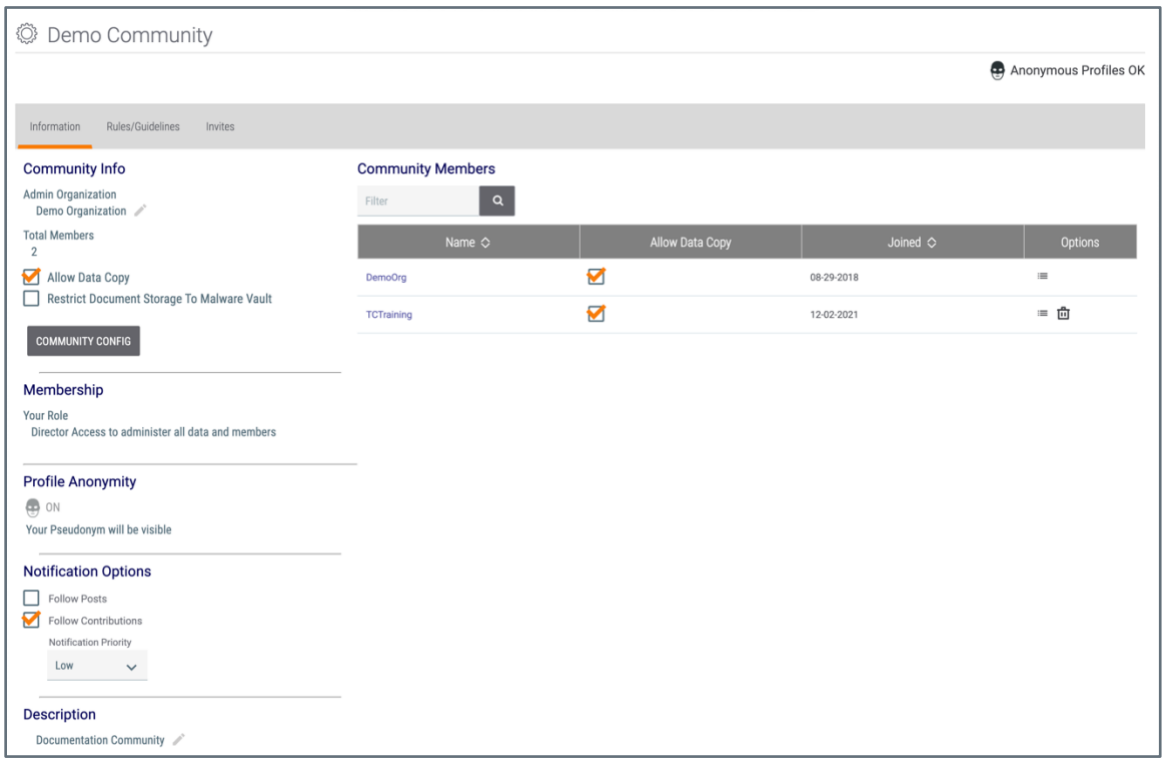

Figure 7

- **Admin Organization**: Click **Edit** to display a dropdown menu from which the Admin Organization for the Community can be selected.

- **Allow Data Copy**: Select the 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 creating a document via the **Create Document** window, when uploading a file to an existing document via the **Details** screen, and when creating an API document 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, if desired.
- **Notification Priority**: Select **Low**, **Medium**, or **High** for the notification priority.
- **Description**: Click **Edit** to edit the Community's description.

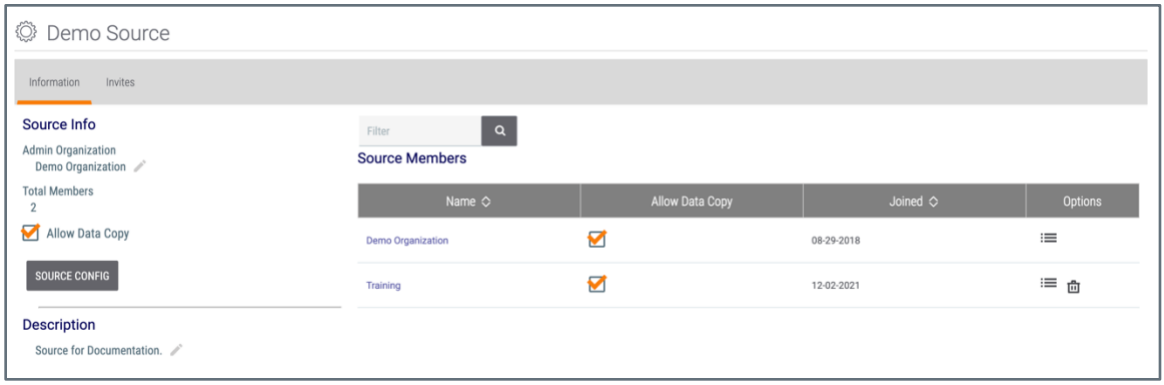

Figure 8

- **Admin Organization**: Click **Edit** to display a dropdown menu from which the Admin Organization for the Source can be selected.
- **Allow Data Copy**: Select the 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 as a System Administrator

1. On the top navigation bar, hover the cursor over **Settings** and select **Account Settings**. The **Account Settings** screen will be displayed (Figure 9).

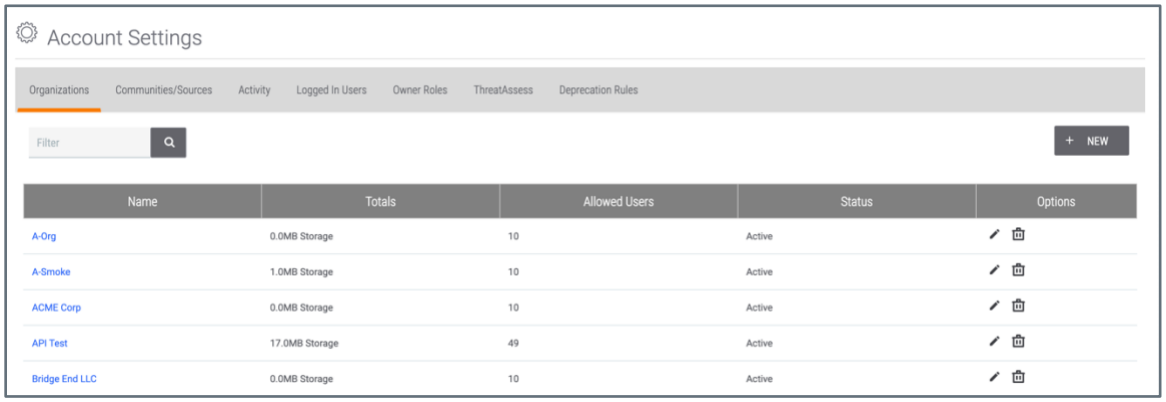

Figure 9

2. Click the **Communities/Sources** tab. The **Communities/Sources** screen will be displayed (Figure 10).

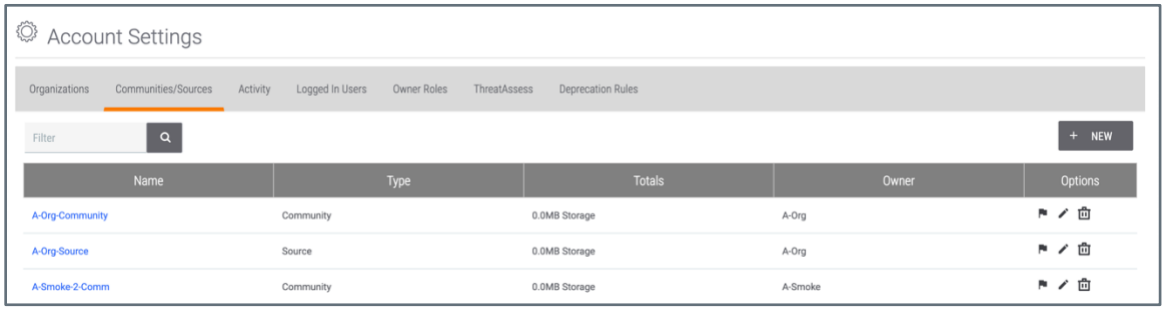

Figure 10

3. Select a Community or Source to display its **Community Info** (Figure 7) or **Source Info** (Figure 8) screen, respectively.

Rules/Guidelines

1. Click **Community Info** at the upper-right corner of the **Community** card (Figure 2). The **Community Info** screen will be displayed (Figure 7).
2. Click the **Rules/Guidelines** tab. The **Rules/Guidelines** screen will be displayed (Figure 11).

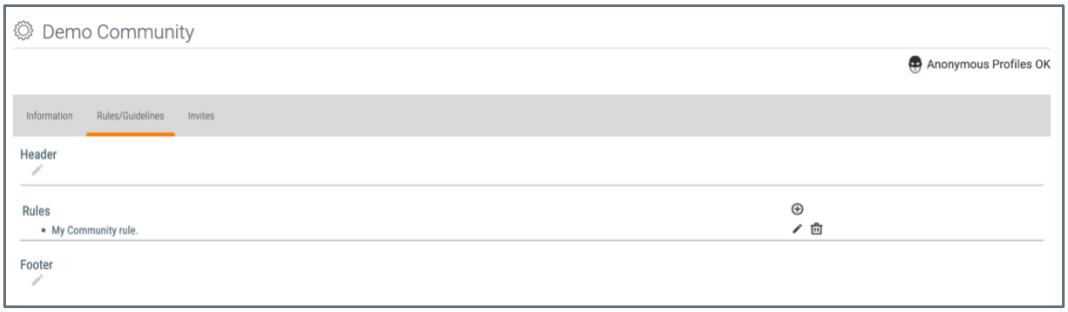

Figure 11

- **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 12).

Figure 12

  - **Order:** The order of appearance for Community rules is sorted incrementally. Enter the corresponding order for the rule.
  - **Text:** Enter the contents of the Community rule.
  - Click the **SAVE** button to create the new Community rule.
- **Footer**: Click **Edit** to create or edit a footer for the Community rules and guidelines.

Invites

Invite Users to a Community

1. Click **Community Info** at the upper-right corner of the **Community** card (Figure 2). The **Community Info** screen will be displayed (Figure 7).
2. Click the **Invites** tab. The **Invites** screen will be displayed (Figure 13).

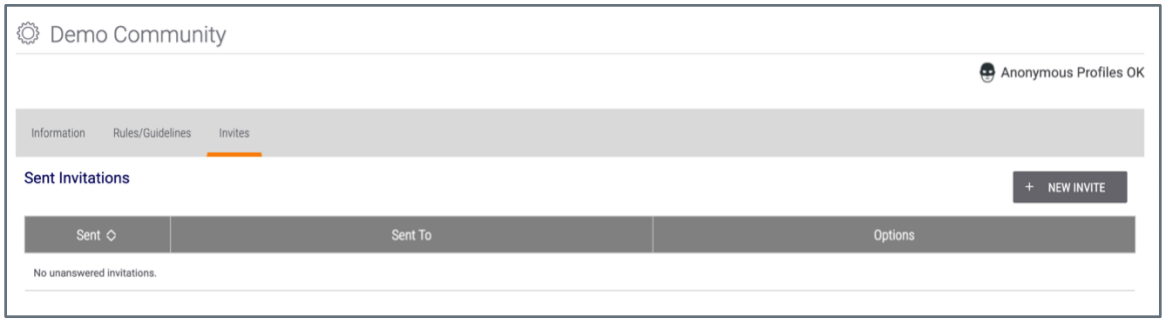

Figure 13

3. Click the **+ NEW INVITE** button. The **Send Community Invite** window will be displayed (Figure 14).

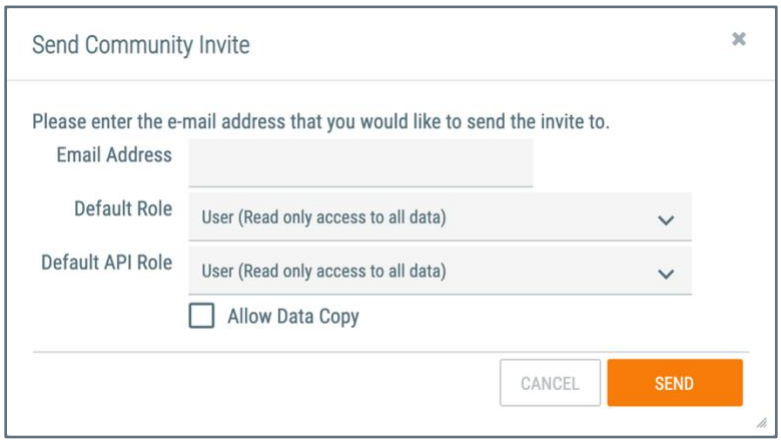

Figure 14

- **Email Address**: Enter the recipient's email address.

> **Important**: If the email address is not currently associated with an account, the recipient will be able to use the invite code provided in the email to join the Community after establishing an account.

- **Default Role**: Select the default role for the invited account. If it is an Org account, all user accounts in the Organization will inherit this role. If it is an individual account, then the account will be set to this role if the invitation is accepted.
- **Default API Role:** Select the default API role for all future API accounts created under this Organization.
- **Allow Data Copy**: Select the checkbox to allow invited users to copy data from this Community to their Organization.
- Click the **SEND** button to send the invitation.

Invite Users to a Source

1. Click **Source Info** at the upper-right corner of the **Source** card (Figure 3). The **Source Info** screen will be displayed (Figure 8).
2. Click the **Invites** tab. The **Invites** screen will be displayed (Figure 15).

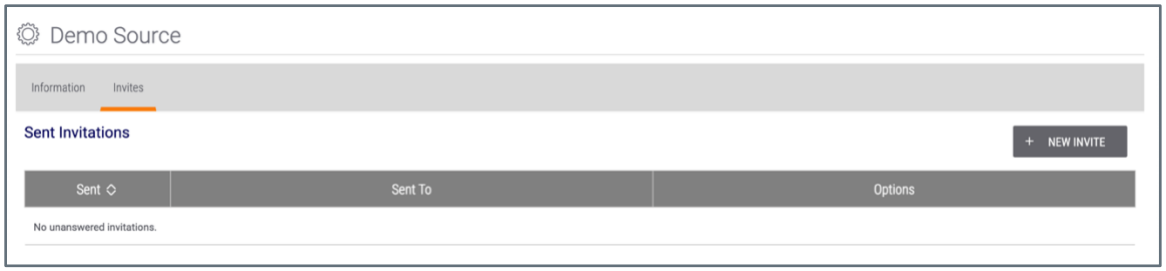

Figure 15

3. Click the **+ NEW INVITE** button. The **Send Source Invite** window will be displayed (Figure 16).

Figure 16

- **Email Address**: Enter the user's email address.

- **Allow Data Copy**: Select the checkbox to allow the user to copy data from the Source to their Organization.
- Click the **SEND** button to send the Source Invite.

The Community (and Source) Config Screen

Access the Community (or Source) Config Screen

1. Log into ThreatConnect with an Editor or Director account for the Community or Source.
2. On the top navigation bar, click **Posts**. The **Posts** screen will be displayed (Figure 1).
3. Select the desired Community or Source in the **My ThreatConnect** card to display its **Community** (Figure 2) or **Source** (Figure 3) screen.
4. Click **Community** (or **Source**) **Config** at the upper-right corner of the **Community** or **Source** card. The **Community Config** (Figure 17) or **Source Config** screen (Figure 18) will be displayed with the **Attribute Types** selected. See the "Attribute Types" section for more information on this tab.

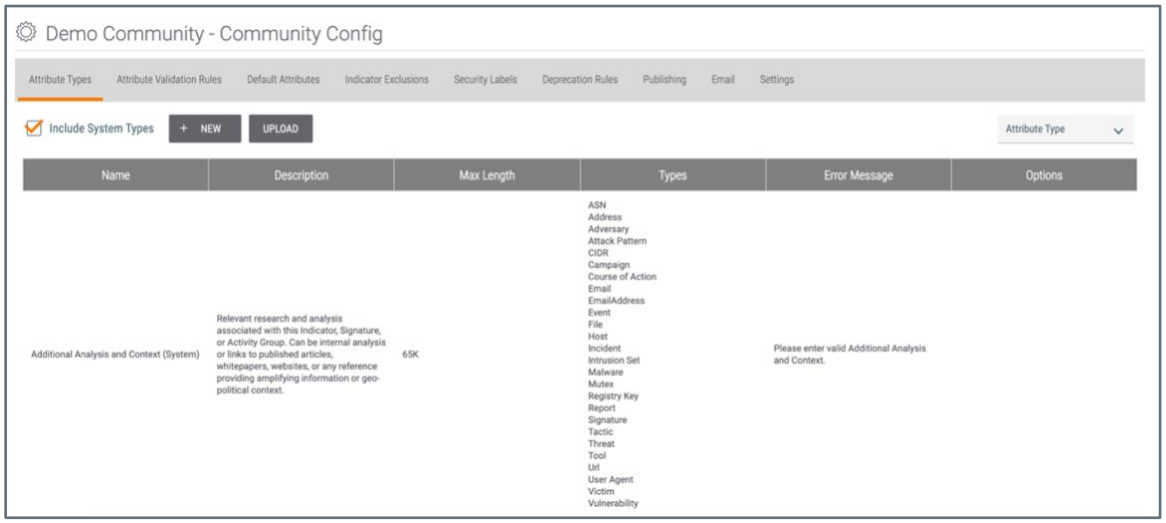

Figure 17

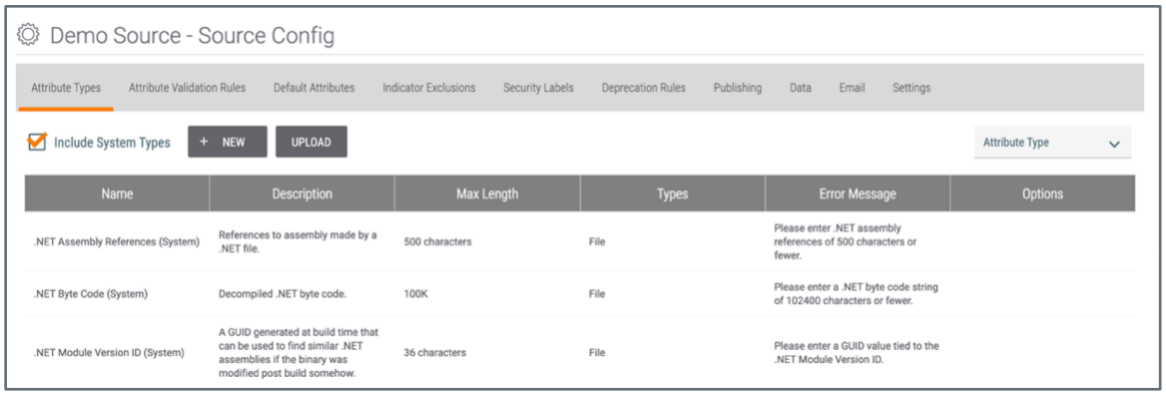

Figure 18

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*.

Attribute Types

Community and Source Administrators can create Attribute Types for use across all their Communities and Sources. Any Organization that is a member of a particular Community or Source will have access to its Attribute Types, in addition to System Attribute Types and the respective Organization's own Attribute Types.

The **Attribute Types** tab of the **Community Config** (Figure 17) and **Source Config** screen (Figure 18) displays existing custom Community or Source Attribute Types, respectively, and System Attribute Types, if the **Include System Rules** checkbox is selected.

Create Attribute Types

Click the **+ NEW** button on the **Attribute Types** screen. The **Configure Attribute Type** window will be displayed (Figure 19).

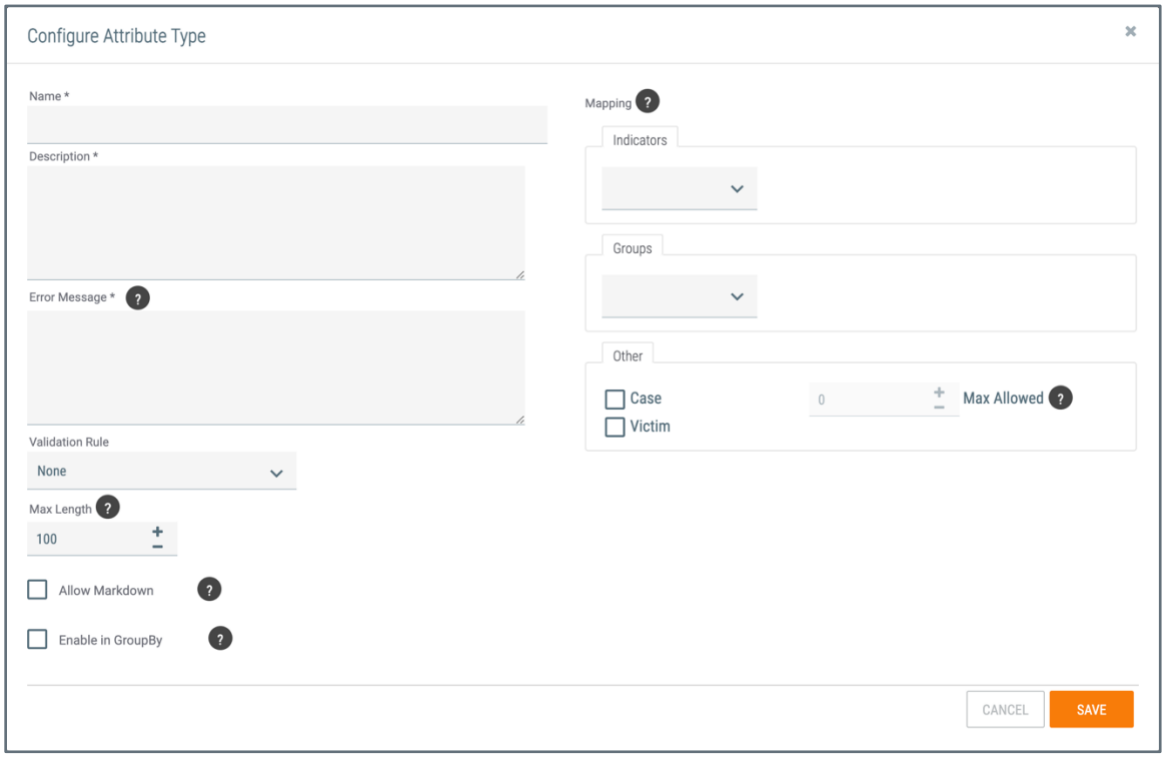

Figure 19

- **Name**: Enter the name of the Attribute Type as it will be displayed in menus and on the **Details** screen for Indicators and Groups.
- **Description**: Enter a description of the System Attribute Type as seen by users when inputting a value for the Attribute Type or when viewing it from the **Details** screen.
- **Error Message**: Enter the message displayed when users try to input a value that does not meet the System Attribute Type's Validation Rules.
- **Validation Rule**: Select the schema that determines whether a user's input is valid when logging an Attribute Type for an Indicator or Group. ThreatConnect is preloaded with a variety of Validation Rules, such as for IP Addresses, Dates, and Country Codes. System, Community, and Organization Administrators can define their own System Attribute Type Validation Rules as needed.
- **Max Length**: Enter the maximum size (in characters) of the System Attribute Type, if applicable, based on the Attribute Type's assigned Validation Rule.

- **Allow Markdown**: Select the checkbox to allow the Markdown language 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 dashboard 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 become enabled. This option allows a user 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 the **SAVE** button.

Upload Attribute Types

Click the **UPLOAD** button on the **Attribute Types** screen. The **Upload Attributes** window will be displayed (Figure 20).

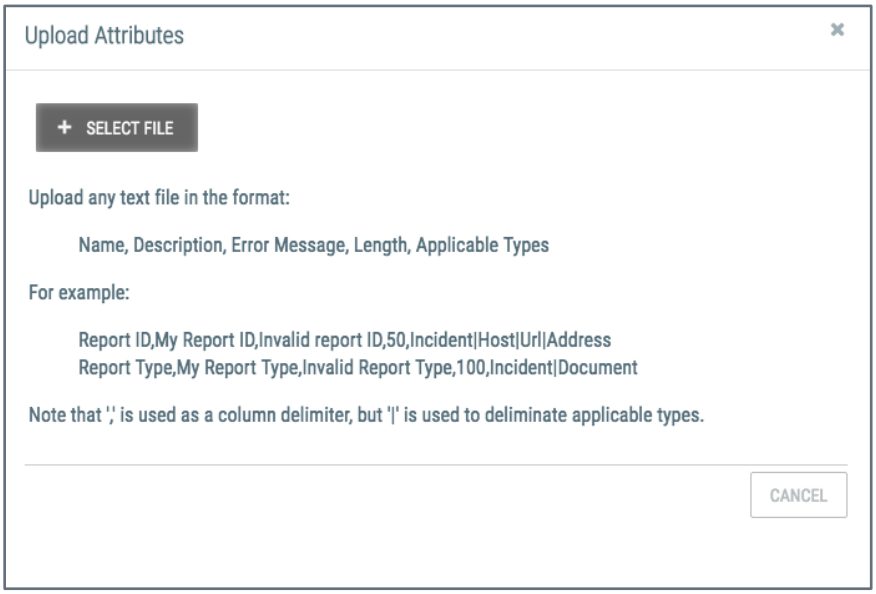

Figure 20

- Click the **+ SELECT FILE** button to locate and select a file to upload.
- After the file is uploaded, click the **SAVE** button.

Attribute Types can be uploaded in a text or JavaScript Object Notation (JSON) file. If uploading an Attribute Type via 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 an Attribute Type via a JSON file, refer to Table 2 for the fields that can be included in the file.

Table 2

Field	Required	Type
allowMarkdown	FALSE	Boolean
description	TRUE	String
errorMessage	TRUE	String
groups	FALSE	String
indicators	FALSE	String
maxLength	TRUE	Integer
name	TRUE	String
system	FALSE	Boolean
version	FALSE	Integer

Note: To upload an Attribute Type as a System Attribute Type, assign the `system` field a value of `true`.

Note: Upon creation of a new Attribute Type, the `version` field is automatically assigned a value of `1`.

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

The following is an example JSON file format used to upload an Attribute Type:

```
{
    "types": [{
        "allowMarkdown": true,
        "description": "Description of Attribute Type",
        "errorMessage": "Enter a valid value",
        "groups": [
            "Adversary",
            "Campaign",
            "Course of Action",
            "Document",
            "Email",
            "Incident",
            "Malware",
            "Threat"
        ],
        "indicators": [
            "Address",
            "EmailAddress",
            "File",
            "Host",
            "Url"
        ],
        "maxLength": 100,
        "name": "Attribute Type Name",
        "system": false,
        "version": 2
    }]
}
```


Edit Attribute Types

Click **Edit** in the **Options** column for the desired Attribute Type. The **Configure Attribute Type** window will be displayed (Figure 19). Configure the fields for the custom Attribute Type as appropriate, and then click the **SAVE** button.

Delete Attribute Types

Click **Delete** in the **Options** column for the desired Attribute Type. The **Delete Attribute Type** window will be displayed. Click the **YES** button to delete the Attribute Type.

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 21) displays the Attribute validation rules available to all Communities and Sources, respectively, on the ThreatConnect instance (that is, the System Attribute validation rules; see the *ThreatConnect System Administration Guide* for more information), as well as the Attribute validation rules specific to the Community and Source (i.e., custom Attribute validation rules), respectively.

Figure 21

Create Attribute Validation Rules

Click the **+ NEW** button on the **Attribute Validation Rules** screen. The **Create Attribute Validation Rule** window will be displayed (Figure 22).

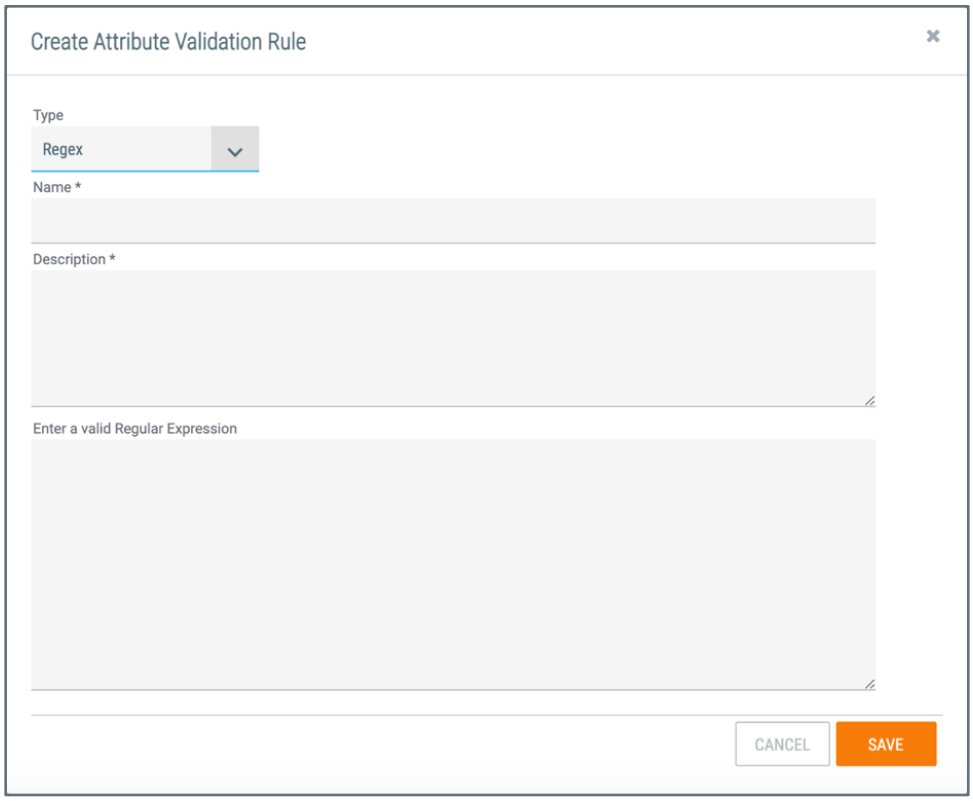

Figure 22

- **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 only considers 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**: presented as a dropdown menu of options—after the Administrator defines the options in the text box on the right—from which users may only select one value (e.g., high, medium, or low priorities)
  - **Select One Radio**: similar to Select One Picklist, but presented as a series of radio buttons
  - **Date**
  - **Date/Time**
  - **Integer:** a whole number, valid in the range specified in the text box on the right (e.g., 0:1440 for "minutes worked")

- **Name**: Enter the name of the Validation Rule as it will be displayed in the **Create Attribute** window (Figure 19) described previously.
- **Description**: Enter, as applicable, a general description of the Validation Rule.
- **Enter a valid Regular Expression:** If applicable, enter the parameters for a Validation Rule as defined previously.
- Click the **SAVE** button to save the new Attribute Validation Rule.

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

Edit Attribute Validation Rules

Click **Edit** in the **Options** column for a custom Attribute Validation Rule (Figure 23). The **Create Attribute Validation Rule** window will be displayed (Figure 22).

> **Note**: To quickly find the custom Attribute Validation Rule to modify, deselect the **Include System Rules** checkbox.

Figure 23

Configure the fields for the custom Attribute Validation Rule as appropriate, and then click the **SAVE** button.

Delete Attribute Validation Rules

Click **Delete** in the **Options** column for a custom Attribute Validation Rule (Figure 23). The **Delete Attribute Validation Rule** window will be displayed. Click the **YES** button to delete the custom Attribute Validation Rule.

Default Attribute Types

To keep an object's **Details** screen from being cluttered, few Attribute Types are prepopulated. However, Administrators may choose to set placeholder default Attribute Types for a Group or Indicator to remind users to populate them as soon as the Group or Indicator is created.

The **Default Attributes** tab of the **Community Config** and **Source Config** screen (Figure 24) displays the existing default Attribute Types for the Community and Source, respectively.

Figure 24

Create Default Attribute Types

Click the **+ NEW** button on the **Default Attributes** screen. The **Create Default Attribute Type** window will be displayed (Figure 25).

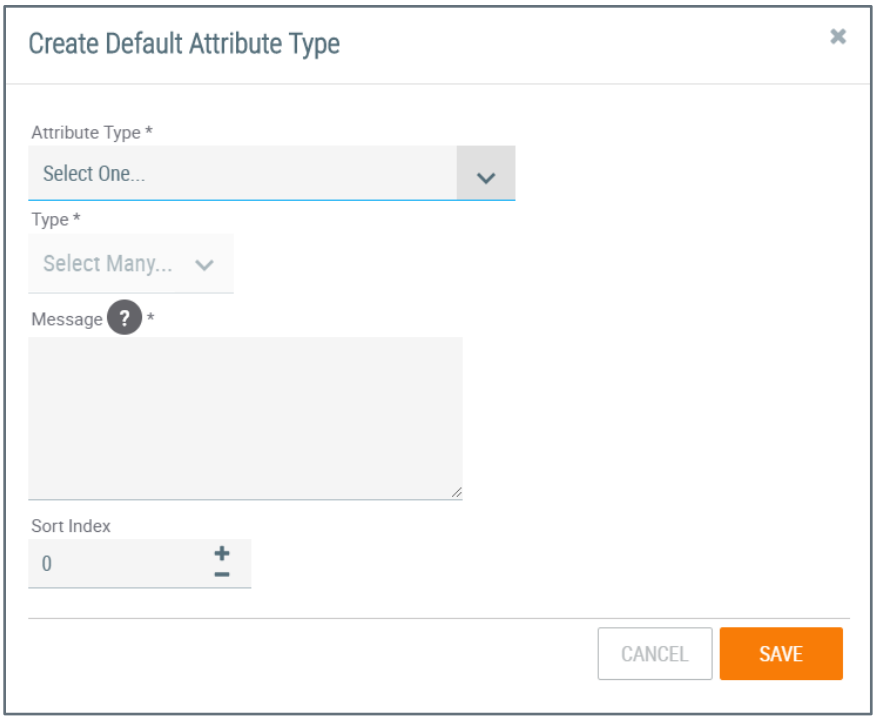

Figure 25

- **Attribute Type**: Select an Attribute Type defined on the **Attribute Types** tab of the **Community Config** screen (Figure 17).

  Note: These options will also include System Attribute Types if the **Include System Types** checkbox is selected on the **Community Config** screen.

- **Type**: Select any applicable Indicators or Groups to which to apply the selected default Attribute Type.

  Important: Only entities that were approved when the Attribute Type was created can be specified.

- **Message**: Enter a string to prompt users to populate this default Attribute Type. The string links to a dialog box to edit the appropriate Attribute Type.
- **Sort Index**: Enter the index used to arrange default Attribute Types. Indices are set in ascending order, meaning that the Attribute ranked **0** will be at the top of the Attribute Types list, and the Attribute Type ranked with the highest number will be at the bottom.
- Click the **SAVE** button.

Edit Default Attribute Types

Click **Edit** in the **Options** column for a default Attribute Type. The **Create Attribute Validation Rule** window will be displayed (Figure 25). Configure the fields for the default Attribute Type as appropriate, and then click the **SAVE** button.

Delete Default Attribute Types

Click **Delete** in the **Options** column for a default Attribute Type. The **Delete Default Attribute Type** window will be displayed. Click the **YES** button to delete the default Attribute Type.

Indicator Exclusions

The purpose of creating an Indicator Exclusion list is to prevent the importation of Indicators that may be deemed legitimate or non-hostile by an Administrator. ThreatConnect allows a user to create an Indicator Exclusion list at the System, Organization, Community, or Source level. The Community- or Source-level list is configured through the **Indicator Exclusions** tab **Community Config** or **Source Config** screen (Figure 26), respectively.

Figure 26

Create Indicator Exclusion Lists

Click **Edit** in the **Options** column for an Indicator (File-SHA1 in this example). The **Exclusion Details** window will be displayed (Figure 27).

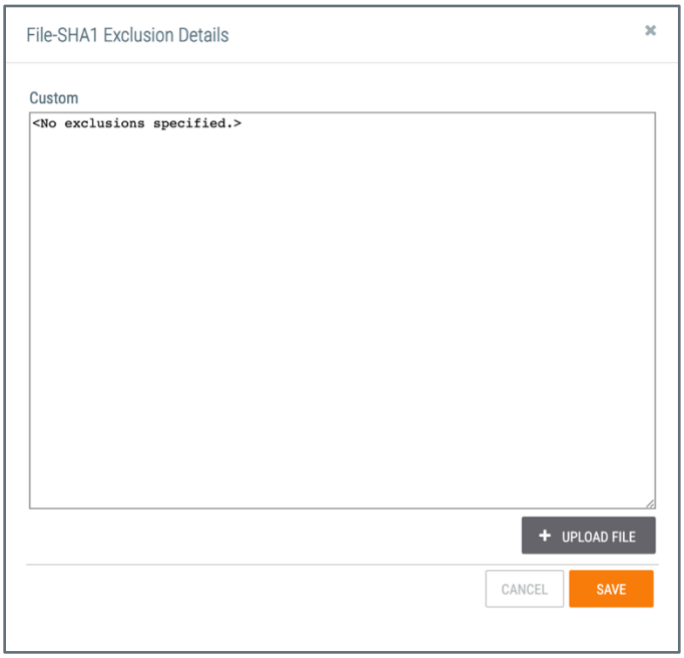

Figure 27

- **Custom**: When creating a new Exclusion List, enter the information directly into the **Custom** text box.
- **+UPLOAD FILE**: Click the **+ UPLOAD FILE** button to navigate to locate and select a file to upload. After a file is selected, the Exclusion list will be uploaded.

  Note: The file must be in **.txt** format. Also, place an asterisk (*) at the beginning and end of the Indicator to exclude all results. For example, ***xyz.com*** in the URL Exclusion list would exclude any URL that contains the string **xyz.com**.

- Click the **SAVE** button.

Edit Indicator Exclusion Lists

Click **Edit** in the **Options** column for an Indicator. The **Exclusion Details** window will be displayed (Figure 27). Edit the Exclusion List directly from the **Custom** text box, or click the **DOWNLOAD** button to download and edit a file, and then click the **+ UPLOAD FILE** button to upload the edited file (Figure 28).

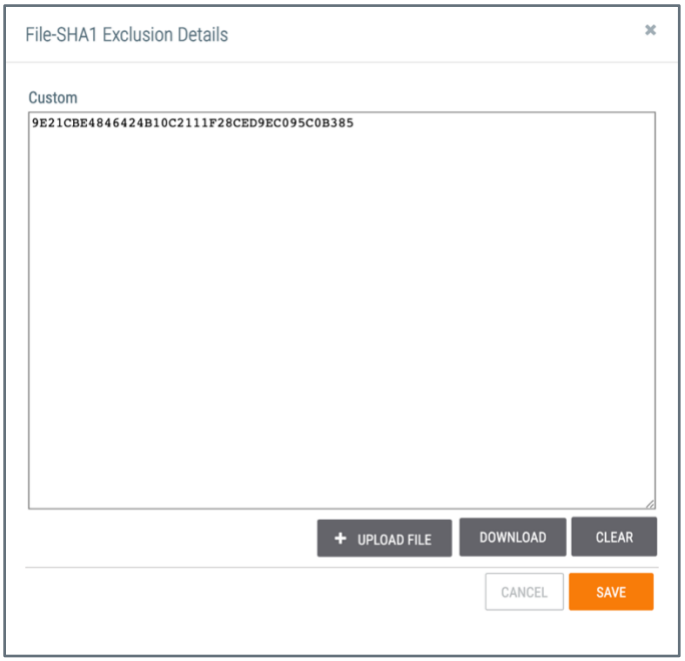

Figure 28

After all changes are made, click the **SAVE** button.

Note: When trying to create an Indicator that has been placed on an Exclusion list, a message will be displayed in the **Create** window warning that the Indicator is contained on a Community- or Source-wide Exclusion list.

Delete Indicator Exclusion Lists

Click **Edit** in the **Options** column for an Indicator. The **Exclusion Details** window will be displayed (Figure 28).

Click the **CLEAR** button. The **Remove Exclusions** window will be displayed. Click the **YES** button, and then click the **SAVE** button on the **Exclusion Details** window.

Security Labels

Directors can define Security Labels for use by all member Organizations. Security Labels are a good way to designate how information should be treated. Within the Common Community, ThreatConnect uses the Traffic Light Protocol (TLP) system published by the Forum of Incident Response and Security Teams™ (FIRST). Administrators can define their own Security Labels based on their Community's or Source's needs and policies.

The **Security Labels** tab of the **Community Config** and **Source Config** screen (Figure 29) displays existing custom Community and Source Security Labels, respectively, and System Security Labels, if the **Include System Labels** checkbox is selected.

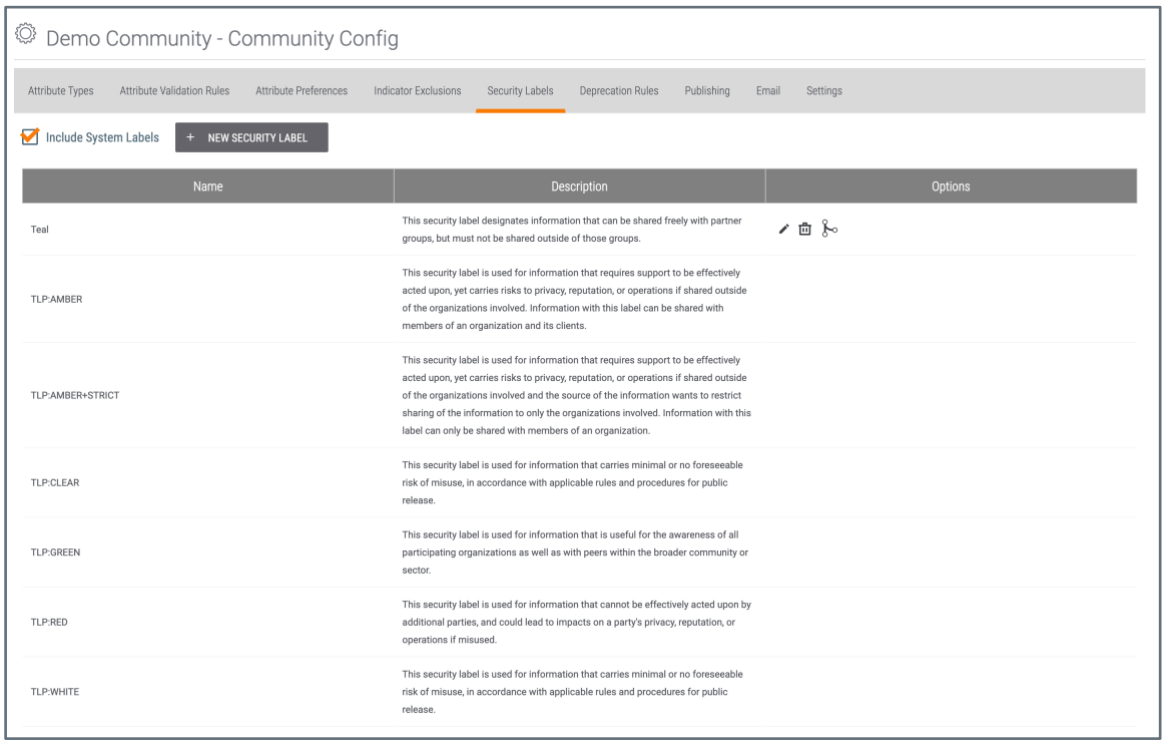

Figure 29

Create Security Labels

Click the **+ NEW SECURITY LABEL** button on the **Security Labels** screen. The **Create Security Label** window will be displayed (Figure 30).

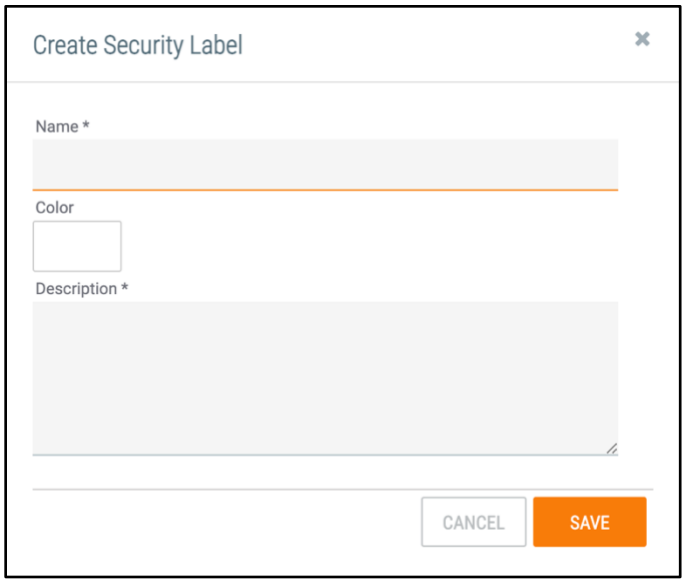

Figure 30

- **Name**: Enter a name for the Security Label.
- **Color**: Click in the box to display the color picker. Users can enter a color value in RGB, HSB, or hexadecimal format, or select a color by clicking and dragging the circle in the color field.
- **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 the **SAVE** button.

Edit Security Labels

Click **Edit** in the **Options** column for the desired custom Security Label. The **Create Security Label** window will be displayed (Figure 30). Make the desired changes to the Security Label, and then click the **SAVE** button.

Delete Security Labels

Click **Delete** in the **Options** column for the desired custom Security Label. The **Delete Security Label** window will be displayed. Click the **YES** button to delete the Security Label.

Consolidate Security Labels

Click **Consolidate** in the **Options** column for the desired custom Security Label. The **Consolidate Security Label** window will be displayed (Figure 31).

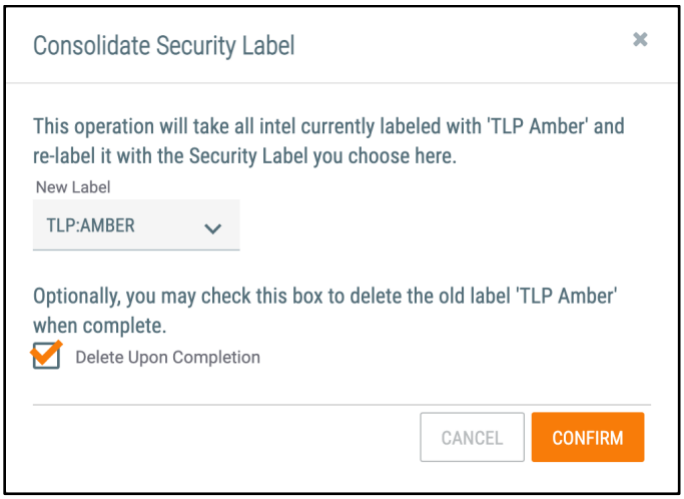

Figure 31

- **New Label**: Select the new Security Label that will be applied to all intel currently labeled with the old Security Label.
- **Delete Upon Completion**: Select the checkbox to delete the old Security Label after consolidation is complete.
- Click the **CONFIRM** button.

Apply Security Labels

Security Labels are most effective when users share or contribute information within ThreatConnect—which allows them to withhold and divulge information with respect to their Organization's policies, based on the Security Label applied to each piece of data. Any Community or Source Security Labels will be available to all users and Organizations within a Community or Source.

Security Labels are applied not just to Groups and Indicators, but also to their Attribute Types. For example, an IP Address Indicator may be considered **TLP:Green** (i.e., peers and partner Organizations may see it). However, its Source Attribute Type may be a sensitive system log that pinpoints a system vulnerability and, thus, may be considered **TLP:Red** (i.e., not to be shared). Administrators are encouraged to familiarize their users with their Community's sharing policies and the Security Labels used to enact them.

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. See *ThreatConnect Account Administration Guide* for instructions on configuring System-wide confidence deprecation rules.

The **Deprecation Rules** tab of the **Community Config** or **Source Config** screen (Figure 32) displays the confidence deprecation rules that have been created for the Community or Source, respectively.

Figure 32

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

Click **Edit** in the **Options** column for the desired confidence deprecation rule. The **Create/Edit Deprecation Rule** window will be displayed (Figure 33). See *Configuring Indicator Confidence Deprecation* for further instruction.

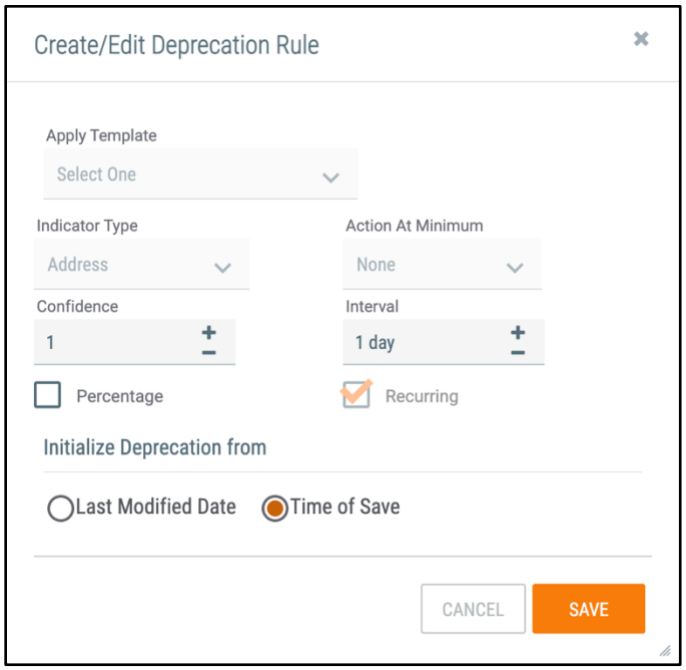

Figure 33

Delete Deprecation Rules

Click **Delete** in the **Options** column for the desired confidence deprecation rule. The **Delete Deprecation Rule** window will be displayed. Click the **YES** button to delete the Deprecation Rule.

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 instances of the platform. Once a Group has been published, it can be shared across instances via the Cross-Intel Sharing App.

All types of Group data objects (Adversary, Attack Pattern, Campaign, Course of Action, Document, E-mail, Event, Incident, Intrusion Set, Malware, Report, Signature, Tactic, Task, Threat, Tool, and Vulnerability) 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 accessible by navigating to the **Browse** screen and then selecting a Group object from the table that is displayed. The **Publishing** tab of the **Community Config** and **Source Config** screen (Figure 34) allows users to view, download, and delete JSON files published in the Community and Source, respectively.

Figure 34

View and Download Published Files

Users can determine which type(s) of published files to display on the **Publishing** screen 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 the published file to be downloaded. The file will be saved to the computer's **Downloads** folder.

Delete Published Files

Click **Delete** in the **Options** column for the published file to be deleted. The **Delete Publication** window will be displayed. Click the **YES** button to delete the published file.

Data

The **Data** tab of the **Source Config** screen (Figure 35) allows users to create a variety of Source feeds, including HTTP Feeds, and inbound and outbound TAXII Exchange Feeds.

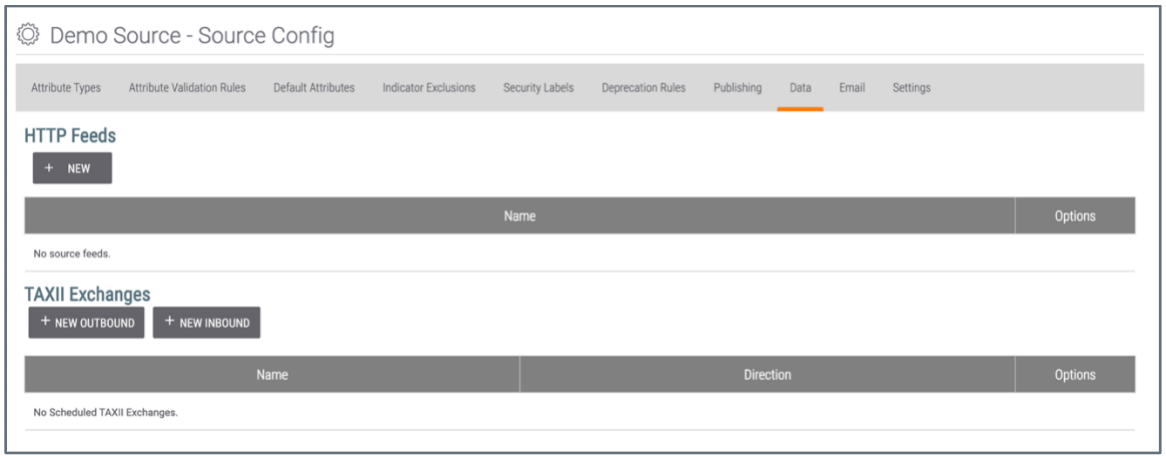

Figure 35

HTTP Feeds

Organization Administrators 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 steps 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 steps 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 steps 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 the ThreatConnect instance to receive feed or phishing 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 36) allows users to create phishing and feed mailboxes in the Community and Source, respectively.

Figure 36

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, the Administrator must specify if the mailbox is meant to receive emails directly from network devices or if it is meant to receive email headers in the form of attachments. ThreatConnect will parse these emails, and when the parsing is complete, if an email meets the minimum email scoring threshold, then ThreatConnect will create an E-mail Group object and Task Group object and link previously

existing Indicators to the E-mail Group object if they are found in the header or body. 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. When the parsing is complete, ThreatConnect will create a Document object from the email's body, create any Indicators that matched the pre-defined feed mailbox regular expressions, and associate the Indicators to the Document.

1. Click the **Create Feed Mailbox** button on the **Email** screen. The **Feed Mailbox Administration** window will be displayed with the **Mailbox** tab selected (Figure 37).

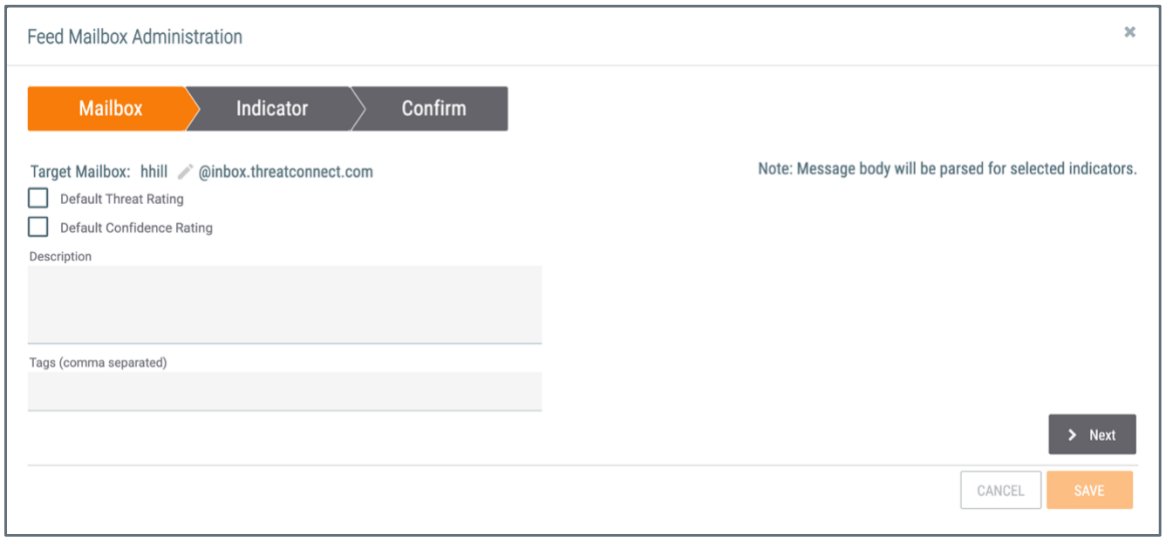

Figure 37

- **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 any Tags, separated by commas, for the Feed Mailbox.
- Click the **Next** button.

2. The **Indicator** tab will be displayed (Figure 38).

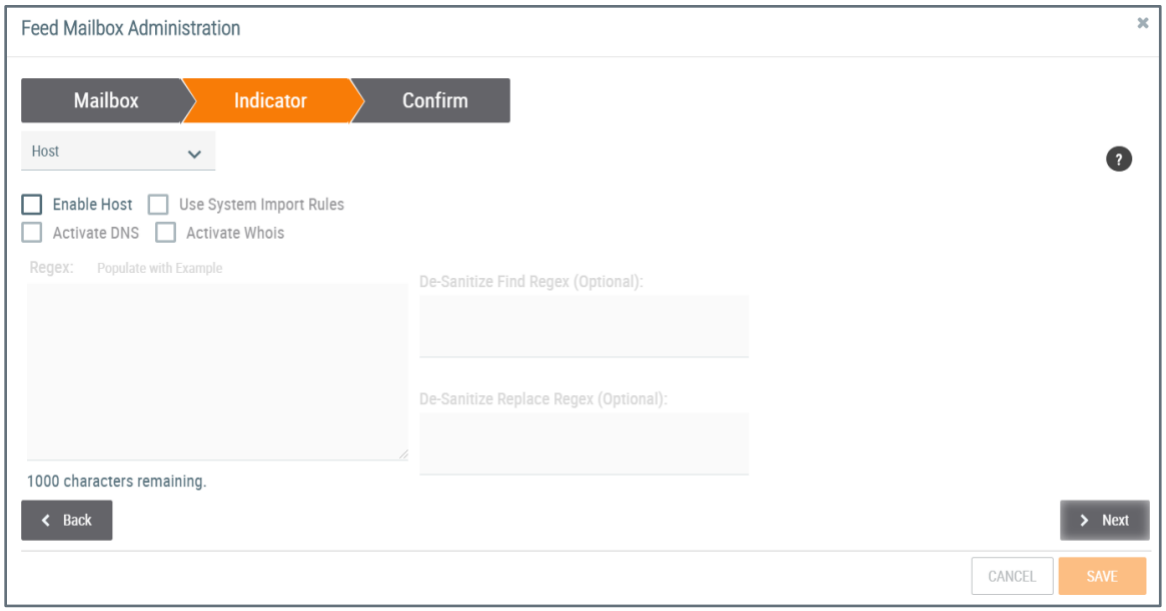

Figure 38

- ‹*Indicator name*›: Select an Indicator type from the dropdown menu. Available Indicator types include **Host**, **Address**, **E-mail Address**, **File**, **URL**, and any custom Indicators that have been added, including ThreatConnect's five built-in custom Indicators. By default, the **Host** Indicator is selected.
- **Enable** ‹*Indicator name*›: Select this checkbox to enable the detection of sanitized Indicators.
- **Use System Import Rules**: Select this checkbox to use the standard import rules run by the system to import the selected Indicator.
- **Activate DNS**: Select this checkbox to activate DNS tracking on the Host Indicator. This option is not displayed for other Indicator types.
- **Activate Whois**: Select this checkbox to activate Whois tracking on the Host Indicator. This option is not displayed for other Indicator types.
- **Regex**: If the **Enable** ‹*Indicator name*› is selected, the user can enter regular expressions to run against the text in an email. The regular expressions should handle sanitized Indicators.
- **De-Sanitize Find Regex (Optional)**: Enter regular expressions to find sanitized Indicator text.
- **De-Sanitize Replace Regex (Optional)**: Enter regular expressions to replace sanitized Indicator text.

> **Note**: Hovering over the **Question Mark** icon at the upper-right corner of the screen displays explanations and examples to help define the criteria for each Indicator Type.

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

- Click the **Next** button.

3. The **Confirm** tab screen will be displayed (Figure 39).

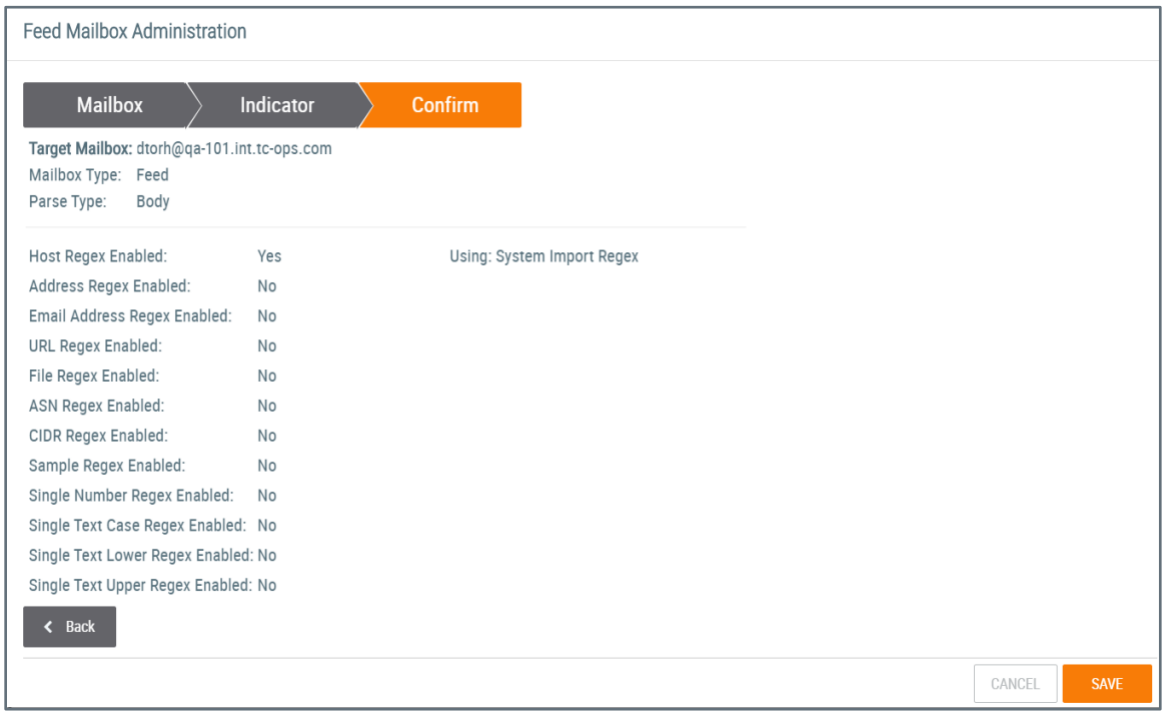

Figure 39

- Review the selections made on the previous tabs.
- Click the **SAVE** button.

Settings

The **Settings** tab of the **Community Config** and **Source Config** screen (Figure 40) allows users to add a DomainTools™ API key in order to enable DomainTools for all Reverse Whois Track queries for a Community or Source, respectively.

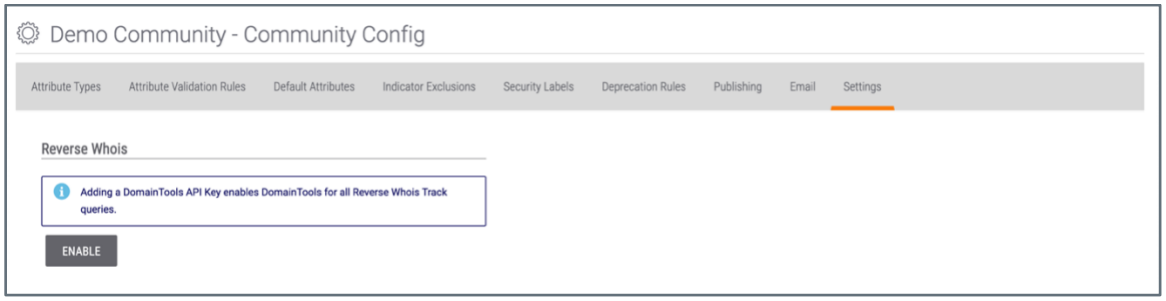

Figure 40

Enable DomainTools

Click the **ENABLE** button on the **Settings** screen. The **Setup DomainTools** window will be displayed (Figure 41).

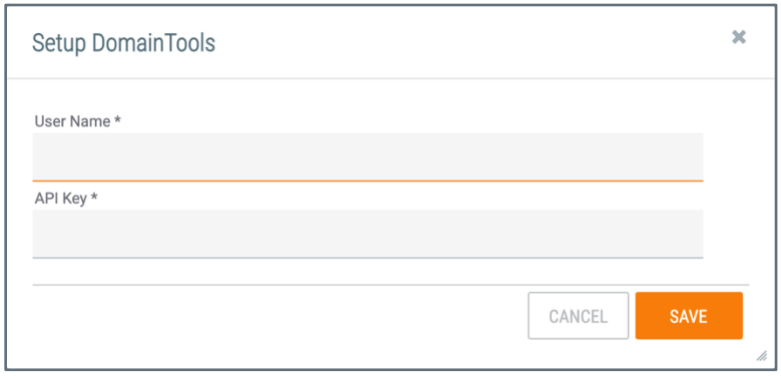

Figure 41

- **User Name**: Enter a username for the account.
- **API Key**: Enter a valid API key to enable DomainTools.
- Click the **SAVE** button.