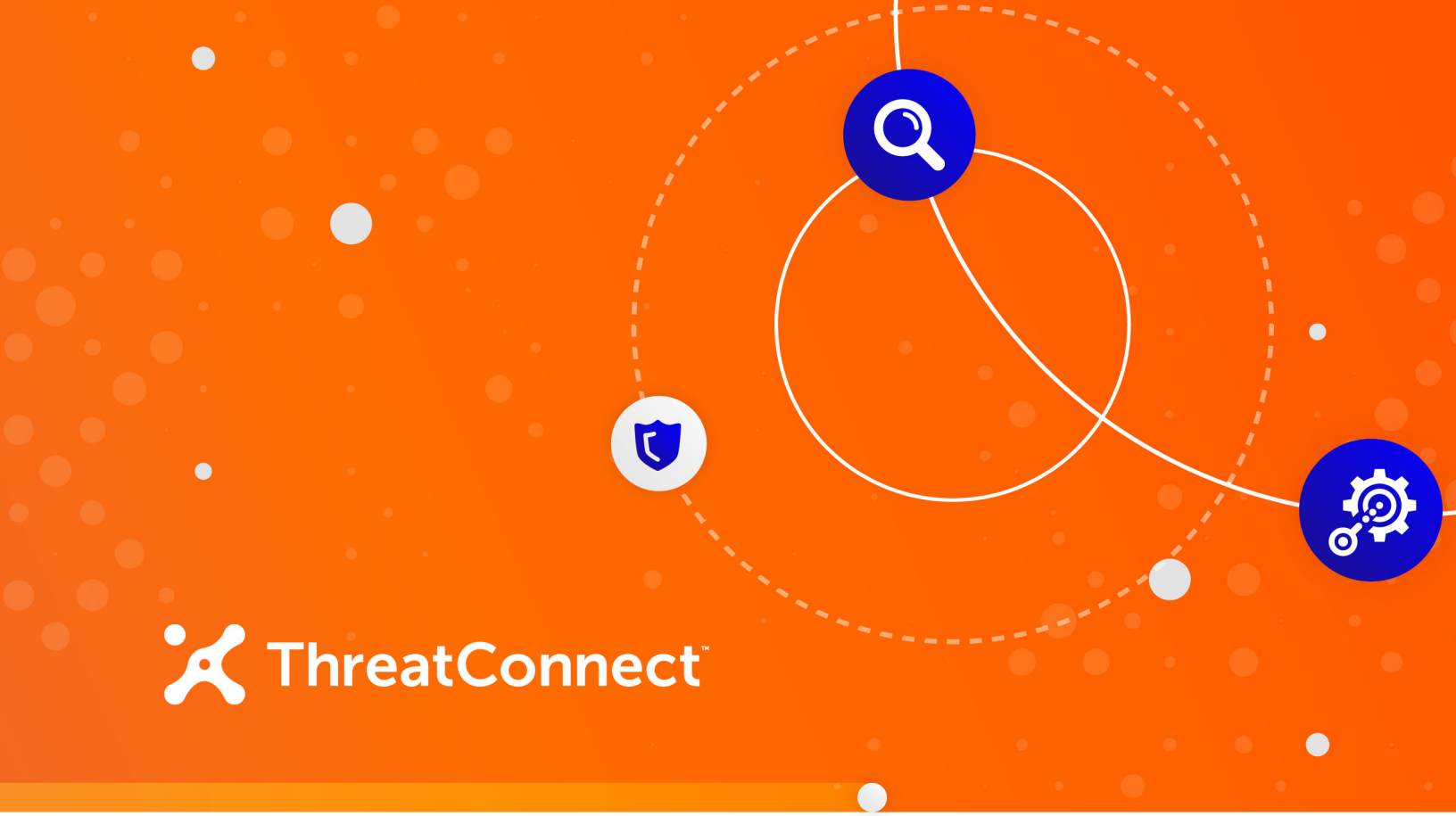

ThreatConnect™

Community and Source Administration

User Guide

Software Version 6.1

February 24, 2021

10011-09 EN Rev. A

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

P: 1.800.965.2708 | F: 1.703.229.4489
www.ThreatConnect.com

Table of Contents

Introduction

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 **Access** and **Roles**, **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. In order to access the Community or Source Configuration or Info options, a user will need to log in with an Organization Administrator account or higher. Then, on the top navigation bar(Figure 1) click on **Posts**, and then select the appropriate Community or Source. This is the simplest way to access the Community or Source Configuration or Info options, and the way that will be used in this guide.

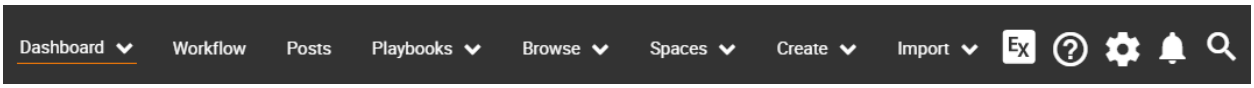

Figure 1

Another way to access Community or Source Configuration or Info options is to log in with a System Administrator account. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon, and the **Settings** menu will appear (Figure 2).

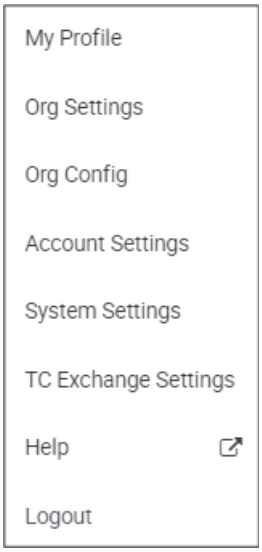

Figure 2

Select **ACCOUNT SETTINGS**. The **Account Settings** screen will appear. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will appear. From this screen, click on an entry to display its **Community** or **Source Info** screen. Then click the **COMMUNITY CONFIG** button to access the **Community Config** screen.

Community Access and Roles

Table 1 displays Community Roles and their descriptions.

Table 1

Community Role	Description
Director	Directors have the same privileges as Editors, but they can also add new users to the Community and assign roles to existing users. In Private Communities, the user that created the Community will be the default Community Administrator. Directors may also delegate this privilege to other users inside, or external to, their Organization.
Editor	Editors can create, delete, or modify any information in the Community. In Private and Industry Communities, vetted users may be given Editor privileges to act as a moderator for all Community data.
Contributor	Contributors can create new data, and they have limited Editor capabilities. They can add Attribute Types, but they cannot delete or edit Indicators or existing Attribute Types posted by others. Most users within Communities will have this role.
Commenter	Commenters can create new Attribute Types and Comments on Indicators and Groups in a Community, but are not allowed to add Associations, new Indicators, or new Groups.
User	Users have read-only access. They do not have write or update access.
Subscriber	Subscribers have read-only access to published data.
Banned	Banned account holders are not permitted access to a Community, including its data or posts.

Configuring Community 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, be able to user their full profile.

NOTE: Many of the following functions can also be performed by clicking on the Posts menu option on the navigation bar and then accessing the Info screen for a Community, Source, or Organization by clicking on its name in the** My ThreatConnect **column.

Follow these steps to configure Community Roles:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community.
2. On the top navigation bar (Figure 1), click **Posts** and the **Posts** screen will appear (Figure 3).

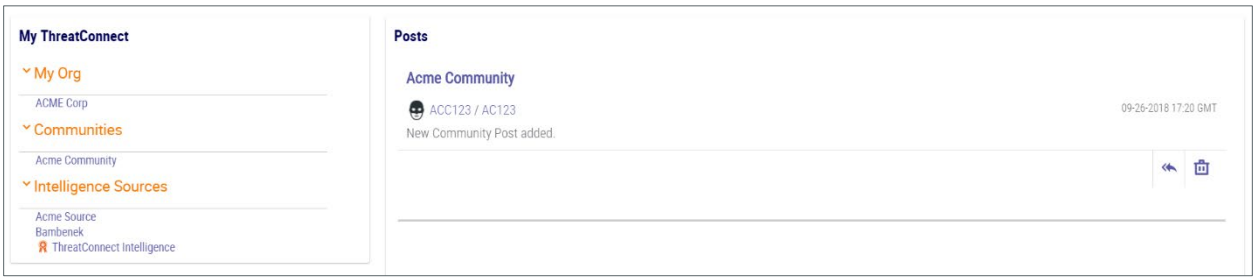

Figure 3

3. Click on the desired Community in the **My ThreatConnect** column, and its **Community** card will appear on the top left of the screen (Figure 4).

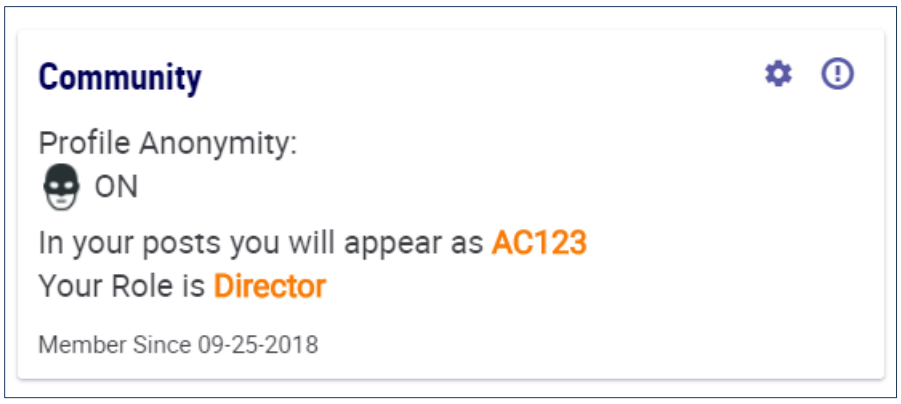

Figure 4

4. Click on the **Community Info**  icon, and the **Community Info** screen will appear (Figure 5).

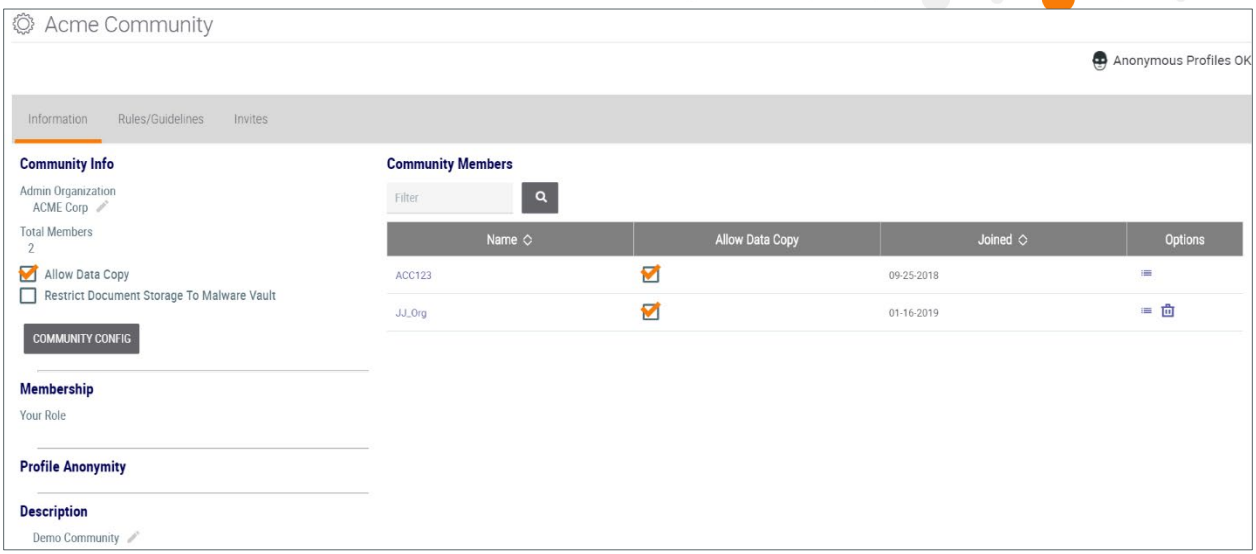

Figure 5

5. Click the corresponding **Users** icon in the **Options** column on the right-hand side for the Community Member to be configured. The **Membership** pop-up screen will appear (Figure 6).

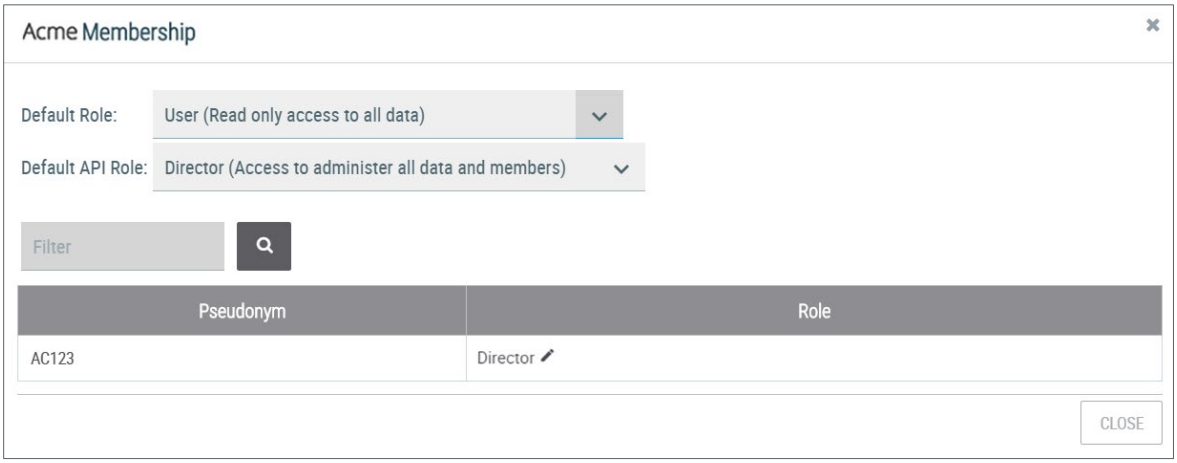

Figure 6

a. **Default Role**: Click on the drop-down menu to set the default role for all future Org members created under this Organization.

b. **Default API Role**: Click on the drop-down menu to set the default API role for all future API accounts created under this Organization.

c. **Role** (of Individual Users): Click on the **Edit** icon next to a role in order to configure it. All changes are applied immediately.

6. Click the **CLOSE** button when done.

Configuring a Community's Rules and Guidelines

Follow these steps to configure a Community's rules and guidelines:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community, and its **Community** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community Info**  icon, and the **Community Info** screen will appear (Figure 5).
5. Click the **Rules/Guidelines** tab, and the **Rules/Guidelines** screen will appear (Figure 7).

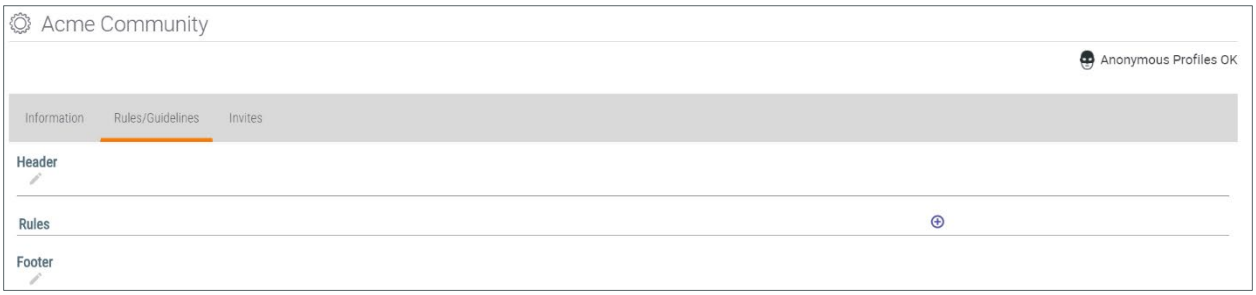

Figure 7

a. **New Rule**: Click on the **New Rule**  icon to add a new rule to the Community. The rules' order of appearance is sorted incrementally, and the order value can be modified.

b. **Edit Header**: Click on the top **Edit**  icon to create or edit a header for the Community rules and guidelines.

c. **Edit Footer**: Click on the bottom **Edit**  icon to create or edit a footer for the Community rules and guidelines.

d. For existing rules, the **Edit**  icon will be displayed. Click on the icon to edit the rule.

e. For existing rules, the **Delete**  icon will be displayed. Click on the icon to delete the rule.

Inviting Users to a Community

Follow these steps to invite users to a Community:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).

3. Click on the desired Community, and its **Community** card will appear on the top left of the screen (Figure 4).

4. Click on the **Community Info**  icon, and the **Community Info** screen will appear (Figure 5).

5. Click the **Invites** tab, and the **Invites** screen will appear (Figure 8).

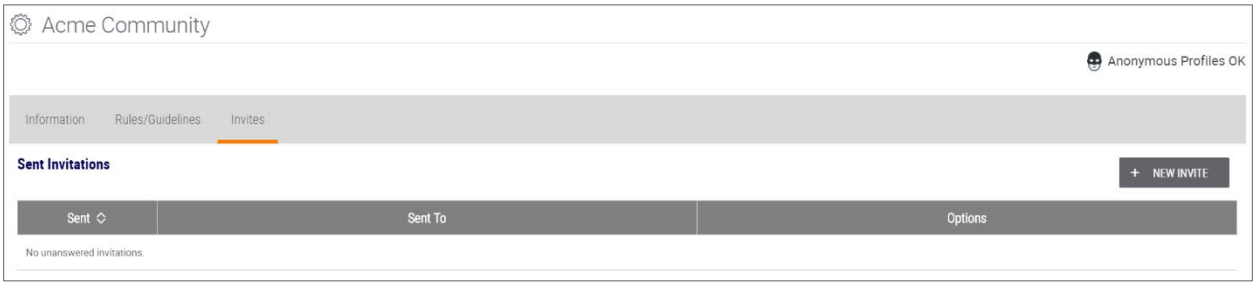

Figure 8

6. Click the **+ NEW INVITE** button, and the **Send Community Invite** pop-up screen will appear (Figure 9).

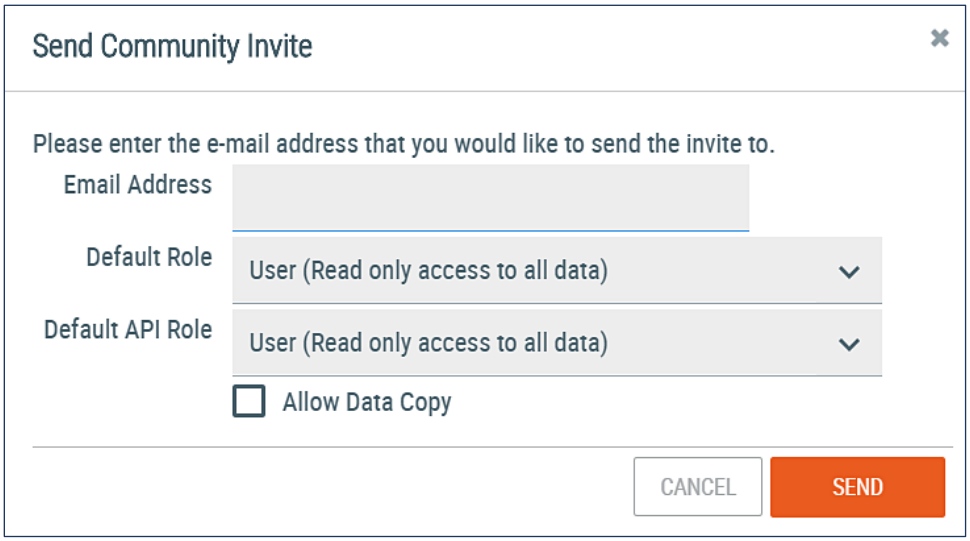

Figure 9

a. **Email Address**: Click in the box to enter the recipient's email address.

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

b. **Default Role**: Click on the drop-down menu to set 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 simply default to this role if it accepts the invitation.

c. **Default API Role:** Click on the drop-down menu to set the default API role for all future API accounts created under this Organization.

d. **Allow Data Copy**: Click the checkbox to allow invited users to copy data from this Community to their Organization.

7. Click the **SEND** button to send the invitation.

Setting Restrictions to Uploading Malware

Follow these steps to prevent users from accidentally uploading malware:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community.
2. On the top navigation bar (Figure 1), click **PostsError! Reference source not found.** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community, and its **Community** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community Info**  icon, and the **Community Info** screen will appear (Figure 5).
5. Click the **Restrict Document Storage to Malware Vault** checkbox. This restriction will now be enforced in three instances: when creating a document via the **Create Document** pop-up screen, when uploading a file to an existing document via the **Details** screen, and when creating an API document in a Community.

Community and Source Attribute Types

How Community and Source Attribute Types Work

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.

Creating Community and Source Attribute Types

Follow these steps to create a Community or Source Attribute Type:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).

Figure 10

NOTE: The Deprecation Rules and Email tabs, as well as the + NEW and UPLOAD buttons, will only be displayed if the corresponding options were selected when creating the Community.

5. Click the **+ NEW** button, and the **Configure Attribute Type** pop-up screen will appear (Figure 11).

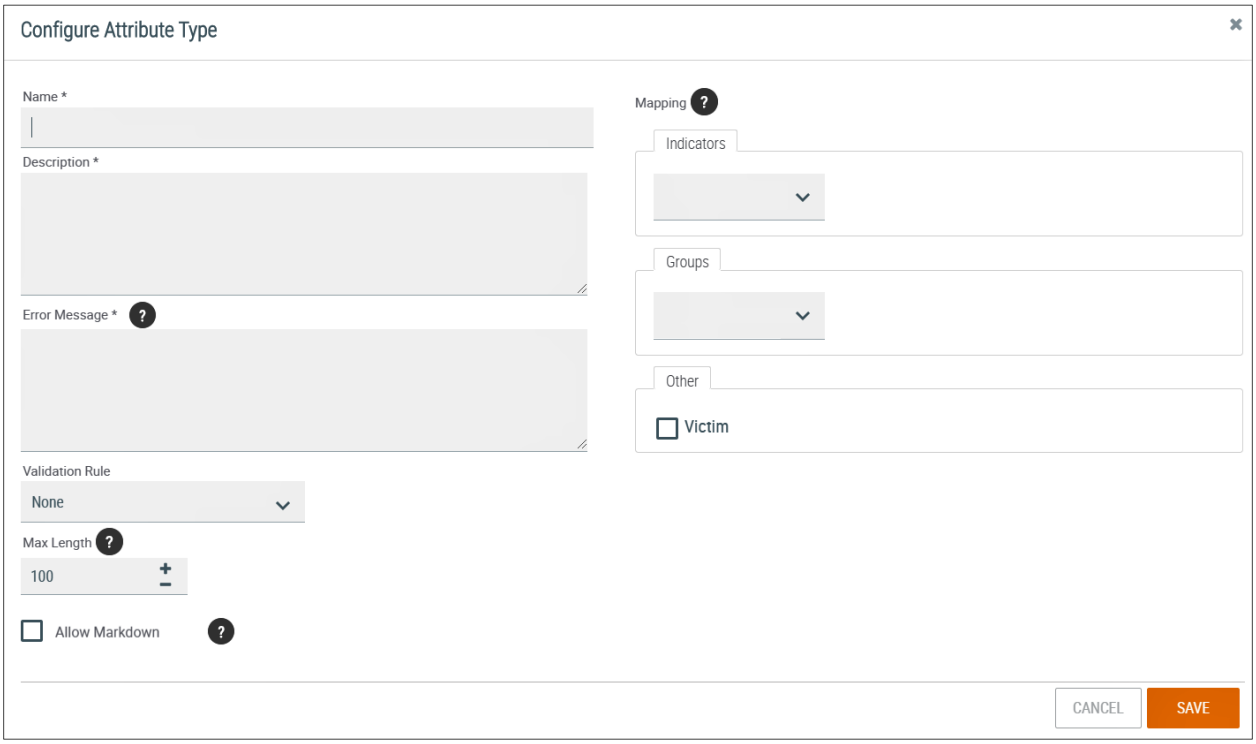

Figure 11

a. **Name**: Click in the box to enter the name of the Attribute Type as it will appear in menus and on the **Details** screen for Indicators and Groups.

b. **Description**: Click in the box to 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.

c. **Error Message**: Click in the box to enter the message presented when users try to input a value that does not meet the System Attribute Type's Validation Rules.

d. **Validation Rule**: Click on the drop-down menu to 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, Country Codes, etc. System, Community, and Organization Administrators are able to define their own System Attribute Type Validation Rules as needed.

e. **Max Length**: Click in the box (or use the plus and minus signs) to manually enter the maximum size, in characters, of the System Attribute Type, if applicable, based on the Attribute Type's assigned Validation Rule.

f. **Allow Markdown**: Click this checkbox to allow the Markdown language to be used when configuring an Attribute Type.

NOTE: Markdown is a markup language used to transform text into HTML for the purpose of formatting. ThreatConnect supports the use of Markdown with several Attribute Types, including Description and Source.

g. **Mapping**: Click the drop-down arrows for Indicators or Groups, and then click on the desired checkboxes to specify the types of entities to which this 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.

6. Click the **SAVE** button to create the custom Attribute Type.

Uploading a Community or Source Attribute Type

Follow these steps to upload a Community or Source Attribute Type:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **UPLOAD** button, and the **Upload Attributes** pop-up screen will appear (Figure 12).

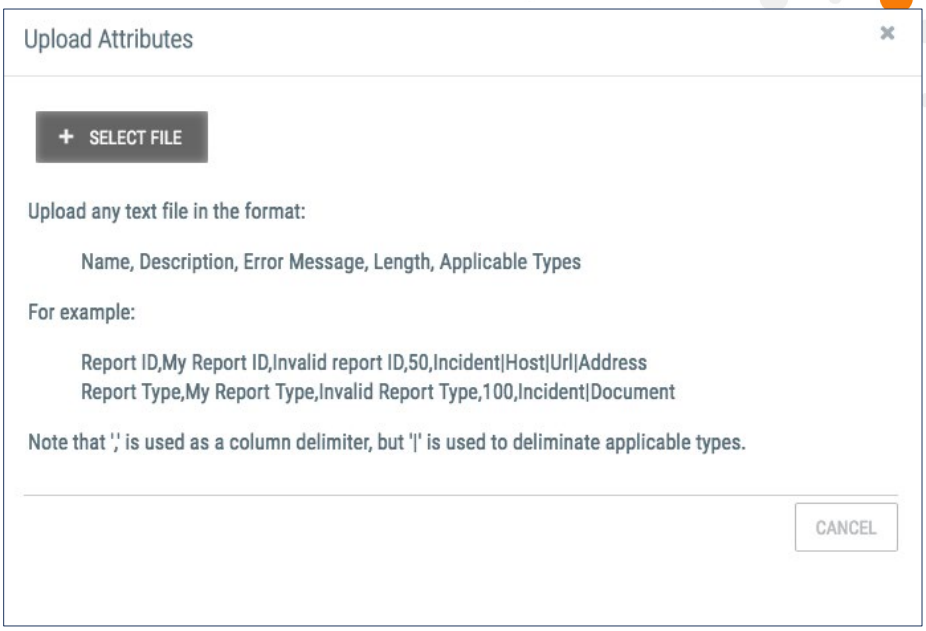

Figure 12

6. Click the **+ SELECT FILE** button, navigate to the desired directory, select a file, and click the **SAVE** button.

Editing Community and Source Attribute Types

Follow these steps to modify an existing Community or Source Attribute Type:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config** icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click on the **Attribute Type** drop-down menu to select the Attribute Type to modify.
6. Click on the **Edit** icon for the Attribute Type.
7. The **Configure Attribute Type** pop-up screen will appear (Figure 11).
8. Configure the fields as appropriate.
9. Click the **SAVE** button to save changes.

Creating Community and Source Attribute Validation Rules

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

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Attribute Validation Rules** tab, and the **Attribute Validation Rules** screen will appear (Figure 13), displaying the existing Community or Source Attribute Validation Rules as well as the ThreatConnect System Attributes Validation Rules, if the **Include System Rules** box is checked.

Figure 13

6. To create a new Community or Source Attribute Validation Rule, click the **+ NEW** button, and the **Create Attribute Validation Rule** pop-up screen will appear (Figure 14).

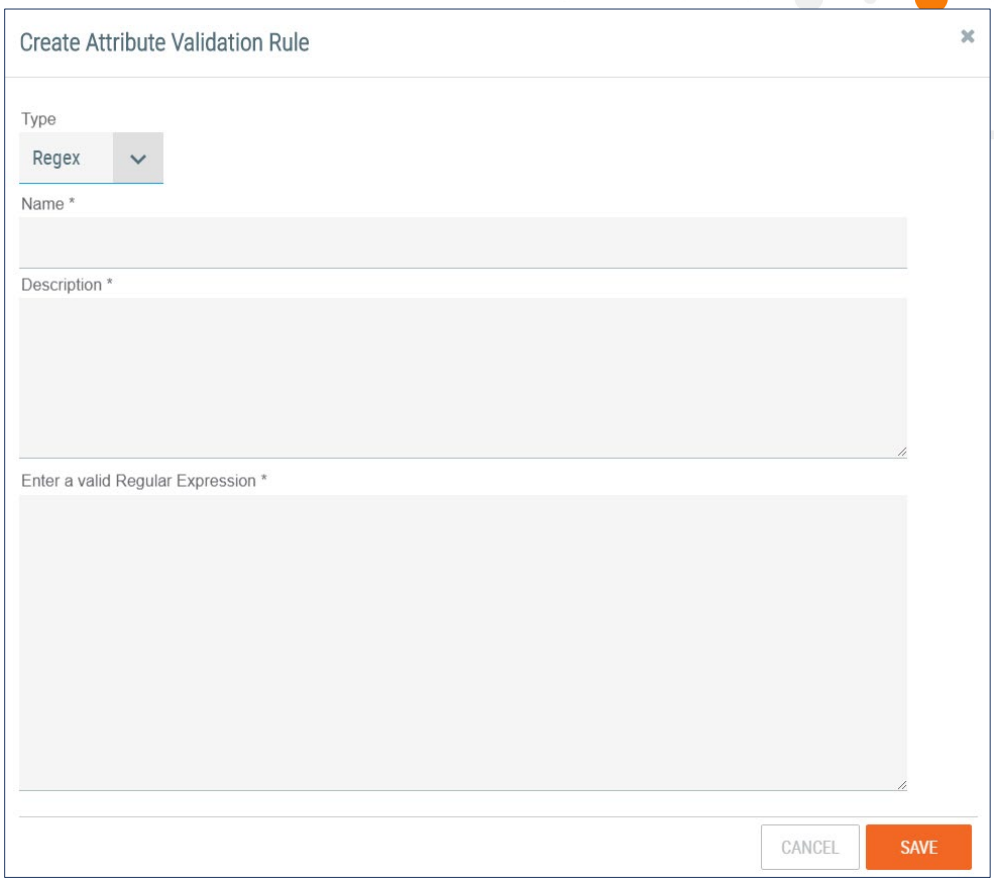

Figure 14

a. **Type**: Click on the drop-down menu to select the schema to use for the Validation Rule. Each option offers the flexibility to determine the valid domain for each Attribute Type.

b. **Regex:** a regular expression that only considers matching inputs to be valid (e.g., an IP address or email address on a certain domain).

   i. **Xsd**: an XML Schema Definition used to validate input (useful for attaching logs from a vendor product)

   ii. **Select One Picklist**: presented as a drop-down 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)

   iii. **Select One Radio**: similar to Select One Picklist, but presented as a series of radio buttons

   iv. **Date**

   v. **Date/Time**

   vi. **Integer:** a whole number, valid in the range specified in the text box on the right (e.g., 0:1440 for "minutes worked")

c. **Name**: Click in the box to enter the name of the Validation Rule as it will appear in the **Create Attribute** prompt described previously.

d. **Description**: Click in the box to enter, as applicable, a general description of the Validation Rule.

e. **Enter a valid Regular Expression:** If applicable, click in the text box to enter the parameters for a Validation Rule as defined previously.

7. Click the **SAVE** button to save and use the new System Attribute Validation Rule. Note that it will have to be attached to an actual Attribute Type in order to validate user input.

Setting Default Attribute Types

To keep Indicator and Group **Details** screens 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 it is created.

Follow these steps to set default Attribute Types:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Default Attributes** tab, and the **Default Attributes** screen will appear (Figure 15), displaying the existing Community or Source Default Attribute Types.

Figure 15

6. To create a new Community or Source Default Attribute Type, click the **+ NEW button**, and the **Create Default Attribute Type** pop-up screen will appear (Figure 16).

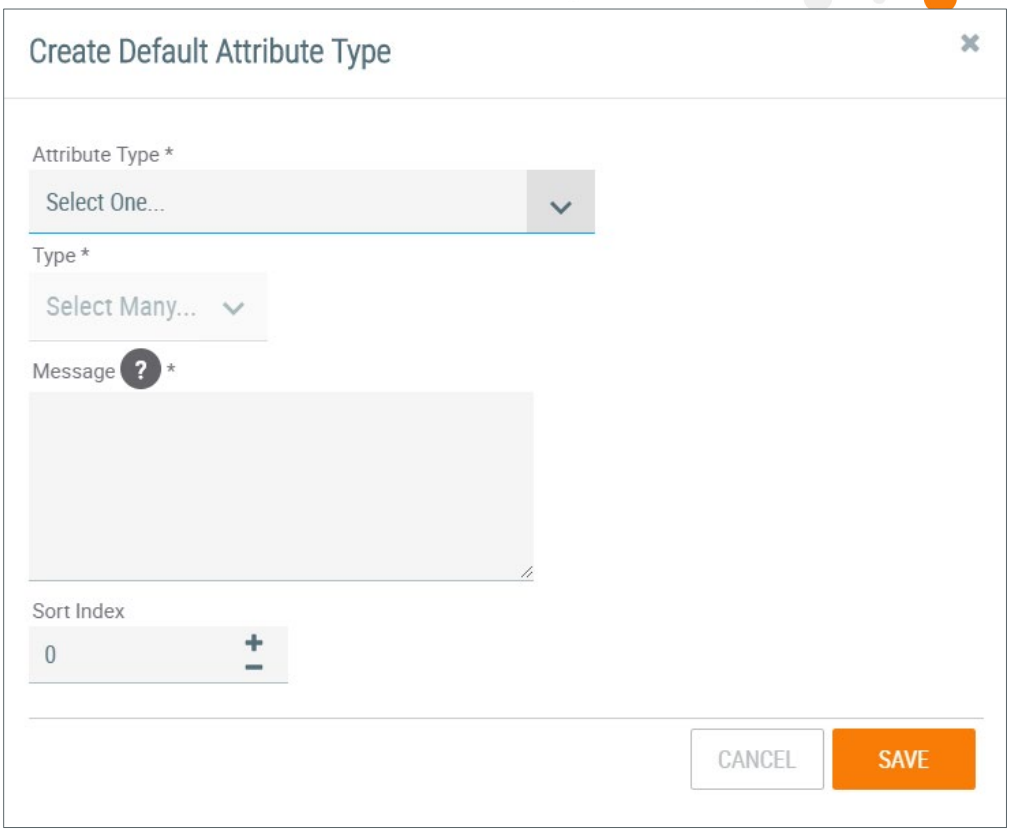

Figure 16

a. **Attribute Type**: Click on the drop-down menu to select one of the Attribute Types defined on the Community Attribute Type screen.

   NOTE: These options also include System Attribute Types.

b. **Type**: Click on the drop-down menu to select any applicable Indicators or Groups to which to apply the default Attribute Type specified previously. Note that only entities that were approved when the Attribute Type was created can be specified.

c. **Message**: Click in the box to 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.

d. **Sort Index**: Click in the box (or use the plus and minus signs) to set the index used to arrange default Attribute Types. Indices are set in ascending order, meaning that the Attribute Type ranked **0** will be at the top of the Attribute Type list, and the Attribute Type ranked with the highest number will be at the bottom.

7. Click the **SAVE** button to save the Community or Source Default Attribute Type settings.

Indicator Exclusion Lists: Community or Source Level

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 **Community Config** or **Source Config** screen.

Creating Community- and Source-Level Indicator Exclusion Lists

Follow these steps to create a Community- or Source-level Indicator Exclusion list:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Indicator Exclusions** tab, and the **Indicator Exclusions** screen will appear (Figure 17).

Figure 17

6. Click on the **Edit**  icon of an Indicator from the **Type** column (File-SHA1 in this example), and the **Exclusion Details** pop-up screen will appear (Figure 18).

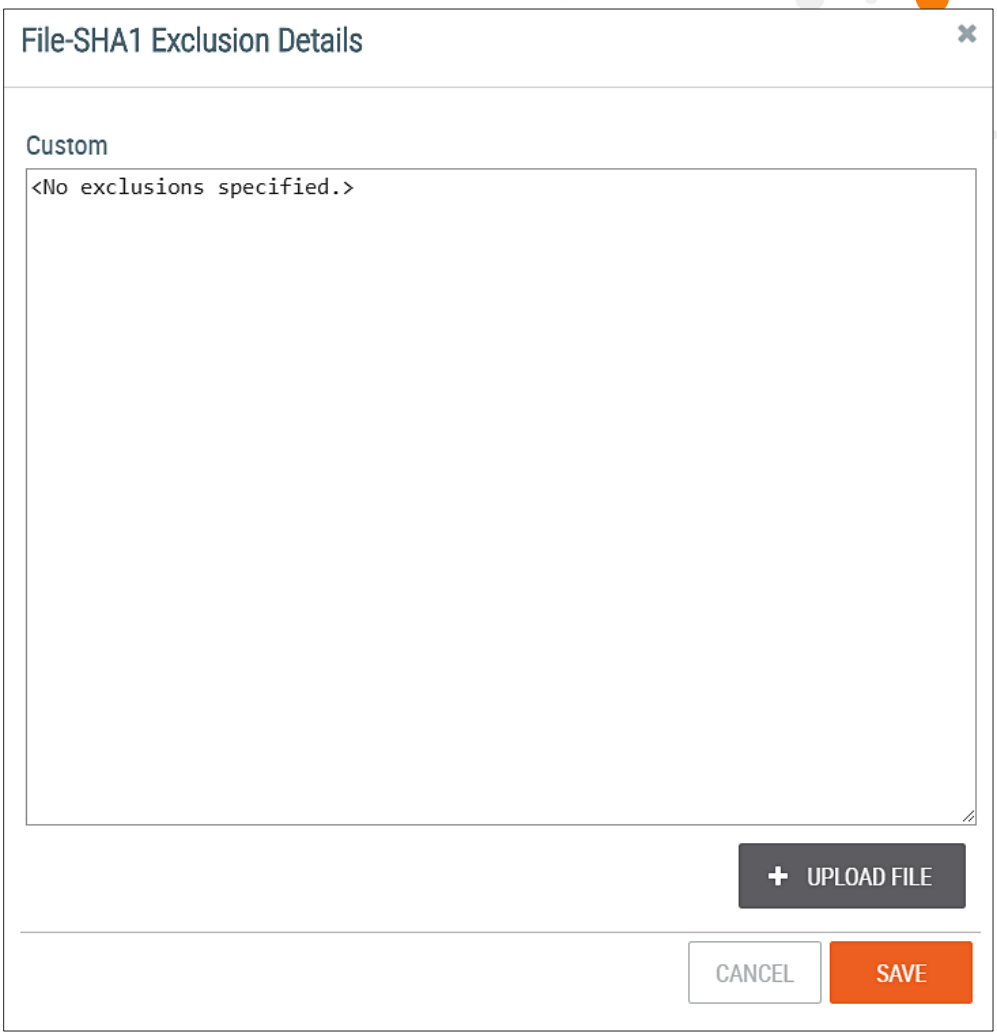

Figure 18

7. When creating a new Exclusion List, enter the information directly into the **Custom** text box, and click the **SAVE** button (Figure 19).

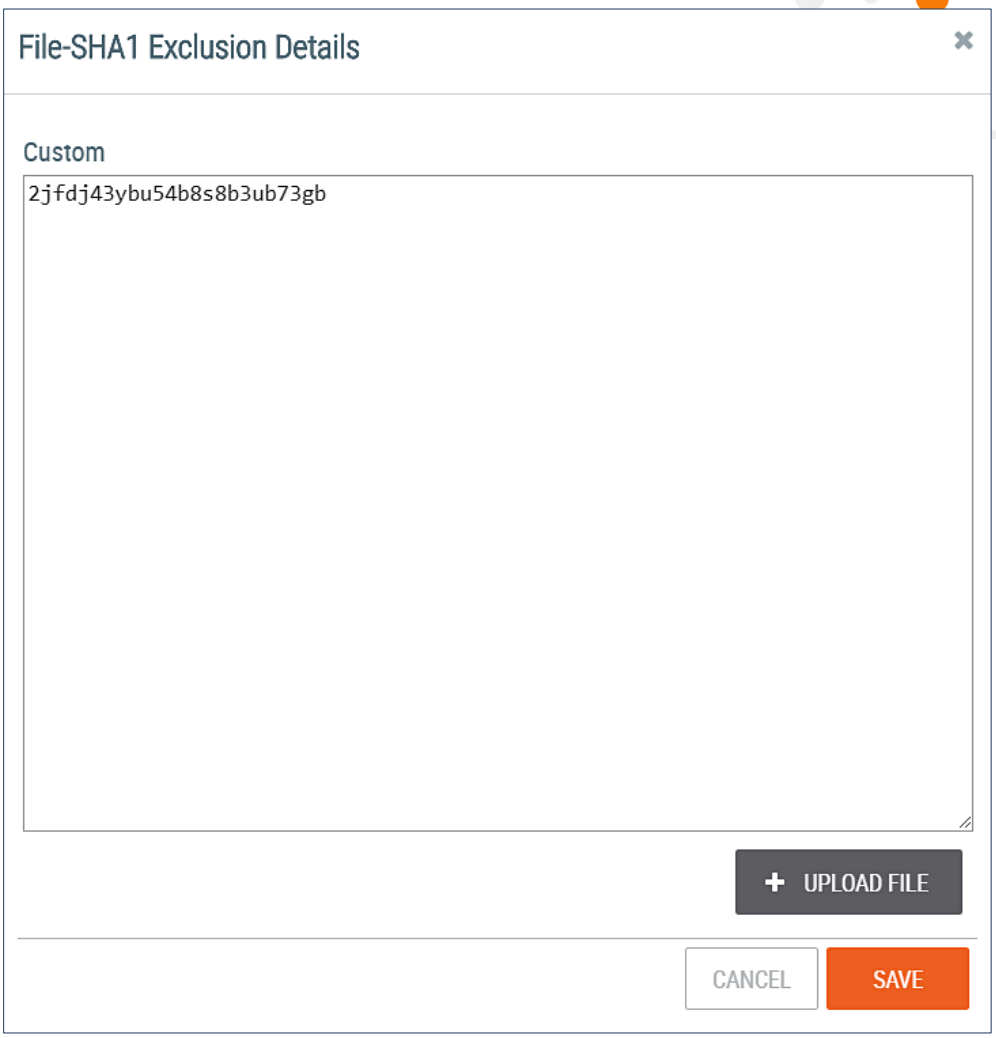

Figure 19

8. Otherwise, click the **+ UPLOAD FILE** button to navigate to the appropriate directory. 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**.
9. Select the desired file, and the Exclusion list will be uploaded (Figure 20).

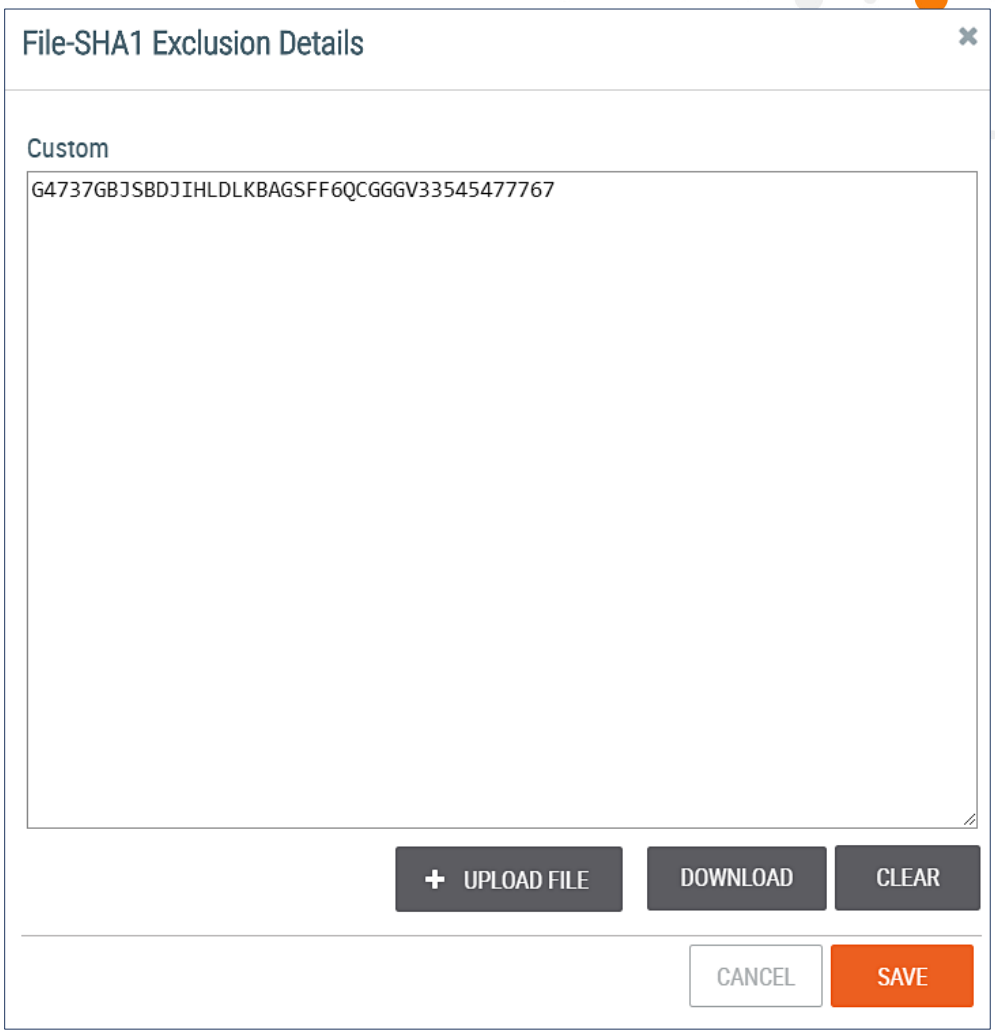

Figure 20

10. Click the **SAVE** button.
11. To modify an existing Exclusion list, edit it directly from the **Custom** text box. Otherwise, click the **DOWNLOAD** button to download and edit a file, and then click the **+ UPLOAD FILE** button to upload the edited file.
12. Click the **SAVE** button.

    NOTE: When trying to create an Indicator that has been placed on an Exclusion list, a message will appear in the Create pop-up screen warning that the Indicator is contained on a Community- or Source-wide Exclusion list.
13. To remove an existing **Custom** Exclusion list, click the **CLEAR** button, and the **Remove Exclusions** pop-up screen will appear (Figure 21).

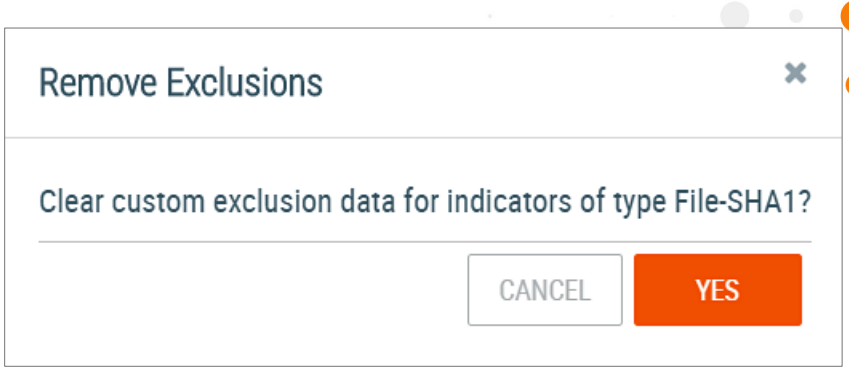

Figure 21

14. Click the **YES** button followed by the **SAVE** button.

Community and Source Security Labels

Purpose of Community and Source 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 developed by the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). Administrators can define their own Security Labels based on their Community's or Source's needs and policies.

Creating Community and Source Security Labels

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

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Security Labels** tab, and the **Security Labels** screen will appear (Figure 22), displaying existing Community or Source Security Labels.

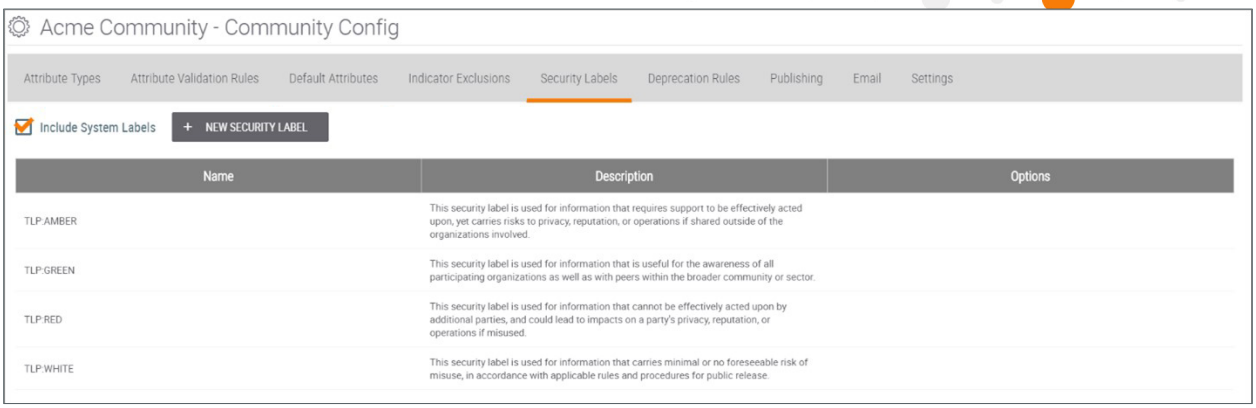

Figure 22

6. To create a new Community or Source Security Label, click the **+ NEW SECURITY LABEL** button, and the **Create Security Label** pop-up screen will appear (Figure 23).

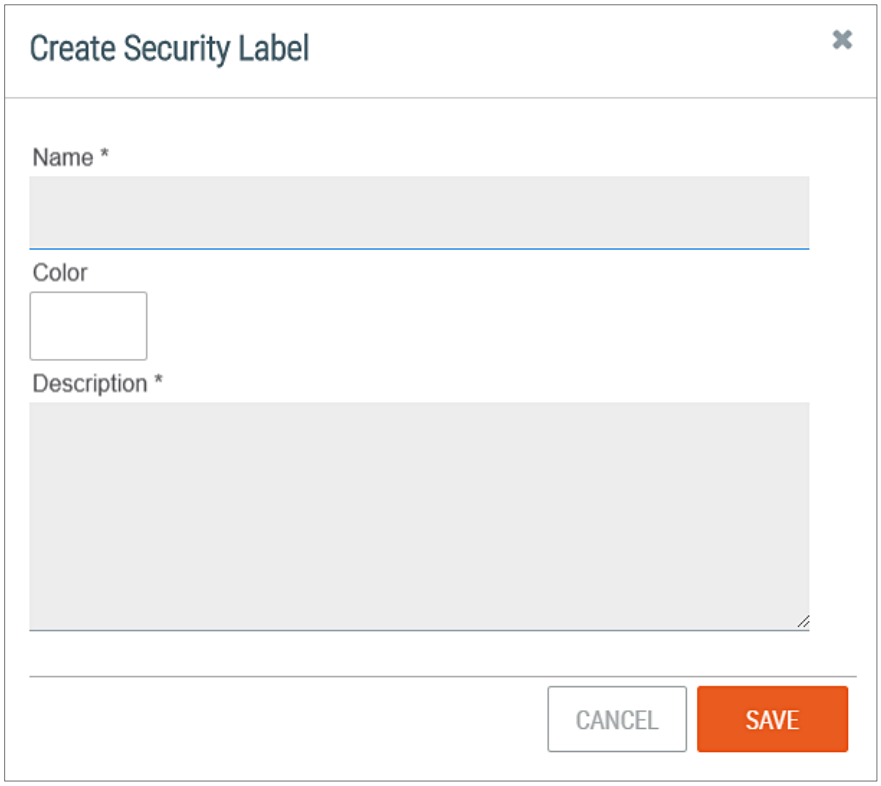

Figure 23

7. Click in the boxes to enter a **Name**, **Color**, and a **Description** for the Security Label. These fields are provided solely for user and Administrator readability, as no policy enforcement is derived from this screen.
8. Click the **SAVE** button to save the Community or Source Security Label.

Using Community and Source 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.

Community or Source Deprecation Rules

Deprecation Rules define how ThreatConnect handles Indicators made irrelevant because of inactivity—queuing them up for deletion when they have met specified deprecation criteria. The next sub-section demonstrates a Deprecation Rule for IP addresses that have not been modified or updated in 180 days. After 180 days of inactivity, ThreatConnect decrements the confidence of the IP Address by 100%, effectively making the Confidence Rating value be **0**. ThreatConnect then deletes those Indicators from the system.

Creating Deprecation Rules

Follow these steps to create a Deprecation Rule:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Deprecation Rules** tab, and the **Deprecation Rules** screen will appear (Figure 24).

Figure 24

6. To create a new Deprecation Rule, click **+ NEW** button, and the **Create/Edit Deprecation Rule** pop-up screen will appear (Figure 25), with fields to enter the **Indicator Type**, **Confidence Amount,** what **Action At Minimum** to take (when an Indicator reaches or goes below **0** Confidence), deprecation time **Interval**, and checkboxes to indicate whether to express the Confidence as a **Percentage** and whether the Deprecation Rule should be **Recurring**.

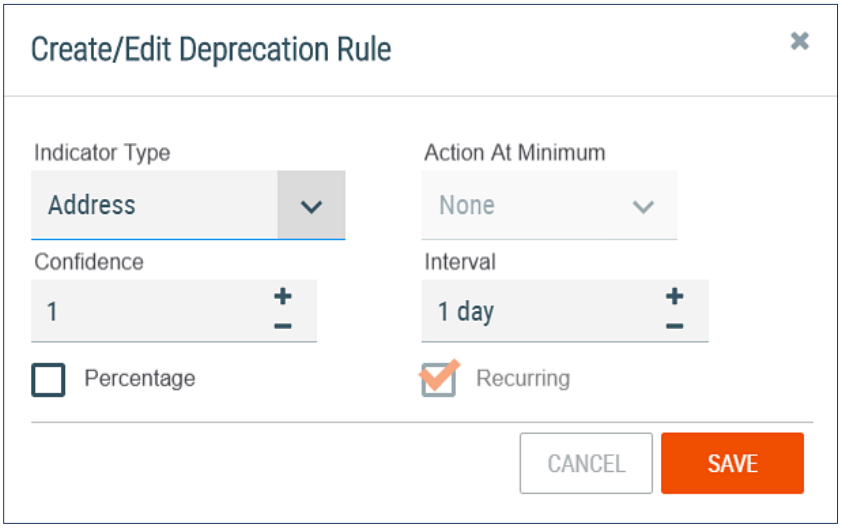

Figure 25

Community or Source 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 TC Cross-Intel Sharing app. (See *The Cross-Intel Sharing App: Sharing Data Across ThreatConnect Instances* for information about how to share published data with other ThreatConnect instances.) All types of Group data objects (Adversary, Campaign, Document, E-mail, Incident, Signature, and Threat) can be published. In order to publish a Group, it must first exist in, or be contributed to, a Community or Source. (See the *Contributing to a Community or Source* article for more details.) The Publish feature is accessible by navigating to the **Browse** screen and then selecting a Group object from the table. In the following section, users will only view and download already-published JSON files.

Viewing and Downloading Published Files

Follow these steps to view and download published JSON files:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Publishing** tab, and the **Publishing** screen will appear (Figure 26).

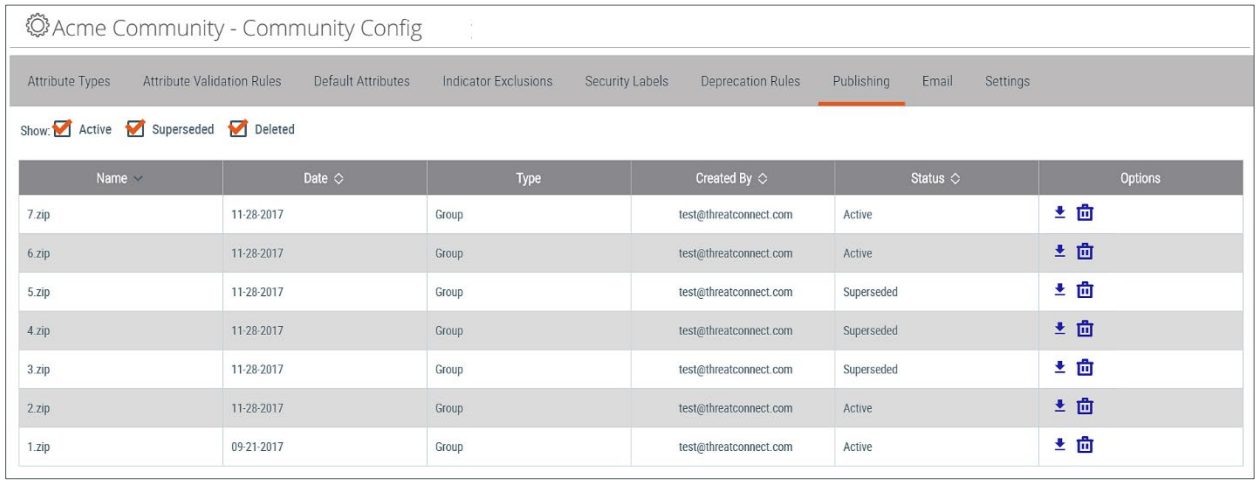

Figure 26

6. Determine the type of files to display by clicking the **Active**, **Superseded**, or **Deleted** checkboxes.
7. Select one of the files in the table and click the **Download**  icon.
8. The file will be saved to the computer's **Downloads** folder from where it can be accessed.

Setting Up Community or Source Email Ingestion

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, configure ThreatConnect as follows:

- The mailInboundEnabled setting is true.
- 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

Creating 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 do the following:

Create a "document" object out of the email's body

Create any Indicators that matched the pre-defined Feed Mailbox regular expressions

Link the Indicators to the document

Follow these steps to create a Feed Mailbox:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Email** tab, and the **Email** screen will appear (Figure 27).

Figure 27

6. Click the **Create Feed Mailbox** button, and the **Feed Mailbox Administration** pop-up screen will appear, with the **Mailbox** tab highlighted (Figure 28).

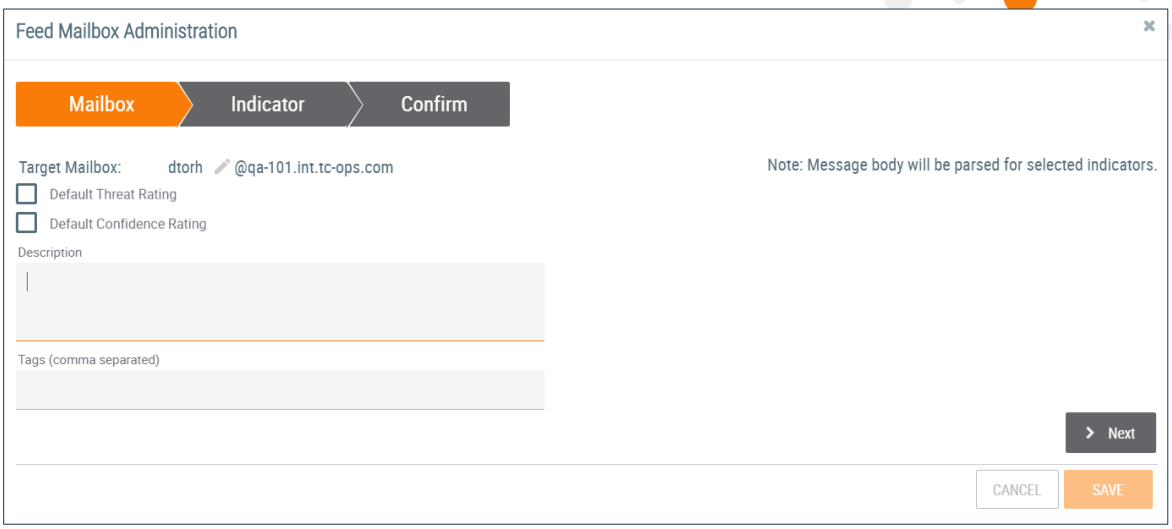

Figure 28

NOTE: A System Administrator can modify the Target Mailbox name at this step.

7. Click the checkboxes to assign a **Default Threat Rating** and **Default Confidence Rating** to found Indicators, enter a **Description**, and click in the **Tags** box to enter Tags.
8. Click the **Next** button to proceed to the Indicator tab (Figure 29).

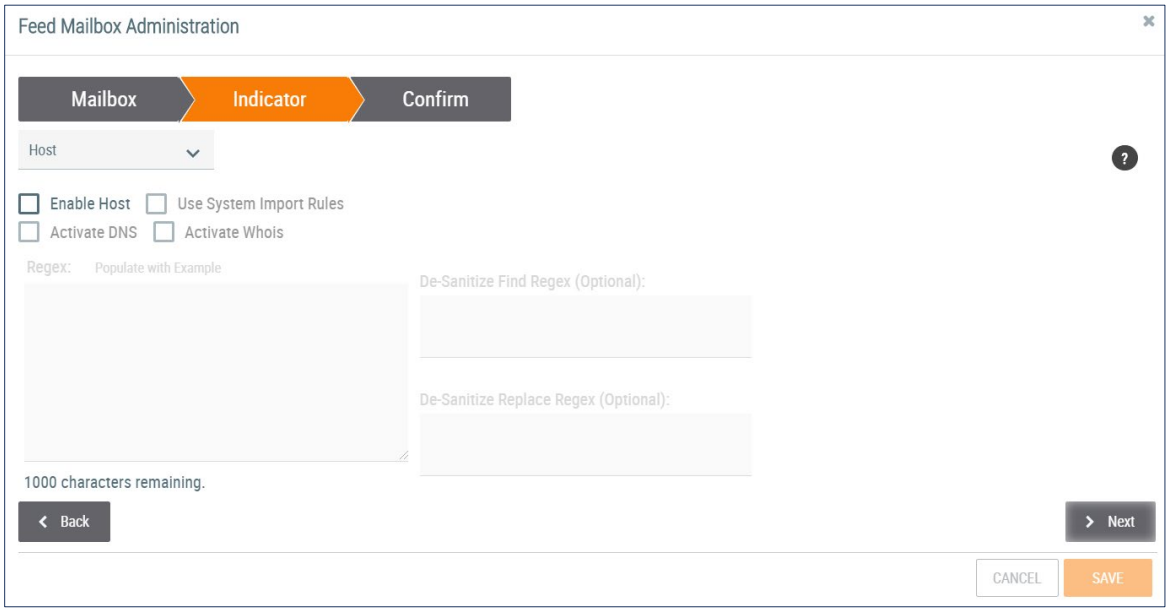

Figure 29

9. Use the drop-down menu to select an Indicator Type (**Host**, **Address**, **E-mail Address**, **File**, **URL**, and any custom Indicators that have been added, including ThreatConnect's five built-in custom Indicators). Enabling an Indicator allows regex entries. The **Question Mark**  icon on the top right of the screen offers 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.

10. Select and modify the other parameters as desired, and click the **Next** button, and the **Confirm** tab screen will appear (Figure 30), offering a summary of the entries.

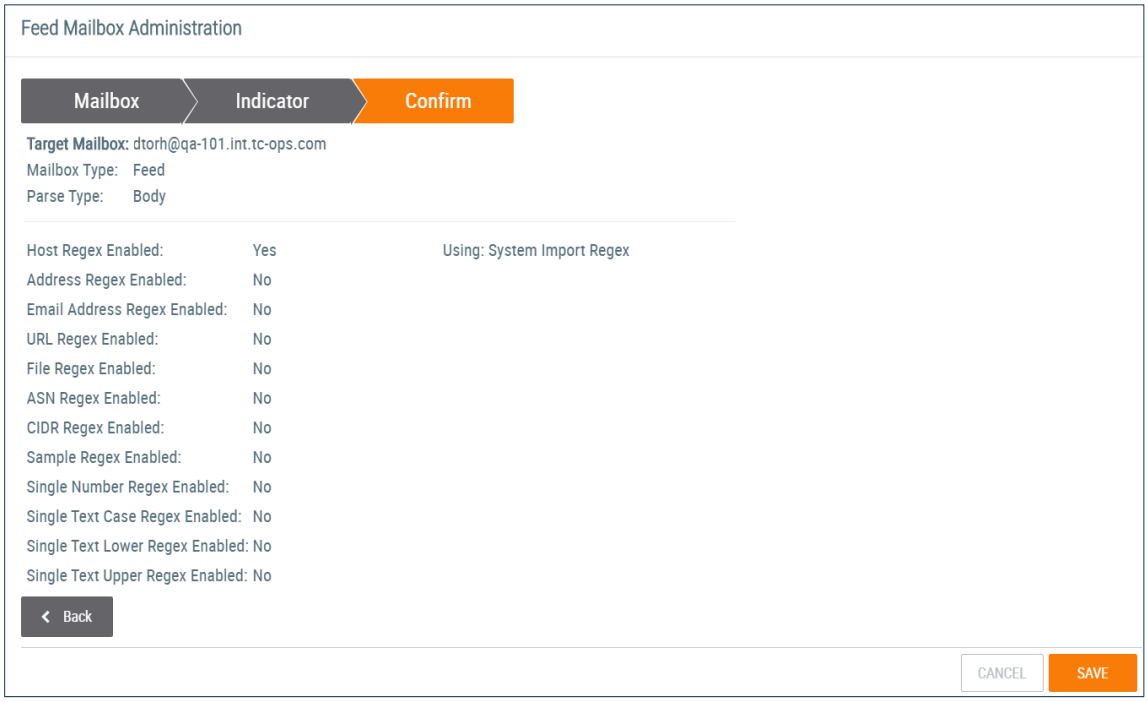

Figure 30

11. Click the **SAVE** button.

Creating 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 do the following:

- Create an Email Object containing the email's header and body.
- Create a Task Object signaling that the email is ready for additional processing.
- Link previously existing Indicators to the Email Object, if they are found in the header or body.
- Link previously existing Victim email addresses to the Email Object, if they are found in the header.

Follow these steps to create a Phishing Mailbox:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Email** tab, and the **Email** screen will appear (Figure 27). Click the **Create Phishing Mailbox** button, and the **Phishing Mailbox Administration** pop-up screen will appear(Figure 31).

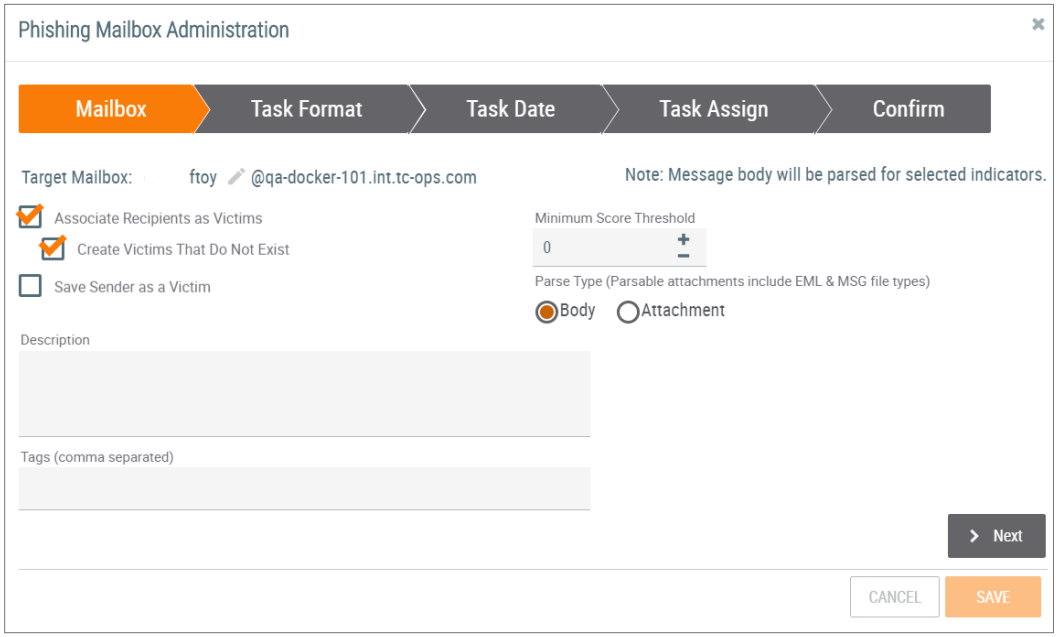

Figure 31

NOTE: A System Administrator can modify the Target Mailbox name at this step.

6. Click one of the checkboxes to **Associate Recipients as Victims** or **Create Victims That Do Not Exist** to create an association between the email and Victim asset.

   NOTE: The association is created only if the Victim asset already exists in ThreatConnect.

7. Click the **Save Sender as Victim** checkbox to create an association between the sender and the Victim Asset.
8. Click in the **Minimum Score Threshold** box (or use the plus and minus signs) to indicate the minimum score that an email must meet in order to be processed.
9. Click one of the **Parse Type** radio buttons to select if the Phishing Mailbox will receive emails directly or in the form of an **.eml** or an **.msg** attachment.

10. Enter a **Description**, and click inside the **Tags** text box to specify Tags for this mailbox.
11. Click the **Next** button to proceed through the steps required for ThreatConnect to assign a task to an analyst when new emails arrive.
12. Click the **SAVE** button.

Settings

The **Settings** tab allows users to add a DomainTools API key in order to enable DomainTools for all Reverse Whois Track queries.

Setting Up DomainTools

Follow these steps to set up DomainTools:

1. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Community or Source, and its **Community** or **Source** card will appear on the top left of the screen (Figure 4).
4. Click on the **Community (or Source) Config**  icon, and the **Community Config** (Figure 10) or **Source Config** screen will appear (Figure 38).
5. Click the **Settings** tab, and the **Settings** screen will appear (Figure 32).

Figure 32

6. Click the **ENABLE** button, and the **Setup DomainTools** pop-up screen will appear (Figure 33)

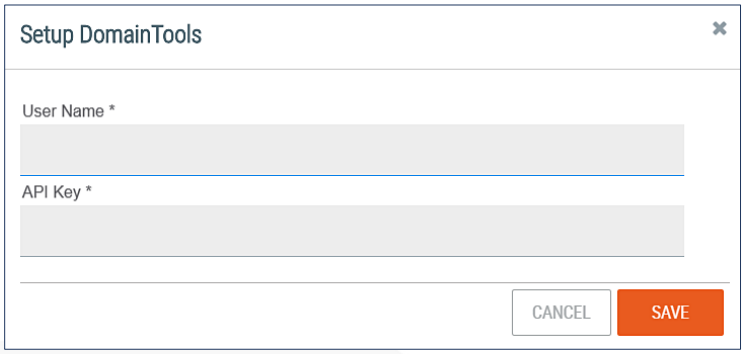

Figure 33

7. Enter a **User Name** and a valid **API Key** and click the **SAVE** button.

Source Access and Roles

Table 2 displays Source Roles and their descriptions.

Source Role	Description
Director	Directors have the same privileges as Editors, but they can also add new users to the Source and assign roles to existing users.
Editor	Editors can create, delete, or modify any information in the Source.
Contributor	Contributors can create new data, and they have limited Editor capabilities. They can add Attribute Types, but they cannot delete or edit Indicators or existing Attribute Types posted by others. Most users within Sources will have this role.
Commenter	Commenters can create new Attribute Types and Comments on Indicators and Groups in a Source, but are not allowed to add Associations, new Indicators, or new Groups.
User	Users have read-only access. They do not have write or update access.
Subscriber	Subscribers have read-only access to published data.
Banned	Banned account holders are not permitted access to a Source, including its data or posts.

Table 2

NOTE: Editors in a Source will not be able to update the rating and confidence unless they are a member of the Organization that owns the Source, but they can delete and update attributes types, etc.

Configuring Source Roles

To configure Source roles, follow the steps in the *Configuring Community Roles* section of this user guide.

Inviting Users to a Source

Follow these steps to invite Users to a Source:

1. Log in with an Organization Administrator account, or higher, valid for the desired Source.
2. On the top navigation bar, click **Posts** (Figure 1**Error! Reference source not found.**) and the **Posts** screen will appear (Figure 3).
3. Click on the desired Source, and its **Source** card will appear on the top left of the screen (Figure 34).

Figure 34

4. Click on the **Source Info**  icon, and the **Source Info** screen will appear (Figure 35).

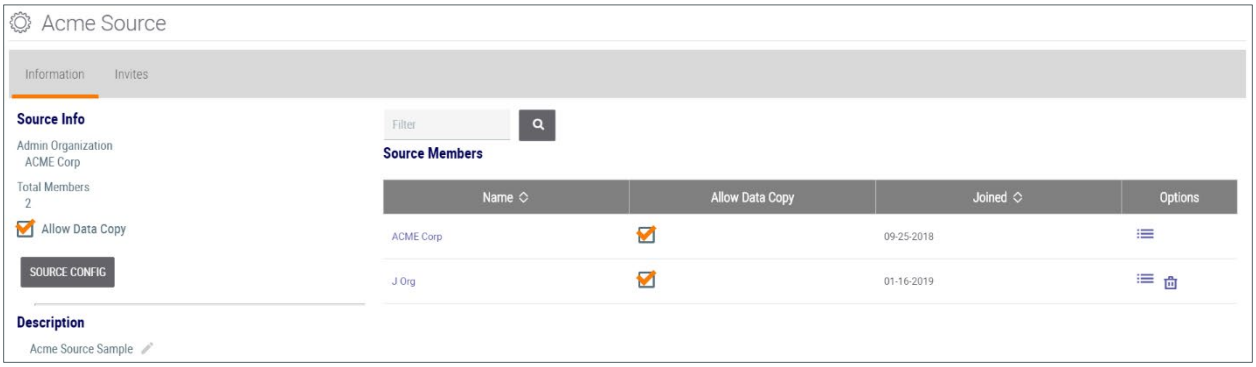

Figure 35

5. Click the **Invites** tab, and the **Invites** screen will appear (Figure 36).

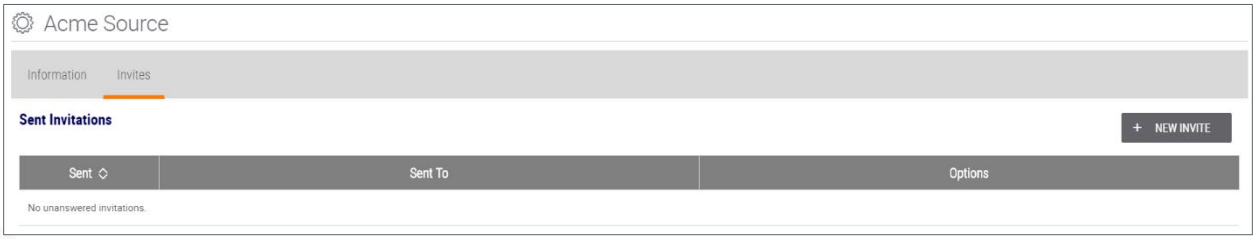

Figure 36

6. Click the **+ NEW INVITE** button, and the **Send Source Invite** pop-up screen will appear

(Figure 37).

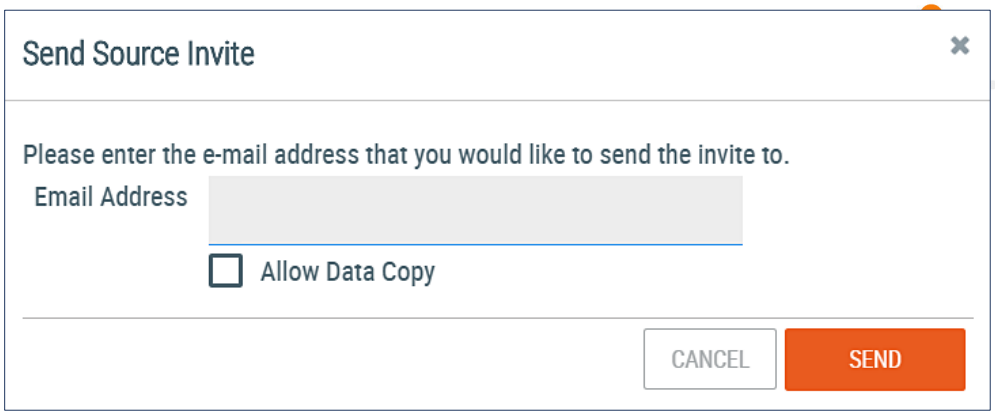

Figure 37

7. Click in the **Email Address** box to enter the user's email address, and, if desired, give the user rights to copy data from the Source to a private Organization by clicking on the **Allow Data Copy** checkbox.
8. Click the **SEND** button to send the Source Invite.

Creating a Source Feed

Follow these steps to create a Source Feed:

1. Log in with an Organization Administrator account, or higher, valid for the desired Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Source, and its **Source** card will appear on the top left of the screen (Figure 34).
4. Click on the **Source Config**  icon, and the **Source Config** screen will appear (Figure 38).

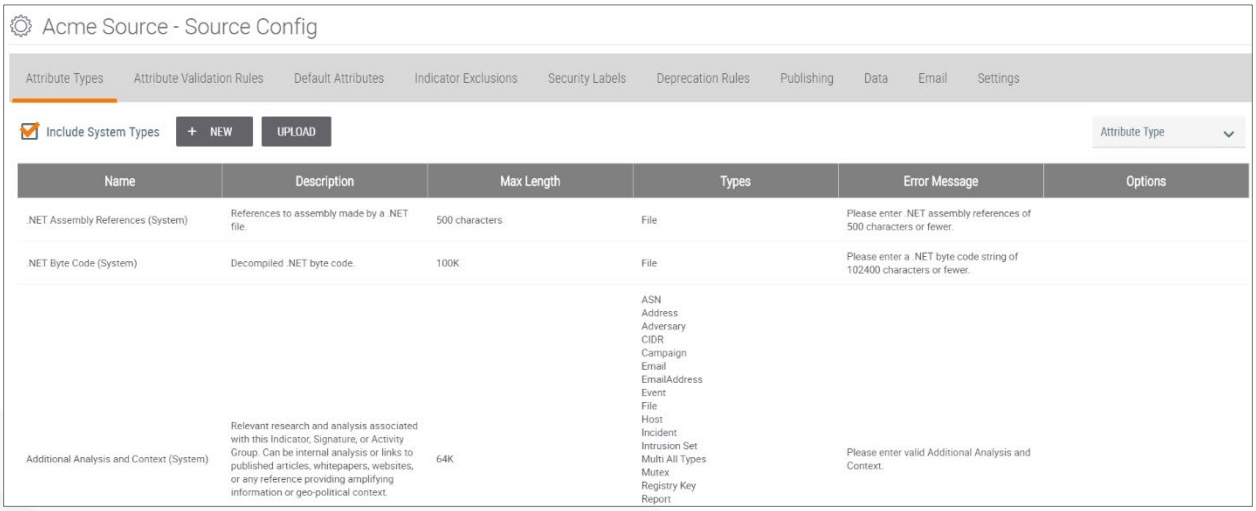

Figure 38

5. Click the **Data** tab, and the **Data** screen will appear (Figure 39).

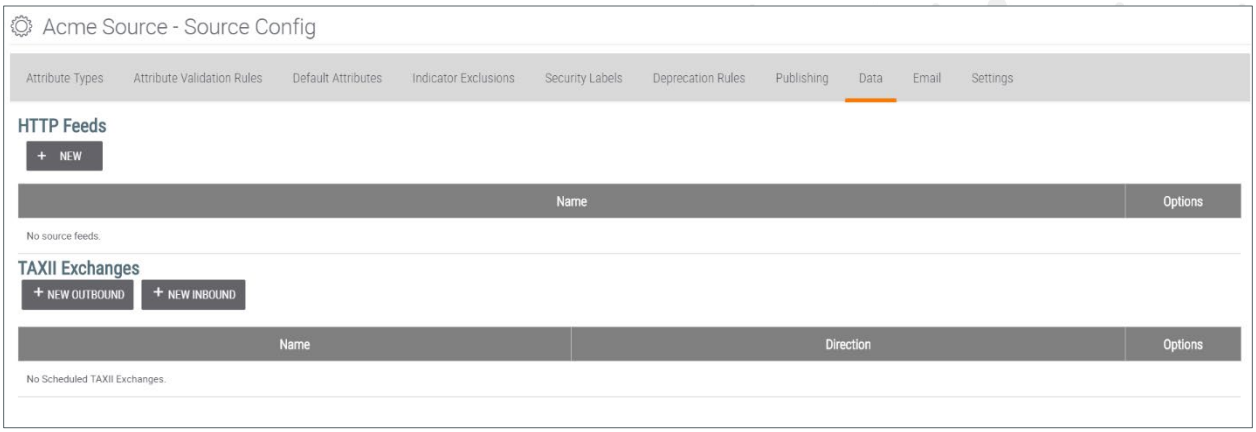

Figure 39

6. Click the **+ NEW** button, and the **Create Source Feed** pop-up screen will appear (Figure 40).

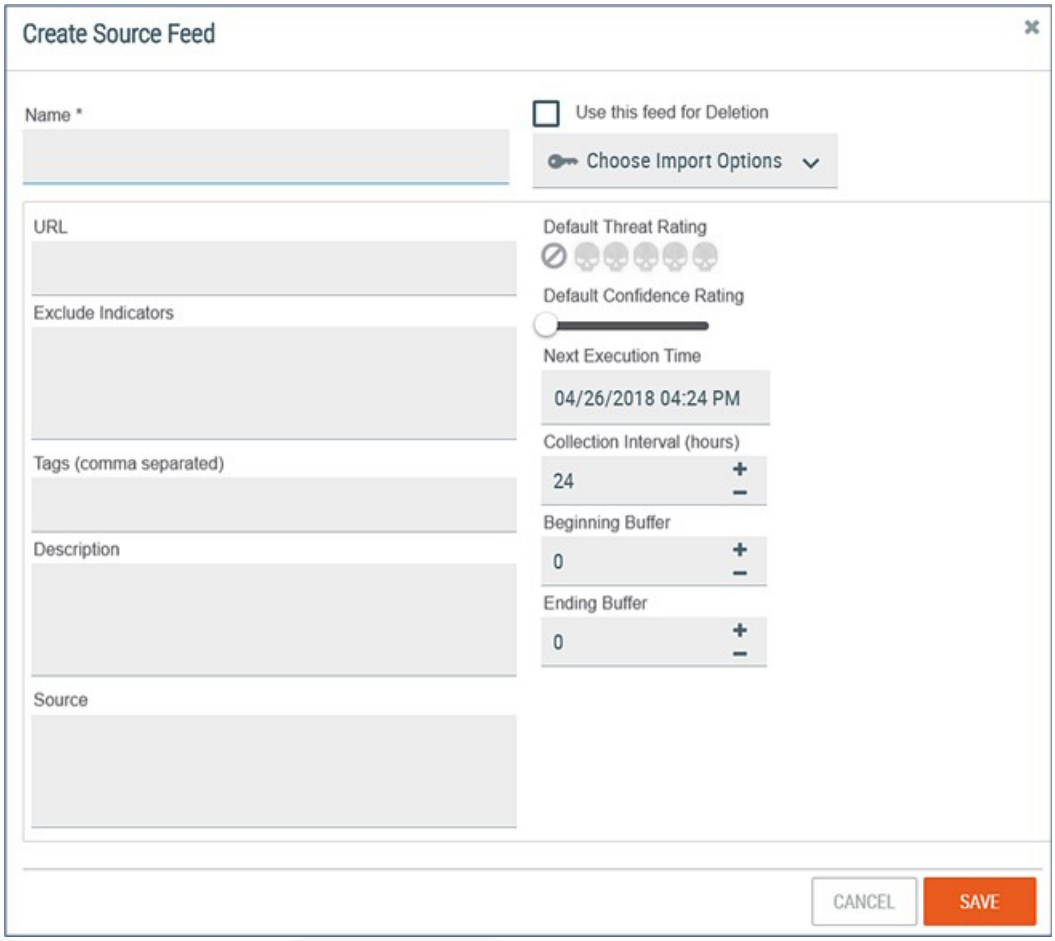

Figure 40

a. **Name**: Click in the box to enter the Source Feed name.

b. **URL**: Click in the box to specify the site path for ThreatConnect to ingest.

c. **Exclude Indicators**: Click in the box to exclude unwanted Indicators.

d. **Tags (comma separated)**: Click in the box to enter Tags for ThreatConnect to apply on Indicators that the Source Feed creates.

e. **Description**: Click in the box to enter a general description to be added to the Description Attribute Type on Indicators imported by the Source Feed.

f. **Source**: Click in the box to enter a Source description to be added to the Source Attribute Type on Indicators imported by the Source Feed.

g. **Use this feed for Deletion**: Click the checkbox to specify whether the Source Feed is creating based on inputs or deleting based on inputs.

h. **Choose Import Options**: Click on the drop-down menu and click the checkboxes corresponding to the Indicators for which the Source Feed should search.

i. **Default Threat Rating**: Click one of the skulls to set the Default Threat Rating.

j. **Default Confidence Rating**: Slide the bar to set the Default Confidence Rating

k. **Next Execution Time**: Click in the box to set the next date and time that the Source Feed will run.

l. **Collection Interval (hours)**: Click in the box (or use the plus and minus signs) to set the interval at which the Source Feed will run.

m. **Beginning Buffer** and **Ending Buffer**: Click in the boxes (or use the plus and minus signs) to tell the Source Feed how many lines to skip at the beginning and at the end of the page.

7. Click the **SAVE** button.

Creating an Inbound TAXII Exchange Feed

An Inbound Trusted Automated eXchange of Indicator Information (TAXII™) Exchange Feed ingests Structured Threat Information eXpression (STIX™) formatted data from a TAXII server.

Follow these steps to create an Inbound TAXII Exchange Feed:

1. Log in with an Organization Administrator account, or higher, valid for the desired Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Source, and its **Source** card will appear on the top left of the screen (Figure 34).
4. Click on the **Source Config**  icon, and the **Source Config** screen will appear (Figure 38).
5. Click the **Data** tab, and the **Data** screen will appear (Figure 39).

6. Click the **+ NEW INBOUND** button, and the **Configure Inbound TAXII Exchange** pop-up screen will appear with the **Taxii** tab highlighted (Figure 41).

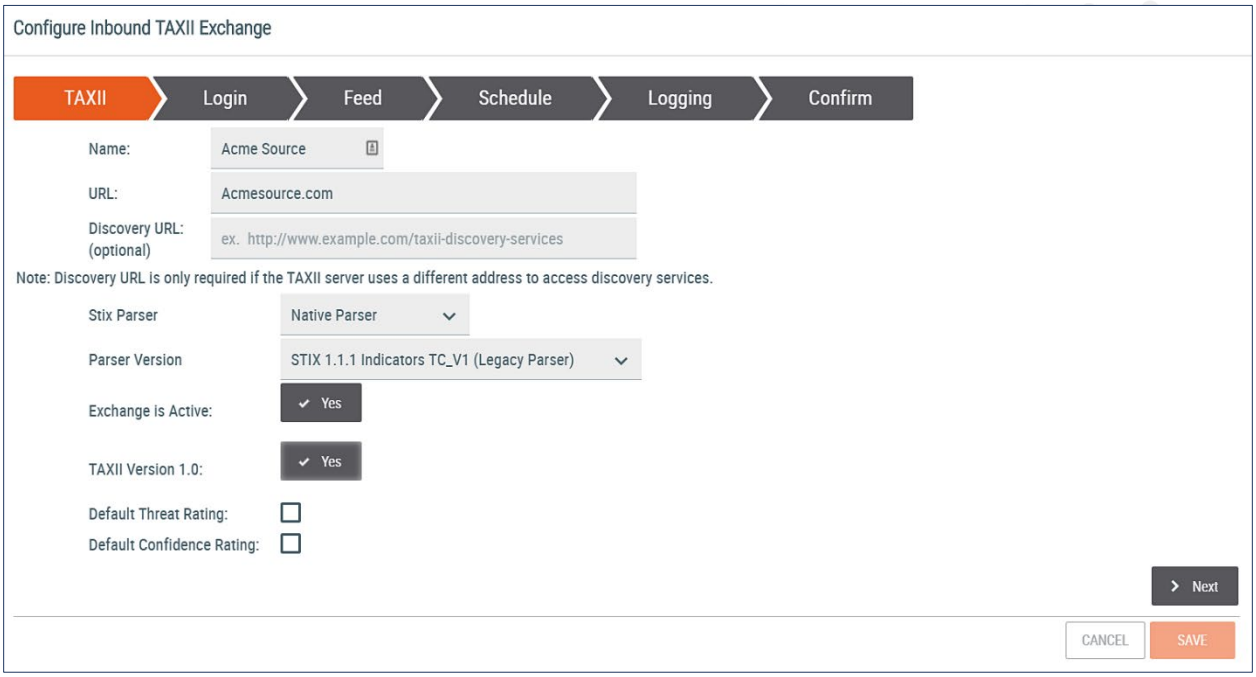

Figure 41

a. **Name**: Click inside the box to enter a name.

b. **URL**: Click inside the box to enter a URL.

c. **Discovery URL**: Click inside the box, if applicable, to enter a Discovery URL.

d. **Stix Parser**: Choose between **Native Parser**, within the app, or the external **STIX Parser**.

e. **Parser Version**: Click the arrow to choose between the legacy STIX version and the new STIX version.

f. **Exchange is Active**: Click the rectangle to toggle between **Yes** and **No**.

g. **Taxii Version 1.0**: Click the rectangle to toggle between **Yes** and **No**.

h. **Default Threat Rating**: Click the checkbox to enter a Threat Rating.

i. **Default Confidence Rating: Click the checkbox to enter a Confidence Rating.**

7. Click the **Next** button, and the **Login** screen will appear (Figure 42).

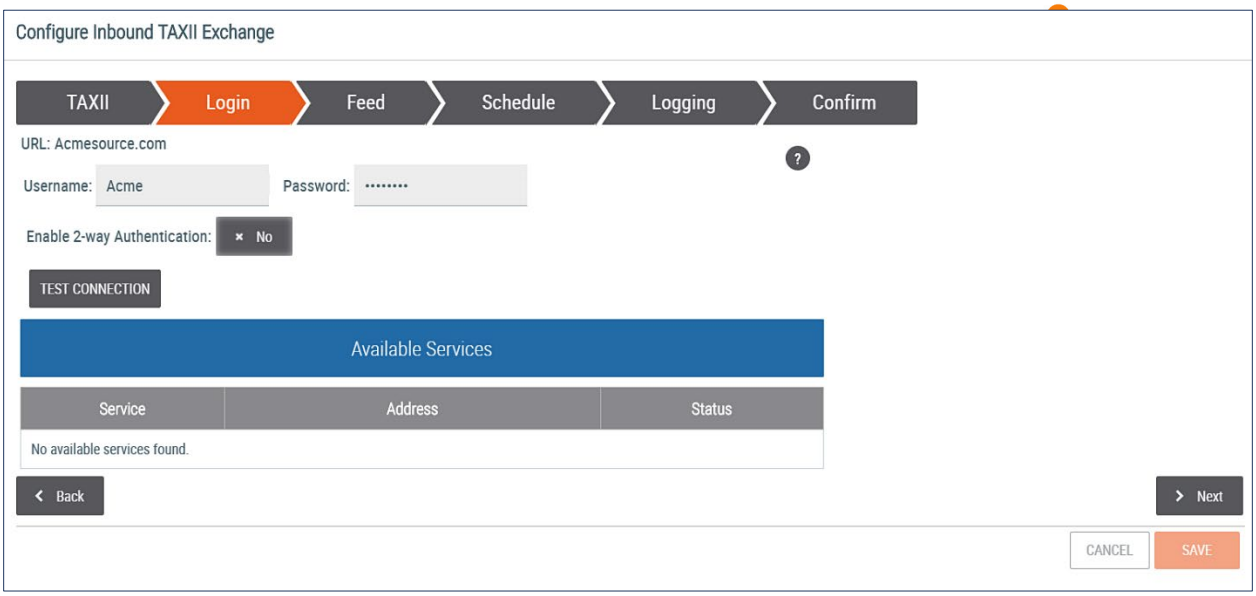

Figure 42

a. **URL**: Verify that the URL displayed is the one entered in the previous step.

b. **Username** and **Password**: Click in the boxes to enter each field.

c. **Enable 2-way Authentication**: Click the rectangle and toggle to **Yes** to provide a **Certificate**. Provide the **Private Key** and **Certificate** found in the **.pem** certificate file.

d. **TEST CONNECTION**: Click on this button to test the connection.

e. Select the appropriate **Service**.

8. Click the **Next** button, and the **Feed** screen will appear (Figure 43).

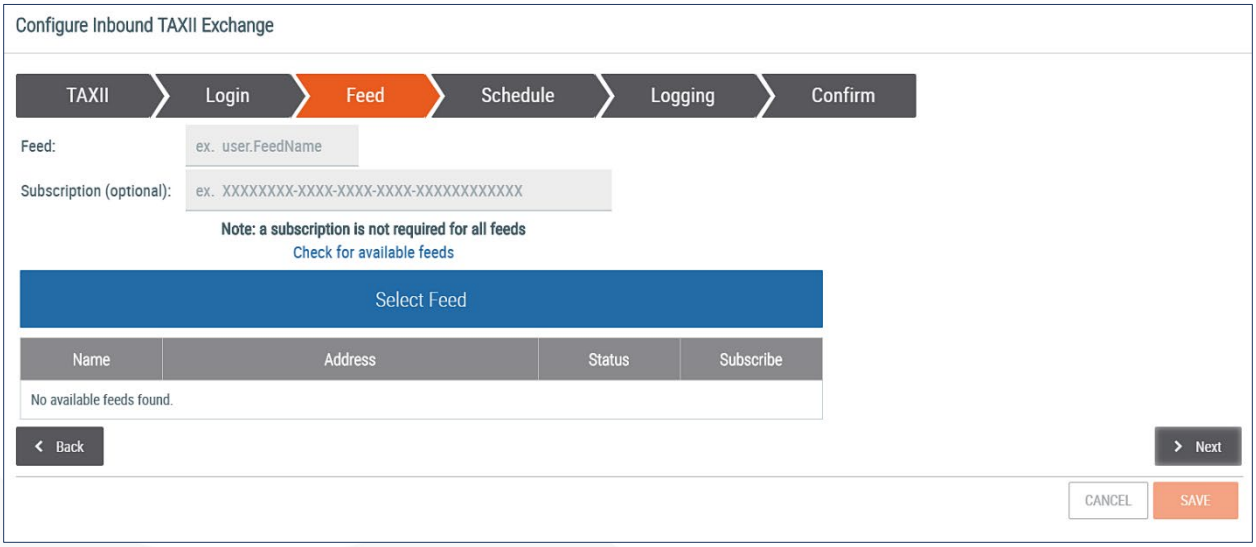

Figure 43

a. **Feed**: Click inside the box to enter the feed name.

b. **Subscription**: If applicable, click inside the box to enter a subscription ID.

c. **Check for available feeds**: Click on the text to view and select a feed.

9. Click the **Next** button, and the **Schedule** screen will appear (Figure 44).

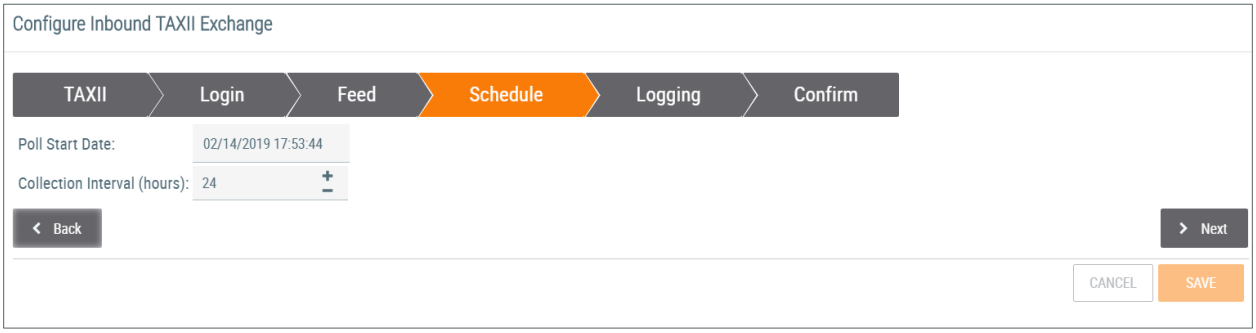

Figure 44

a. **Next Execution Time**: Click in the box, and a calendar will pop up to select the date and time.

b. **Collection Interval**: Click inside the box to manually change the time, or use the plus and minus signs to set the time (in hours).

10. Click the **Next** button, and the **Logging** screen will appear (Figure 45).

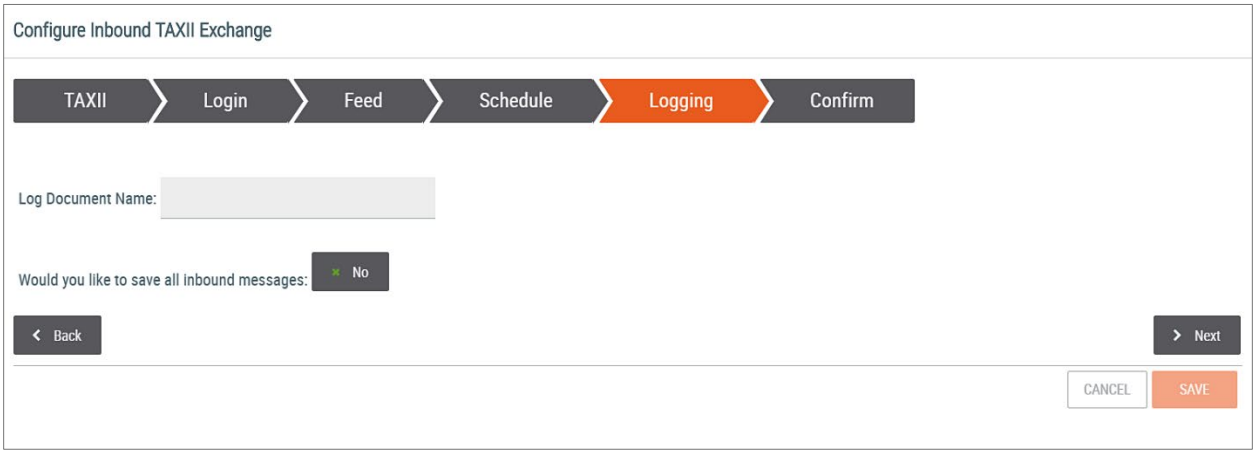

Figure 45

a. **Log Document Name**: Click in the box to enter a name.

b. Would you like to save all inbound messages: Click the rectangle to toggle to Yes.

NOTE: Document storage for the source needs to be allocated.

11. Click the **Next** button, and the **Confirm** screen will appear (Figure 46). Confirm that the entered information is correct.

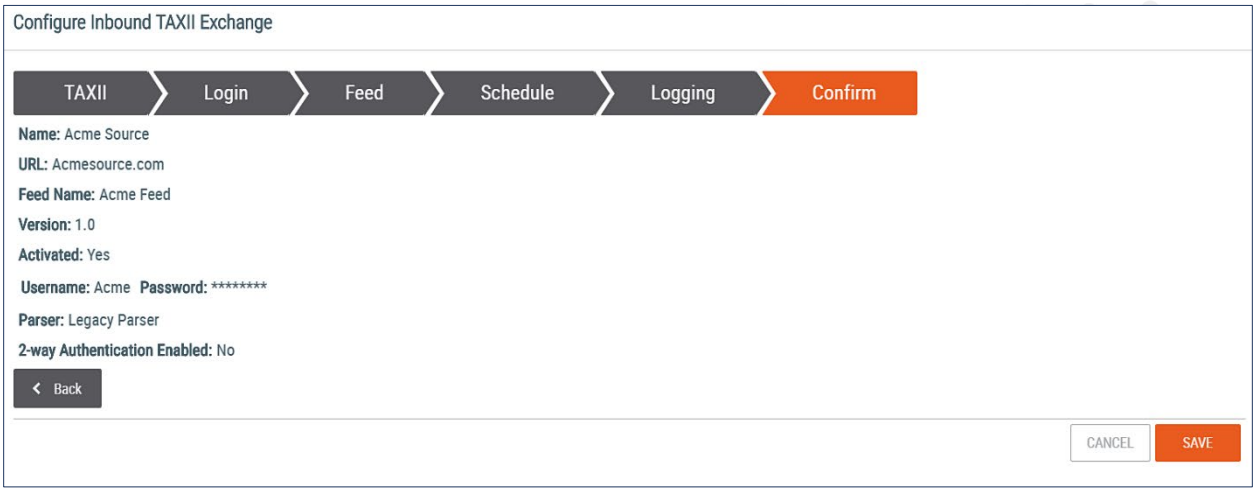

Figure 46

12. Click the **SAVE** button.

Creating an Outbound TAXII Exchange Feed

An Outbound TAXII Exchange Feed pushes STIX-formatted data to a TAXII server via a mailbox.

Follow these steps to create an Outbound TAXII Exchange Feed:

1. Log in with an Organization Administrator account, or higher, valid for the desired Source.
2. On the top navigation bar (Figure 1**Error! Reference source not found.**), click **Posts** and the **Posts** screen will appear (Figure 3).
3. Click on the desired Source, and its **Source** card will appear on the top left of the screen (Figure 34).
4. Click on the **Source Config**  icon, and the **Source Config** screen will appear (Figure 38).
5. Click the **Data** tab, and the **Data** screen will appear (Figure 39).
6. Click the **+ NEW OUTBOUND** button, and the **Configure Outbound TAXII Exchange** pop-up screen will appear with the **Taxii** tab highlighted (Figure 47).

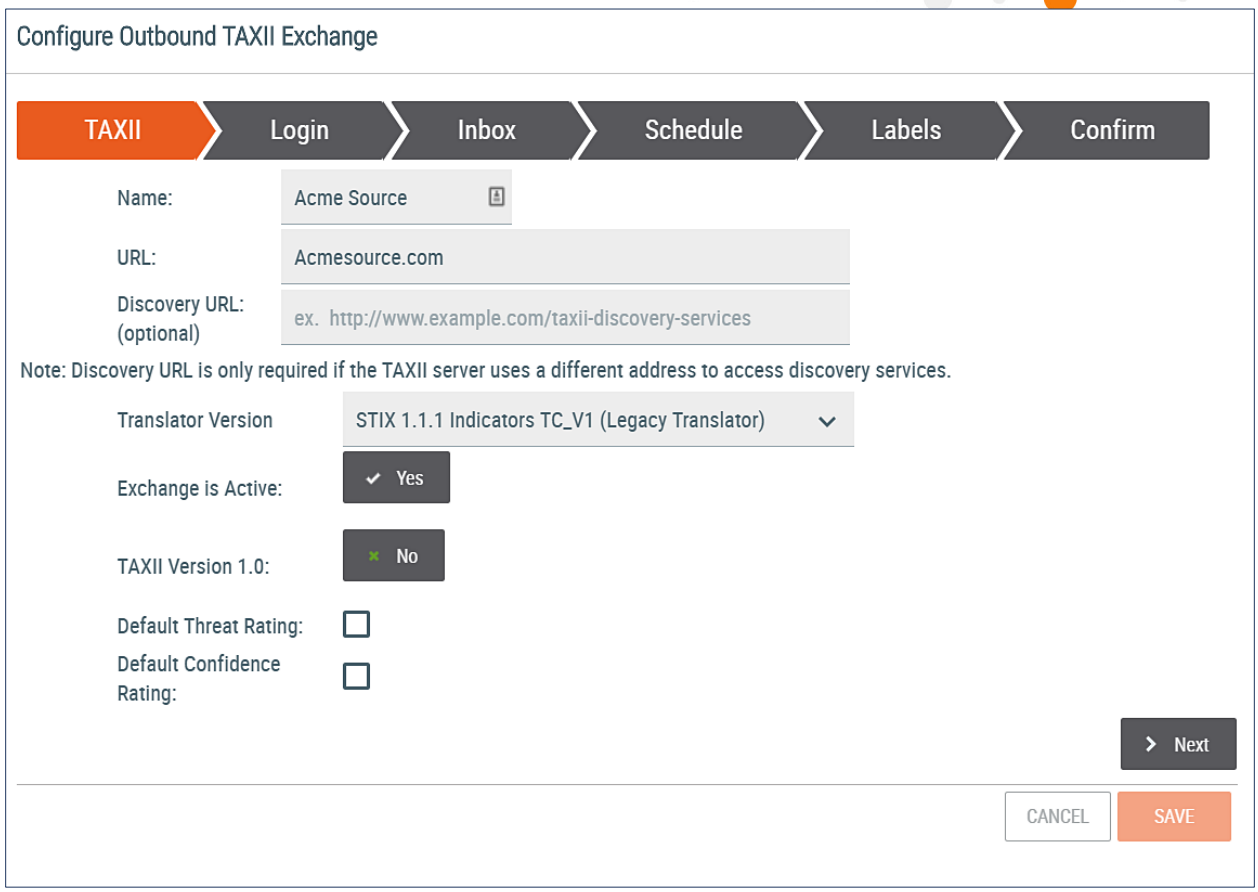

Figure 47

a. **Name**: Click in the box to enter a name.

b. **URL**: Click in the box to enter a URL.

c. **Discovery URL**: If applicable, click in the box to enter a Discovery URL.

d. **Translator Version**: Click the arrow to choose the version.

e. **Exchange is Active**: Click the rectangle to toggle between Yes and No.

f. **Taxii Version** 1.0: Click the rectangle to toggle between Yes and No.

g. **Default Threat Rating**: Click the checkbox to enter a Threat Rating.

h. **Default Confidence Rating**: Click the checkbox to enter a Confidence Rating.

7. Click the **Next** button, and the **Login** screen will appear (Figure 48).

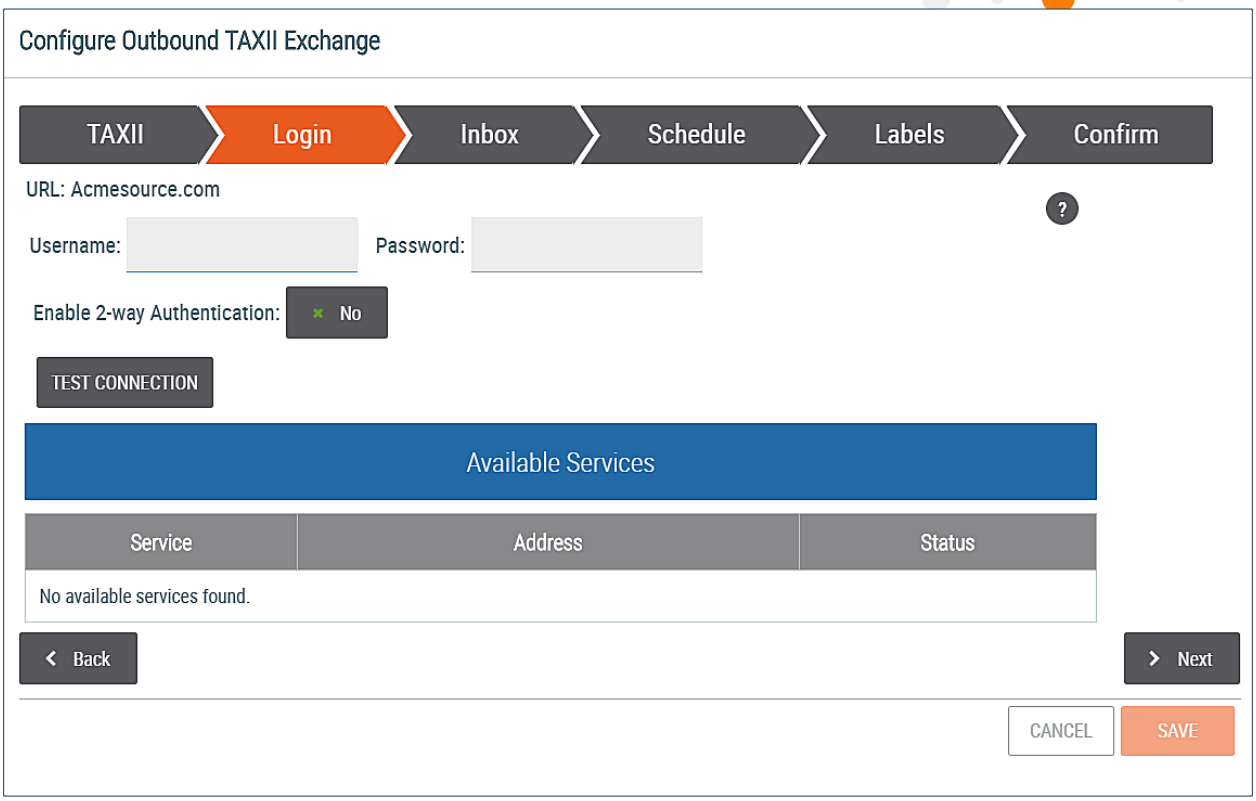

Figure 48

a. **URL**: Verify that the URL displayed is the one entered in the previous step.

b. **Username** and **Password**: Click in the boxes to enter each field.

c. **Enable 2-way Authentication**: Click the rectangle and toggle to **Yes** to provide a **Certificate**. Provide the **Private Key** and **Certificate** found in the **.pem** certificate file.

d. **TEST CONNECTION**: Click on this button to test the connection.

e. Select the appropriate **Service**.

8. Click the **Next** button, and the **Inbox** screen will appear (Figure 49).

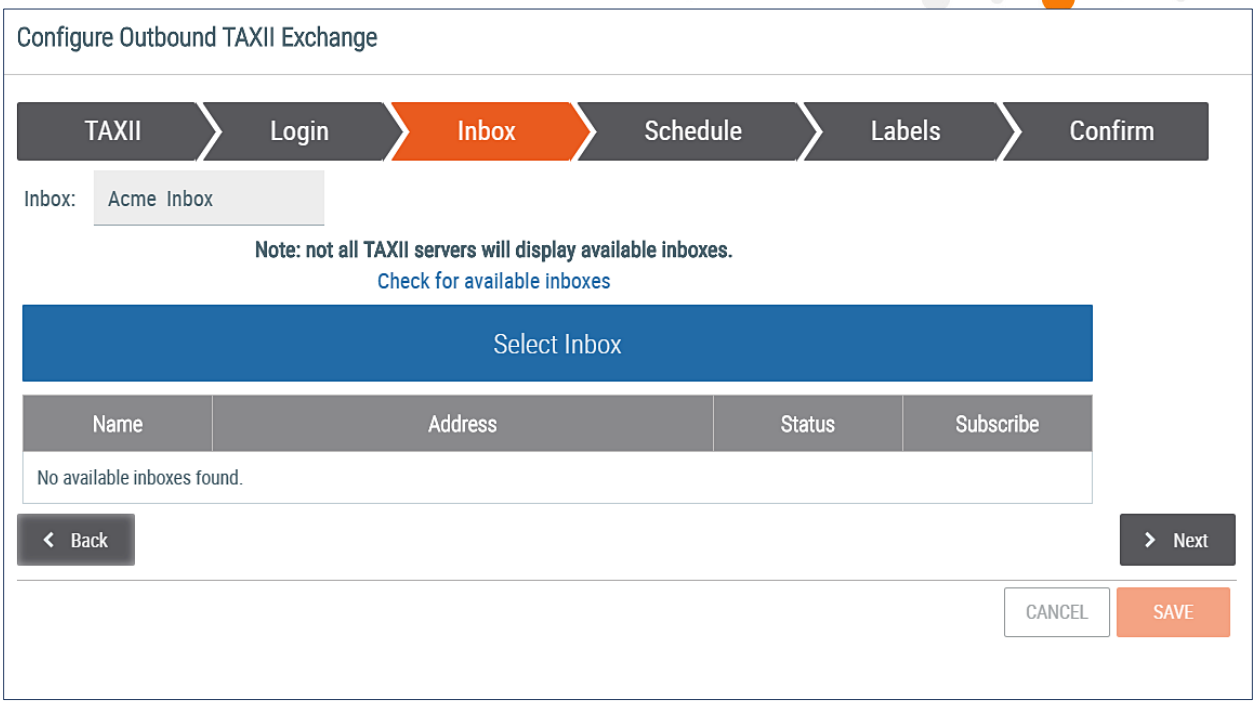

Figure 49

f. **Inbox**: Click in the box to enter a name.

g. **Check for available inboxes**: Click on the text to view and select an Inbox.

9. Click the **Next** button, and the **Schedule** screen will appear (Figure 50).

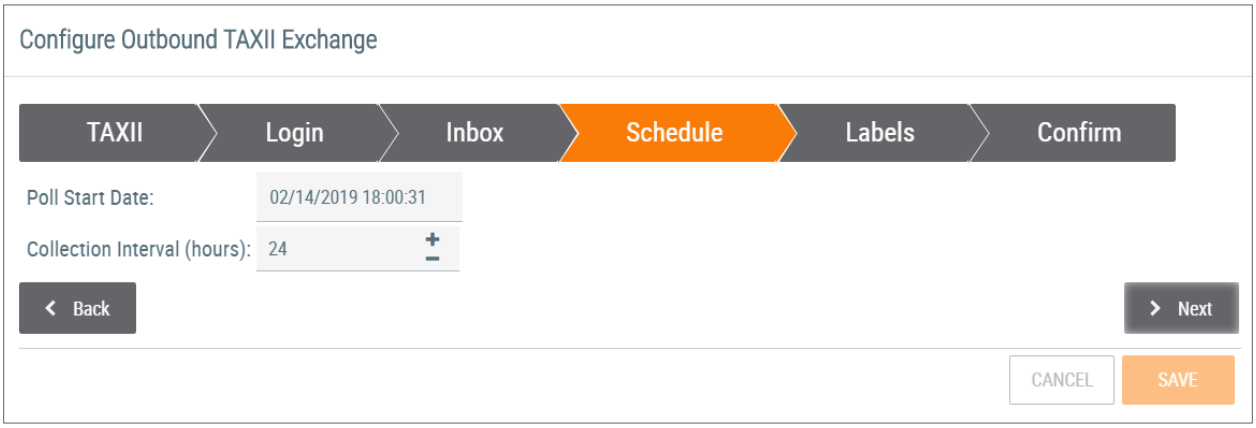

Figure 50

a. **Poll Start Date**: Click in the box, and a calendar will pop up to select the date and time.

b. **Collection Interval**: Click inside the box to manually change the time, or use the plus and minus signs to set the time (in hours).

10. Click the **Next** button, and the **Labels** screen will appear (Figure 51).

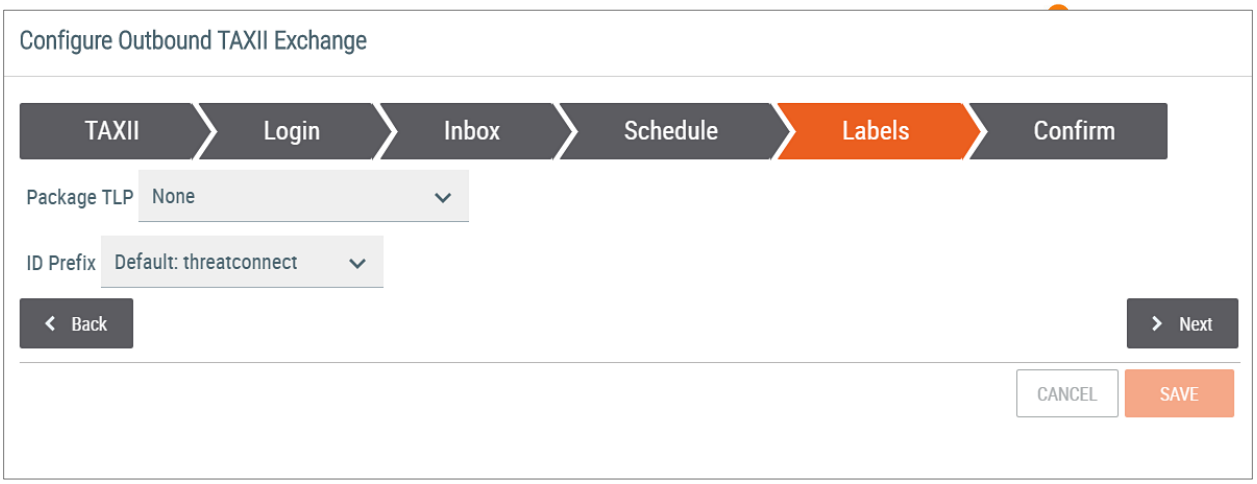

Figure 51

11. If desired, click the **Package TLP** drop-down menu to assign a Security Label to the feed.
12. Click the **ID Prefix** drop-down menu to assign a namespace prefix for generated STIX IDs. The default prefix is **threatconnect**, but the user can also choose the **Source Name** or a **Custom** name as a prefix.
13. Click the **Next** button, and the **Confirm** Screen will appear (Figure 52). Confirm that the entered information is correct.

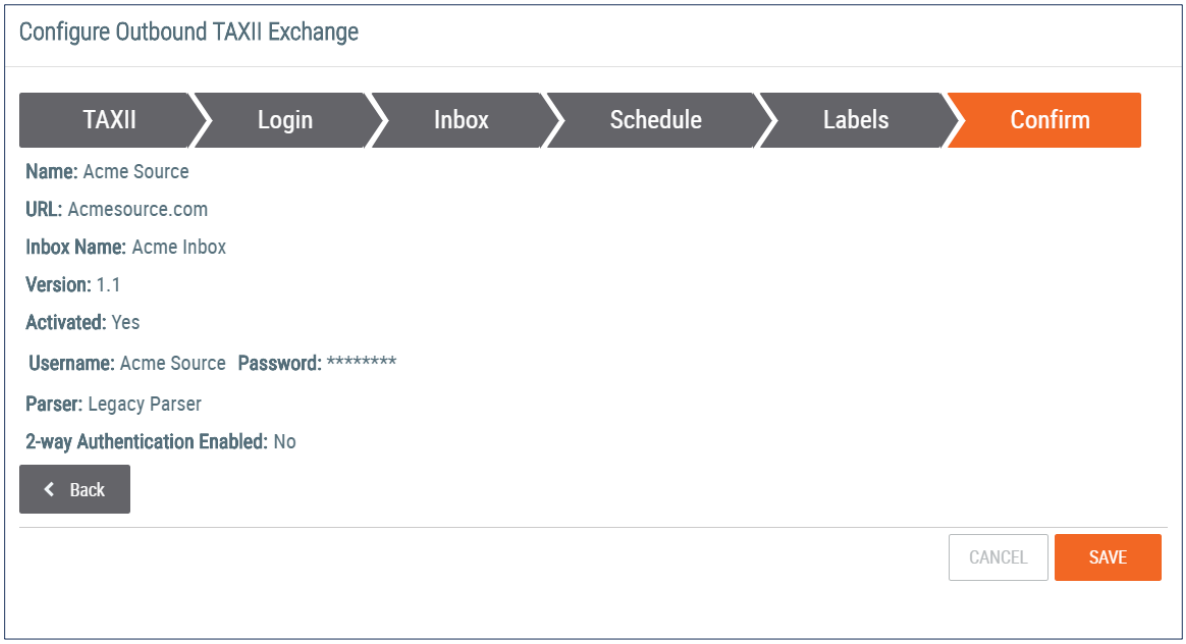

Figure 52

14. Click the **SAVE** button.