

# Community and Source Administration

User Guide

Software Version 6.2

June 21, 2021



©2021 ThreatConnect, Inc.

Threat Connect® is a registered trademark of ThreatConnect, Inc.  
STIX™ and TAXII™ are trademarks of the MITRE Corporation.





## Table of Contents

OVERVIEW.....	5
ACCESS THE COMMUNITY (OR SOURCE) CONFIG SCREEN.....	5
ACCESS THE COMMUNITY (OR SOURCE) INFO SCREEN.....	7
COMMUNITY AND SOURCE ROLES AND ACCESS.....	11
Configure Community and Source Roles .....	11
THE COMMUNITY (AND SOURCE) INFO SCREEN.....	14
Rules/Guidelines .....	14
Invites .....	15
Invite Users to a Community .....	15
Invite Users to a Source.....	16
Restrict Document Storage to Malware Vault .....	17
THE COMMUNITY (AND SOURCE) CONFIG SCREEN.....	18
Attribute Types.....	18
Create Attribute Types.....	18
Upload Attribute Types.....	20
Edit Attribute Types .....	22
Delete Attribute Types.....	23
Attribute Validation Rules.....	23
Create Attribute Validation Rules.....	23
Edit Attribute Validation Rules .....	25
Delete Attribute Validation Rules.....	26
Default Attribute Types .....	26
Create Default Attribute Types .....	26
Edit Default Attribute Types.....	28
Delete Default Attribute Types .....	28
Indicator Exclusions.....	29
Create Indicator Exclusion Lists .....	29
Edit Indicator Exclusion Lists.....	32



Delete Indicator Exclusion Lists.....	32
<b>Security Labels .....</b>	<b>33</b>
Create Security Labels .....	33
Edit Security Labels .....	35
Delete Security Labels .....	35
Consolidate Security Labels .....	36
Apply Security Labels.....	36
<b>Deprecation Rules.....</b>	<b>37</b>
Create Deprecation Rules .....	37
Edit Deprecation Rules.....	38
Delete Deprecation Rules.....	39
<b>Publishing .....</b>	<b>39</b>
View and Download Published Files.....	40
Delete Published Files.....	40
<b>Email Ingestion.....</b>	<b>41</b>
Create a Feed Mailbox.....	41
Create a Phishing Mailbox.....	44
<b>Settings.....</b>	<b>45</b>
Enable DomainTools .....	45
<b>Data .....</b>	<b>46</b>
HTTP Feeds.....	46
TAXII Exchanges .....	47





## 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 **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.

## Access the Community (or Source) Config Screen

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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).

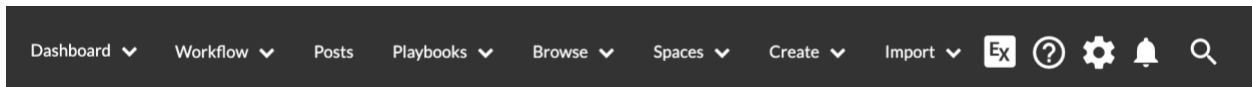


Figure 1

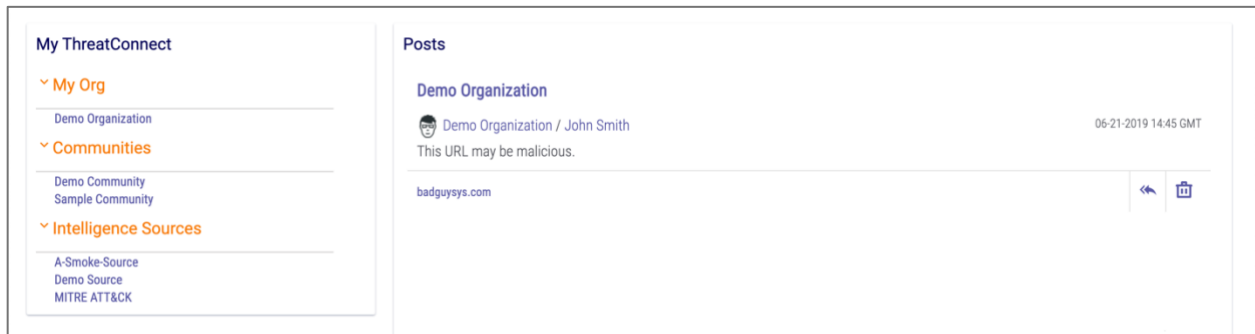


Figure 2

3. Click on the desired Community or Source in the **MyThreatConnect** card, and its **Community** (Figure 3) or **Source** (Figure 4) screen will be displayed.

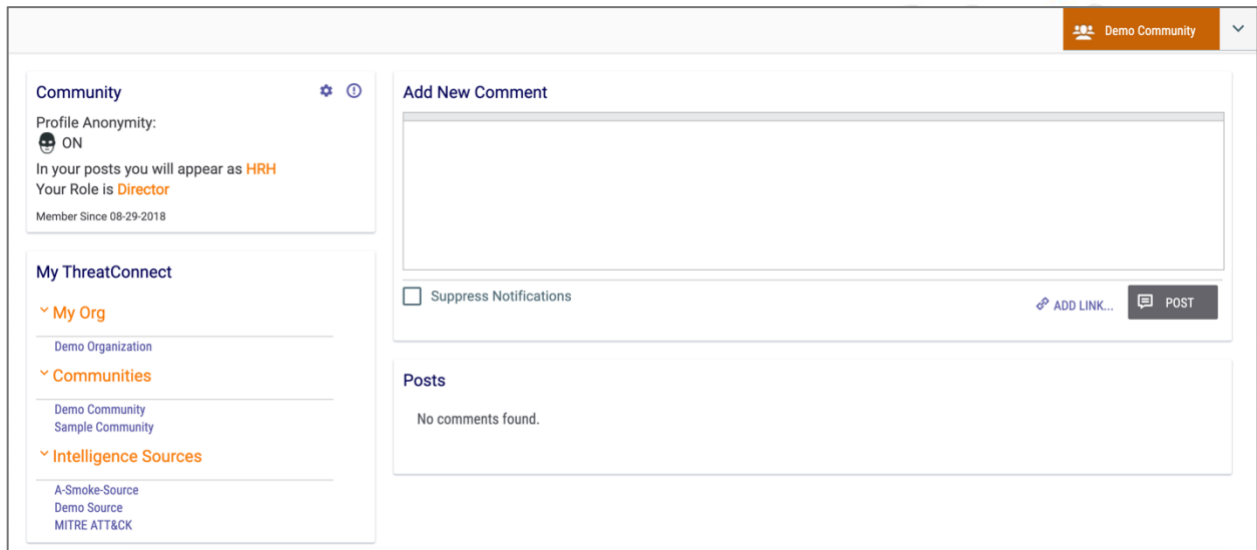


Figure 3

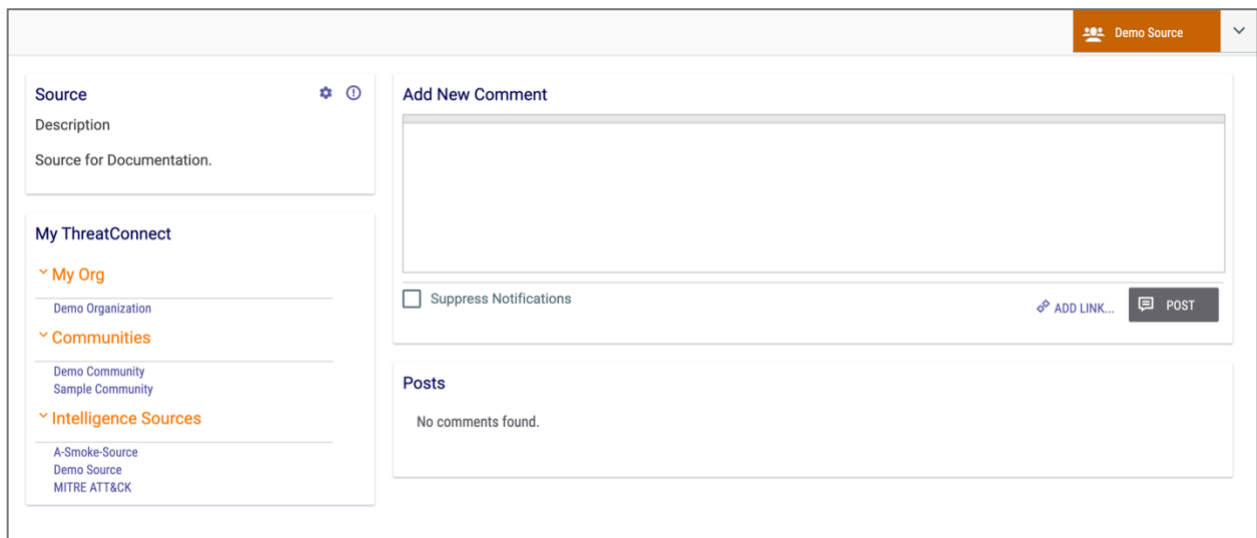



Figure 4

4. Click on the **Community** (or **Source**) **Config**  icon at the upper-right corner of the **Community** or **Source** card, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.



Demo Community - Community Config

Attribute Types | Attribute Validation Rules | Default Attributes | Indicator Exclusions | Security Labels | Deprecation Rules | Publishing | Email | Settings

Include System Types   + NEW   UPLOAD   Attribute Type ▼

Name	Description	Max Length	Types	Error Message	Options
.NET Assembly References (System)	References to assembly made by a .NET file.	500 characters	File	Please enter .NET assembly references of 500 characters or fewer.	
.NET Byte Code (System)	Decompiled .NET byte code.	100K	File	Please enter a .NET byte code string of 102400 characters or fewer.	
.NET Module Version ID (System)	A GUID generated at build time that can be used to find similar .NET assemblies if the binary was modified post build somehow.	36 characters	File	Please enter a GUID value tied to the .NET Module Version ID.	
.NET Source Code (System)	Decompiled .NET byte code into source code.	100K	File	Please enter a decompiled .NET code of 102400 characters or fewer.	
.NET TypeLib ID (System)	The TypeLib ID is a GUID generated by Visual Studio during a .NET project creation.	36 characters	File	Please enter a GUID value tied to the .NET Module Version ID.	
			ASN Address		

Figure 5

Demo Source - Source Config


Attribute Types | Attribute Validation Rules | Default Attributes | Indicator Exclusions | Security Labels | Deprecation Rules | Publishing | Data | Email | Settings

Include System Types   + NEW   UPLOAD   Attribute Type ▼

Name	Description	Max Length	Types	Error Message	Options
.NET Assembly References (System)	References to assembly made by a .NET file.	500 characters	File	Please enter .NET assembly references of 500 characters or fewer.	
.NET Byte Code (System)	Decompiled .NET byte code.	100K	File	Please enter a .NET byte code string of 102400 characters or fewer.	
.NET Module Version ID (System)	A GUID generated at build time that can be used to find similar .NET assemblies if the binary was modified post build somehow.	36 characters	File	Please enter a GUID value tied to the .NET Module Version ID.	

Figure 6

## Access the Community (or Source) Info Screen

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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **MyThreatConnect** card, and its **Community** (Figure 3) or **Source** (Figure 4) screen will be displayed.
4. Click the **Community** (or **Source**) **Info**  icon at the upper-right corner of the **Community** or **Source** card, and the **Community Info** (Figure 7) or **Source Info** screen (Figure 8) will be displayed.



Demo Community

Information Rules/Guidelines Invites

Anonymous Profiles OK

### Community Info

Admin Organization  
Demo Organization

Total Members  
1

Allow Data Copy  
 Restrict Document Storage To Malware Vault

COMMUNITY CONFIG

### Community Members

Filter

Name	Allow Data Copy	Joined	Options
DemoOrg	<input checked="" type="checkbox"/>	08-29-2018	

### Membership

Your Role  
Director Access to administer all data and members

### Profile Anonymity

ON  
Your Pseudonym will be visible

### Notification Options

Follow Posts  
 Follow Contributions  
Notification Priority  
Low

### Description

Documentation Community

Figure 7

Demo Source

Information Invites

### Source Info

Admin Organization  
Demo Organization

Total Members  
1

Allow Data Copy

SOURCE CONFIG

### Source Members

Filter

Name	Allow Data Copy	Joined	Options
Demo Organization	<input checked="" type="checkbox"/>	08-29-2018	

### Description


Source for Documentation.

Figure 8

5. Click the **COMMUNITY CONFIG** or **SOURCE CONFIG** button to access the **Community Config** (Figure 5) or **Source Config** (Figure 6) screen for the selected Community or Source.

Alternatively, the **Community** (or **Source**) **Info** screen can be accessed by logging in with a System Administrator account.



1. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon, and the **Settings** menu will be displayed (Figure 9).

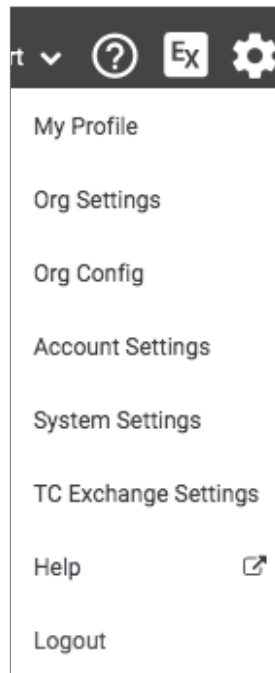


Figure 9

2. Select **Account Settings**. The **Account Settings** screen will be displayed (Figure 10).

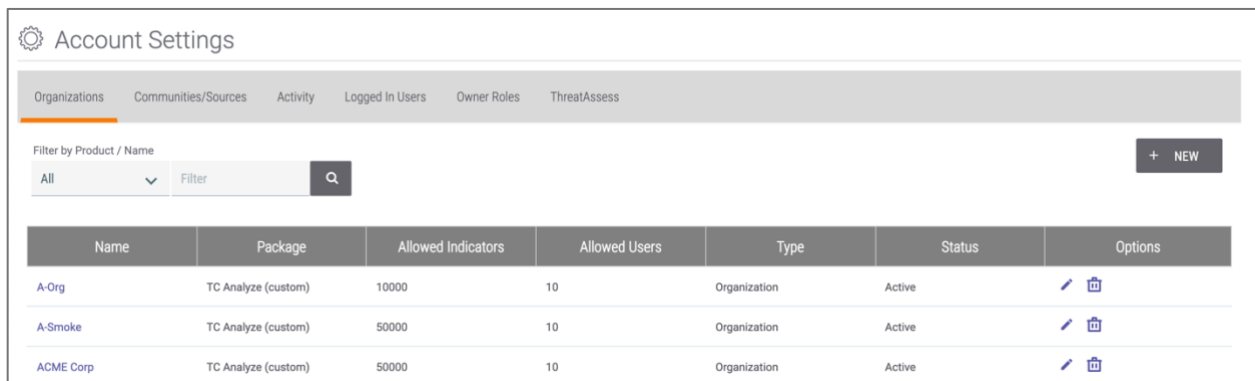


Figure 10

3. Click the **Communities/Sources** tab, and the **Communities/Sources** screen will be displayed (Figure 11).



Account Settings						
Organizations Communities/Sources Activity Logged In Users Owner Roles ThreatAssess						
Filter						+ NEW
Name	Type	Category	Totals	Allowed Indicators	Owner	Options
A-Org-Community	Community		0.0MB Storage	50000	A-Org	
A-Org-Source	Source		0.0MB Storage	50000	A-Org	
A-Smoke-Comm	Community	Premium	0.0MB Storage	50000	A-Smoke	
A-Smoke-Source	Source	ThreatConnect	6.9MB Storage	50000	A-Smoke	

Figure 11

4. On the **Communities/Sources** screen, click on an entry to display its **Community Info** (Figure 7) or **Source Info** (Figure 8) 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 <a href="#">published</a> data from a Community or Source.

***NOTE: 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, be able to use their full profile.

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 be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4), respectively.



### Community

Profile Anonymity:  
 ON

In your posts you will appear as **HRH**  
Your Role is **Director**

Member Since 08-29-2018

Figure 12

### Source

Description

Source for Documentation.

Figure 13

4. Click the **Community Info** icon at the upper-right corner of the **Community** card, and the **Community Info** screen will be displayed (Figure 7).
5. Click the corresponding **Users** icon in the **Options** column to configure the Community Member. The **Membership** window will be displayed (Figure 14).

#### DemoOrg Membership

Default Role: User (Read only access to all data) ▾

Default API Role: Director (Access to administer all data and members) ▾


Filter

Pseudonym	Role
HRH	Director
AC123	User

CLOSE

Figure 14




- **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 the **Edit**  icon to the right of a user's role to change their role. All changes are applied immediately.
6. Click the **CLOSE** button when done.





## The Community (and Source) Info Screen

### Rules/Guidelines

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 be displayed (Figure 2).
3. Click on the desired Community in the **My ThreatConnect** card, and its **Community** card (Figure 12) will be displayed at the upper-left corner of the **Community** screen (Figure 3).
4. Click the **Community Info**  icon at the upper-right corner of the **Community** card, and the **Community Info** screen will be displayed (Figure 7).
5. Click the **Rules/Guidelines** tab, and the **Rules/Guidelines** screen will be displayed (Figure 15).

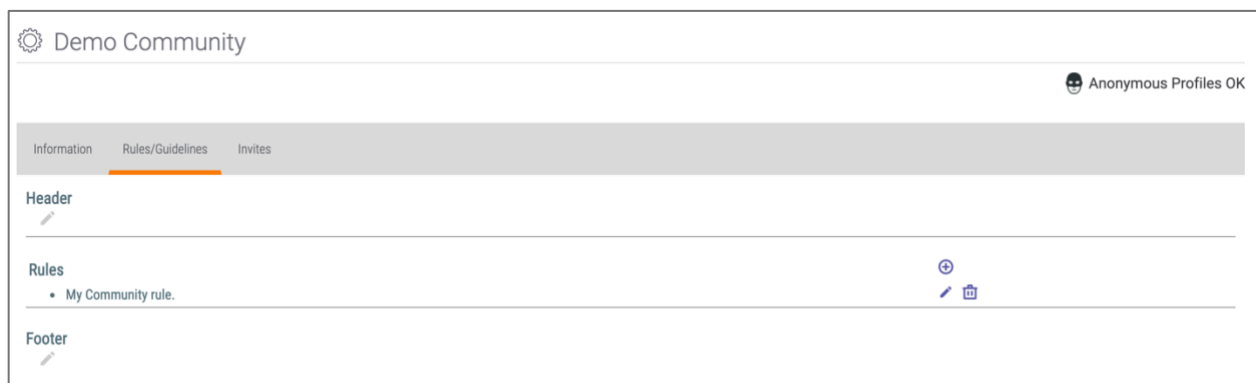


Figure 15






- **Header:** Click the **Edit**  icon to create or edit a header for the Community rules and guidelines.
- **Rules:** For existing rules, click the **Edit**  icon or **Delete**  icon to edit or delete a rule, respectively. To add a new rule to the Community, click the **New Rule**  icon, and the **Create Community Rule** window will be displayed (Figure 16).




Figure 16



- **Order:** The order of appearance for Community rules is sorted incrementally. Enter the corresponding order for the rule, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Text:** Enter the contents of the Community rule.
- Click the **SAVE** button to create the new Community rule.
- **Footer:** Click the **Edit**  icon to create or edit a footer for the Community rules and guidelines.

## Invites

### 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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community in the **My ThreatConnect** card, and its **Community** card (Figure 12) will be displayed at the upper-left corner of the **Community** screen (Figure 3).
4. Click the **Community Info**  icon at the upper-right corner of the **Community** card, and the **Community Info** screen will be displayed (Figure 7).
5. Click the **Invites** tab, and the **Invites** screen will be displayed (Figure 17).

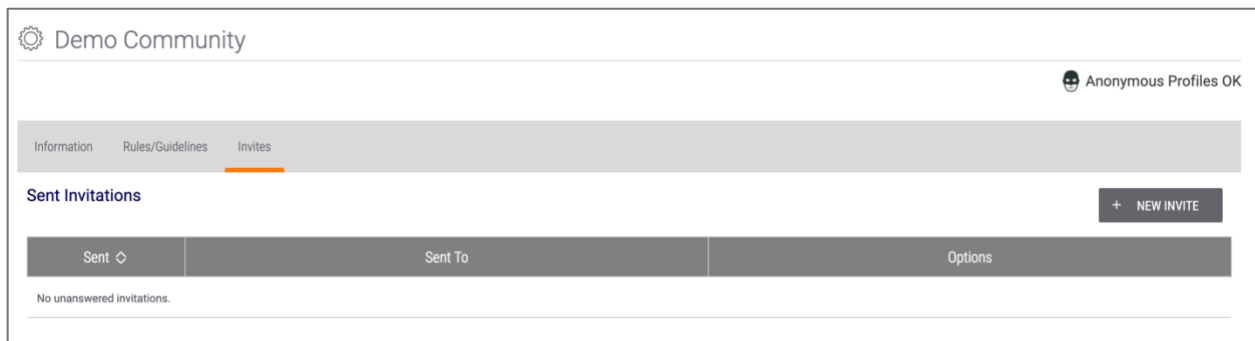


Figure 17

6. Click the **+ NEW INVITE** button, and the **Send Community Invite** window will be displayed (Figure 18).



Figure 18


- **Email Address:** 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 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.

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

## 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 (Figure 1), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Source in the **My ThreatConnect** card, and its **Source** card (Figure 13) will be displayed at the upper-left corner of the **Source** screen (Figure 4).
4. Click on the **Source Info**  icon, and the **Source Info** screen will be displayed (Figure 8).
5. Click the **Invites** tab, and the **Invites** screen will be displayed (Figure 19).

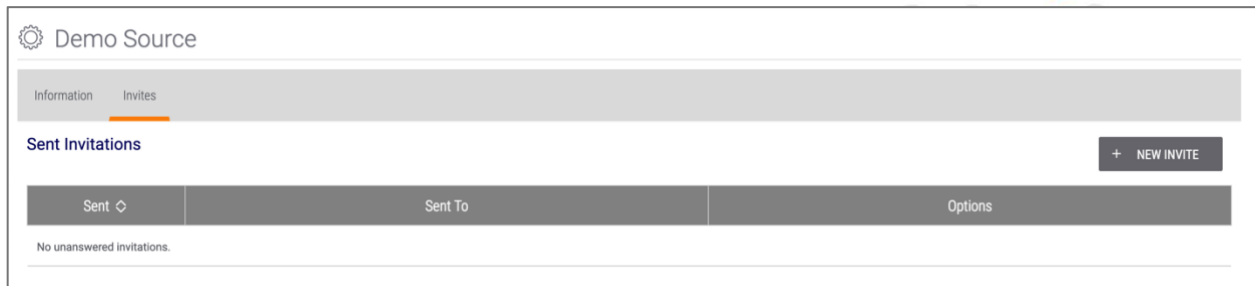


Figure 19

6. Click the **+ NEW INVITE** button, and the **Send Source Invite** window will be displayed (Figure 20).

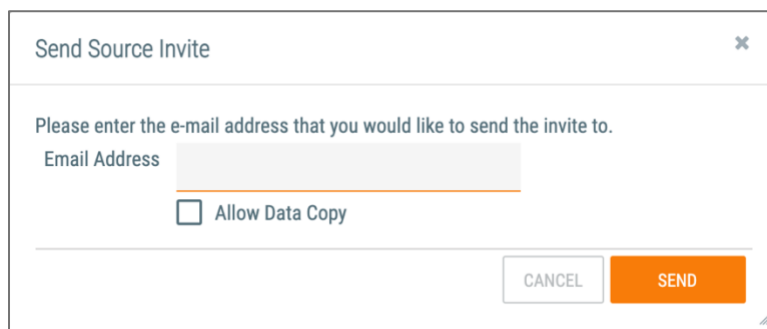



Figure 20

- **Email Address:** Enter the user's email address.
- **Allow Data Copy:** Select the checkbox to grant the user rights to copy data from the Source to a private Organization, if desired.

7. Click the **SEND** button to send the Source Invite.

## Restrict Document Storage to Malware Vault

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 be displayed (Figure 2).
3. Click on the desired Community in the **My ThreatConnect** card, and its **Community** card (Figure 12) will be displayed at the upper-left corner of the **Community** screen (Figure 3).
4. Click the **Community Info**  icon at the upper-right corner of the **Community** card, and the **Community Info** screen will be displayed (Figure 7).
5. Select 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** window, when uploading a file to an existing document via the **Details** screen, and when creating an API document in a Community.




## The Community (and Source) Config Screen

### 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.

#### Create 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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed. Each screen displays existing custom Community or Source Attribute Types as well as the ThreatConnect System Attribute Types, if the **Include System Rules** checkbox is selected.

***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** window will be displayed (Figure 21).



Figure 21

- **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. Alternatively, use the plus and minus symbols to add or subtract increments of 1, respectively.
- **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](#).*

- **Mapping:** Select the Indicators or Groups 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.

## Upload Attribute Types

1. Repeat Steps 1–4 in the “Create Attribute Types” section.
2. Click the **UPLOAD** button, and the **Upload Attributes** window will be displayed (**Error! Reference source not found.**).

Upload Attributes

+ SELECT FILE

Upload any text file in the format:

Name, Description, Error Message, Length, Applicable Types

For example:

```
Report ID,My Report ID,Invalid report ID,50,Incident|Host|Url|Address  
Report Type,My Report Type,Invalid Report Type,100,Incident|Document
```

Note that ',' is used as a column delimiter, but '|' is used to delimitate applicable types.

CANCEL

**Figure 22**

3. Click the + **SELECT FILE** button to locate and select a file to upload, and then 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",
        "Document",
        "Email",
        "Incident",
        "Campaign",
        "Threat"
      ],
      "indicators": [
        "Address",
        "EmailAddress",
        "File",
        "Host",
        "Url"
      ],
      "maxLength": 100,
      "name": "System Attribute Type Name",
      "system": false,
      "version": 2
    }
  ]
}
```


## Edit Attribute Types

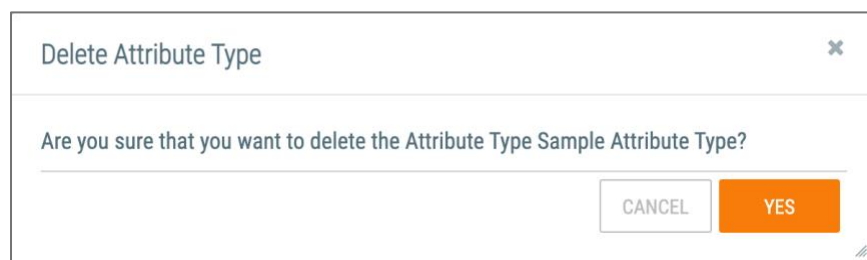
1. Repeat Steps 1-4 in the "Create Attribute Types" section.
2. Use the **Attribute Type** drop-down menu to select the custom Attribute Type to modify.  
***NOTE:** To quickly find the custom Attribute Type to modify, deselect the Include System Types checkbox.*
3. Click the **Edit**  icon in the **Options** column for the desired Attribute Type. The **Configure Attribute Type** window will be displayed (Figure 21).



4. Configure the fields for the custom Attribute Type as appropriate.
5. Click the **SAVE** button to save changes to the custom Attribute Type.

## Delete Attribute Types

1. Repeat Steps 1–4 in the “Create Attribute Types” section.
2. Use the **Attribute Type** drop-down menu to select the custom Attribute Type to modify.
3. Click the **Delete**  icon in the **Options** column for the desired Attribute Type. The **Delete Attribute Type** window will be displayed (Figure 23).




**Figure 23**

4. Click the **YES** button to delete the Attribute Type.

## Attribute Validation Rules

### Create Attribute Validation Rules

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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Attribute Validation Rules** tab, and the **Attribute Validation Rules** screen will be displayed (Figure 24), displaying the existing Community or Source Attribute Validation Rules as well as the ThreatConnect System Attributes Validation Rules, if the **Include System Rules** checkbox is selected.



Demo Community - Community Config

Attribute Types | **Attribute Validation Rules** | Default Attributes | Indicator Exclusions | Security Labels | Deprecation Rules | Publishing | Email | Settings

Include System Rules    + NEW

Name	Type	Rule	Description	Options
128-bit Hex String (System)	Regex	[hidden]	128-bit hexadecimal string.	
32-bit Hex String (System)	Regex	[hidden]	32-bit hexadecimal string.	
512-bit Hex String (System)	Regex	[hidden]	512-bit hexadecimal string.	
Adversary Motivation Type (System)	SelectOne	[hidden]	The general intent of the attackers or adversary.	

Figure 24

6. To create a new Community or Source Attribute Validation Rule, click the + NEW button. The **Create Attribute Validation Rule** window will be displayed (Figure 25).

Create Attribute Validation Rule [X]

Type  
Regex [v]

Name \*  
[Text Input]

Description \*  
[Text Area]

Enter a valid Regular Expression  
[Text Area]

[CANCEL] [SAVE]


Figure 25

- **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 21) 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.
7. Click the **SAVE** button to save the new Attribute Validation Rule.
- NOTE: The custom Attribute Validation Rule will need to be assigned to an Attribute in order to validate user input.***

## Edit Attribute Validation Rules

1. Repeat Steps 1–5 in the “Create Attribute Validation Rules” section.
  2. Click the **Edit**  icon in the **Options** column for the desired Attribute Validation Rule (Figure 26). The **Create Attribute Validation Rule** window will be displayed (Figure 25).
- NOTE: To quickly find the custom Attribute Validation Rule to modify, deselect the Include System Rules checkbox.***



**Figure 26**

3. Configure the fields for the custom Attribute Validation Rule as appropriate.
4. Click the **SAVE** button to save changes to the custom Attribute Validation Rule.



## Delete Attribute Validation Rules


1. Repeat Steps 1–5 in the “Create Attribute Validation Rules” section.
2. Click the **Delete**  icon in the **Options** column for the desired Attribute Validation Rule. The **Delete Attribute Validation Rule** window will be displayed (Figure 27).



Figure 27

3. Click the **YES** button to delete the custom Attribute Validation Rule.

## 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 the Group or Indicator is created.

### Create 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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Default Attributes** tab, and the **Default Attributes** screen will be displayed (Figure 28), displaying the existing Community or Source default Attribute Types.



Figure 28

- To create a new Community or Source default Attribute Type, click the **+ NEW** button, and the **Create Default Attribute Type** window will be displayed (Figure 29).

Figure 29


- Attribute Type:** Select an Attribute Type defined on the **Attribute Types** tab of the **Community Config** screen (Figure 5).  
*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.  
*NOTE: 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, or use the plus and minus symbols to add or subtract increments of 1, respectively. 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.

7. Click the **SAVE** button to create the default Attribute Type.

## Edit Default Attribute Types

1. Repeat Steps 1-5 in the “Create Default Attribute Types” section.
2. Click the **Edit**  icon in the **Options** column for the desired default Attribute Type (Figure 30). The **Create Attribute Validation Rule** window will be displayed (Figure 29).

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




The screenshot shows a web application interface titled "Demo Community - Community Config". At the top, there is a navigation bar with tabs: "Attribute Types", "Attribute Validation Rules", "Default Attributes", "Indicator Exclusions", "Security Labels", "Deprecation Rules", "Publishing", "Email", and "Settings". The "Default Attributes" tab is selected. Below the navigation bar is a "+ NEW" button. The main content area displays a table with the following columns: "Type", "Attribute", "Message", "Sort Index", and "Options". The table contains one row with the following data: "File", ".NET Assembly References", "Test", "1", and an edit/delete icon.

Type	Attribute	Message	Sort Index	Options
File	.NET Assembly References	Test	1	 

Figure 30

3. Configure the fields for the default Attribute Type as appropriate.
4. Click the **SAVE** button to save changes to the default Attribute Type.

## Delete Default Attribute Types

1. Repeat Steps 1-5 in the “Create Default Attribute Types” section.
2. Click the **Delete**  icon in the **Options** column for the desired default Attribute Type. The **Delete Default Attribute Type** window will be displayed (Figure 31).

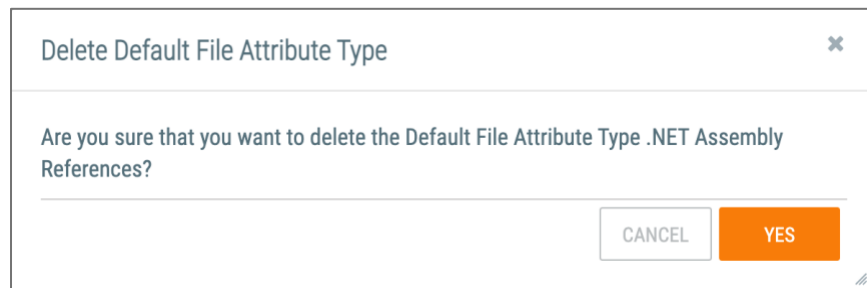


Figure 31


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


### Create Indicator Exclusion Lists

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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Indicator Exclusions** tab, and the **Indicator Exclusions** screen will be displayed (Figure 32).



Type	Exclusion Count	Options
Address-IPv4	None	
Address-IPv6	None	
ASN-AS Number	None	

Figure 32

6. Click the **Edit**  icon in the **Options** column for an Indicator (File-SHA1 in this example), and the **Exclusion Details** window will be displayed (Figure 33).



File-SHA1 Exclusion Details

Custom

<No exclusions specified.>

+ UPLOAD FILE

CANCEL SAVE

**Figure 33**

7. When creating a new Exclusion List, enter the information directly into the **Custom** text box, and click the **SAVE** button (Figure 34).





File-SHA1 Exclusion Details

Custom

2jfdj43ybu54b8s8b3ub73gb

+ UPLOAD FILE

CANCEL SAVE

**Figure 34**

- To upload a file, click the + **UPLOAD FILE** button to navigate to locate and select a file. After a file is selected, the Exclusion list will be uploaded (Figure 35).

**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.*



File-SHA1 Exclusion Details

Custom

G4737GBJSBDJIHLDLKBAGSFF6QCGGGV33545477767

+ UPLOAD FILE    DOWNLOAD    CLEAR

CANCEL    SAVE

Figure 35

9. Click the **SAVE** button.

## Edit Indicator Exclusion Lists

1. Repeat Steps 1–6 in the “Create Indicator Exclusion Lists” section.
2. 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 35).
3. 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

1. Repeat Steps 1–6 in the “Create Indicator Exclusion Lists” section.
2. Click the **CLEAR** button (Figure 35), and the **Remove Exclusions** window will be displayed (Figure 36).

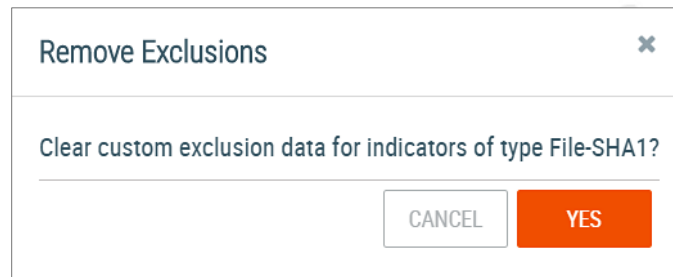



Figure 36

3. Click the **YES** button, followed by 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 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.

### Create Security Labels

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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Security Labels** tab, and the **Security Labels** screen will be displayed (Figure 37), displaying existing custom Community or Source Security Labels as well as the ThreatConnect System Labels, if the **Include System Labels** checkbox is selected.



Demo Community - Community Config

Attribute Types   Attribute Validation Rules   Default Attributes   Indicator Exclusions   **Security Labels**   Deprecation Rules   Publishing   Email   Settings

Include System Labels   **+ NEW SECURITY LABEL**

Name	Description	Options
TLP:AMBER	This security label is used for information that requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	
TLP:GREEN	This security label is used for information that is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	
TLP:RED	This security label is used for information that cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	
TLP:WHITE	This security label is used for information that carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	

Figure 37

- To create a new Community or Source Security Label, click the **+ NEW SECURITY LABEL** button, and the **Create Security Label** window will be displayed (Figure 38).

### Create Security Label ✕

Name \*

Color

Description \*

Figure 38

- Name:** Enter a name for the Security Label.




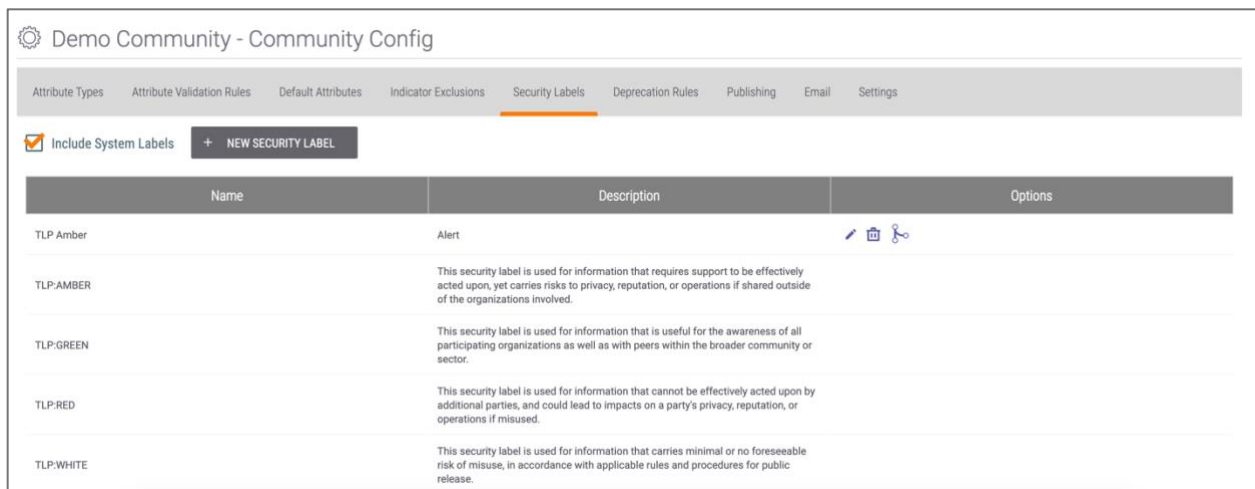
- **Color:** Click in the box to display the color picker. Users can enter a color value in RGB, HSB, or hexadecimal format, or select a color by clicking and dragging the circle in the color field.
- **Description:** Enter a description for the Security Label.




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

7. Click the **SAVE** button to save the custom Community or Source Security Label.

## Edit Security Labels

1. Repeat Steps 1–5 in the “Create Security Labels” section.
2. Click the **Edit**  icon in the **Options** column (Figure 39), and the **Create Security Label** window will be displayed (Figure 38).




Name	Description	Options
TLP:Amber	Alert	  
TLP:AMBER	This security label is used for information that requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	
TLP:GREEN	This security label is used for information that is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	
TLP:RED	This security label is used for information that cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	
TLP:WHITE	This security label is used for information that carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	

**Figure 39**

3. Make the desired changes to the Security Label, and then click the **SAVE** button.

## Delete Security Labels

1. Repeat Steps 1–5 in the “Create Security Labels” section.
2. Click the **Delete**  icon in the **Options** column (Figure 39), and the **Delete Security Label** window will be displayed (Figure 40).

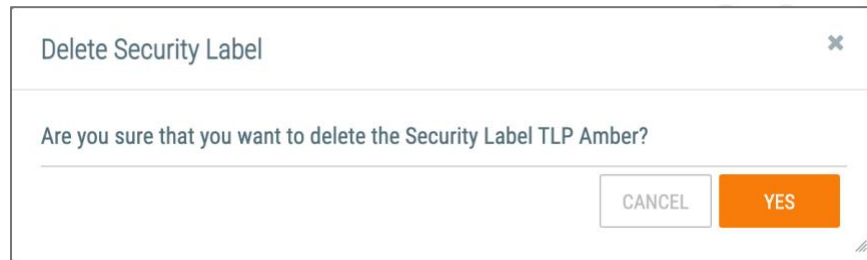



Figure 40

3. Click the **YES** button to delete the Security Label.

## Consolidate Security Labels

1. Repeat Steps 1-5 in the "Create Security Labels" section.
2. Click the **Consolidate**  icon in the **Options** column (Figure 39), and the **Consolidate Security Label** window will be displayed (Figure 41).

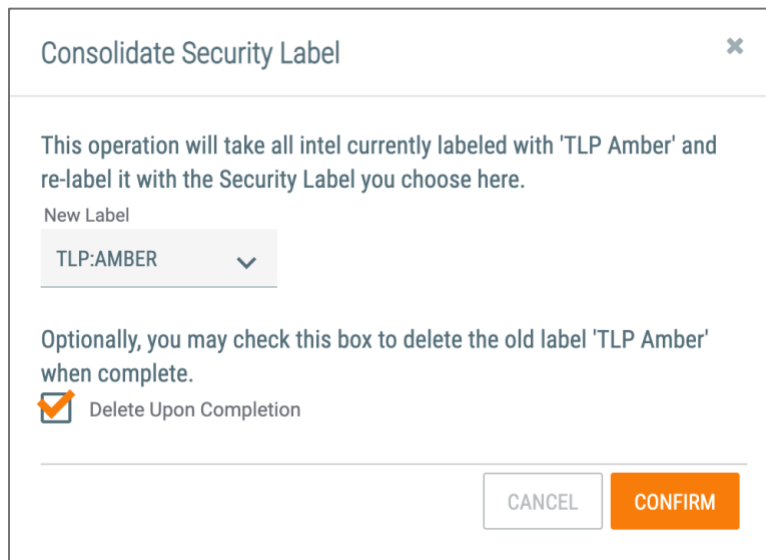


Figure 41

- **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.

3. Click the **CONFIRM** button to consolidate the selected Security Labels.

## 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

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.

### Create Deprecation Rules


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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Deprecation Rules** tab, and the **Deprecation Rules** screen will be displayed (Figure 42).



Figure 42




6. To create a new Deprecation Rule, click + **NEW** button, and the **Create/Edit Deprecation Rule** window will be displayed (Figure 43).

**Figure 43**

- **Indicator Type:** Select the Indicator Type to which the Deprecation Rule will be applied.
- **Confidence Amount:** Enter the amount by which the Confidence Rating should decrease if not updated by a ThreatConnect user, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Percentage:** Select the checkbox to use the value entered in the **Confidence** box as a percentage instead of a numerical value. For example, if the **Confidence** is 5 and **Percentage** is unchecked, the Confidence Rating will drop by a value of 5 (e.g., from 60 to 55) when it is deprecated. If the **Confidence** is 5 and **Percentage** is checked, the Confidence Rating will drop by 5% (e.g., from 60 to 57).
- **Action At Minimum:** Select an action to take when the Confidence Rating of an Indicator drops to 0. Options include **None**, **Set Inactive**, and **Delete**.
- **Interval:** Enter the number of days after which the Confidence Rating should decrease, or use the plus and minus symbols to add or subtract increments of 1, respectively.
- **Recurring:** Select the checkbox for the Deprecation Rule to be applied on a recurring basis instead of just once.

7. Click the **SAVE** button to create the new Deprecation Rule.

## Edit Deprecation Rules

1. Repeat Steps 1–5 in the “Create Deprecation Rules” section.
2. Click the **Edit**  icon in the **Options** column (Figure 44), and the **Create/Edit Deprecation Rule** window will be displayed (Figure 43).



Indicator Type	Interval	Amount	Percentage	Recurring	Action At Minimum	Options
Address	1 day	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	None	

Figure 44

3. Make the desired changes to the Deprecation Rule, and then click the **SAVE** button.

### Delete Deprecation Rules

1. Repeat Steps 1–5 in the “Create Deprecation Rules” section.
2. Click the **Delete** icon in the **Options** column (Figure 44), and the **Delete Deprecation Rule** window will be displayed (Figure 45).

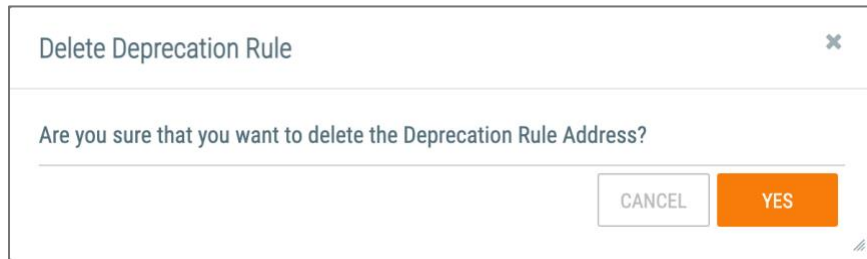


Figure 45

3. 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 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.

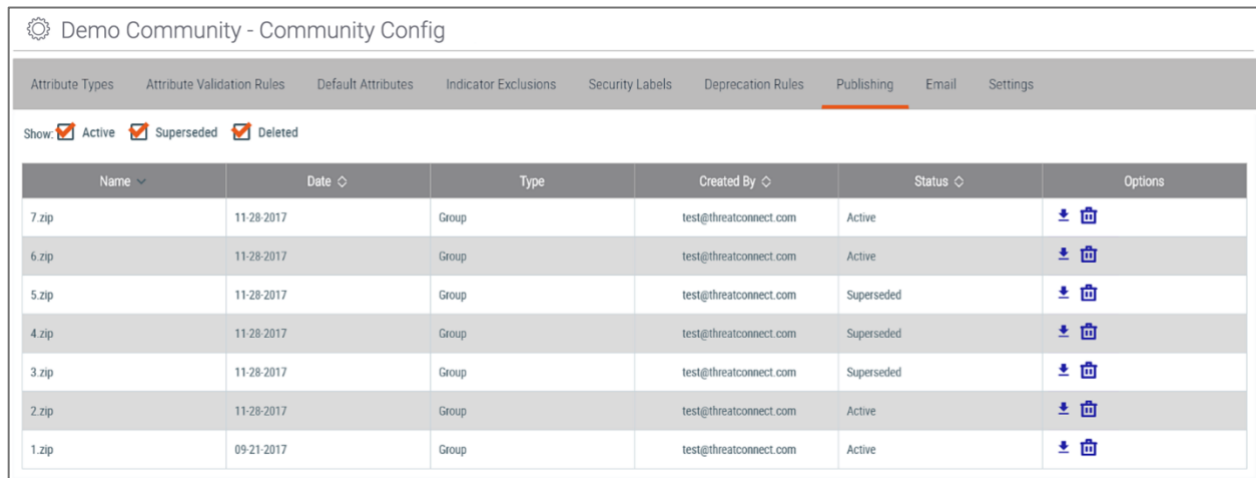
All types of Group data objects (Adversary, Campaign, Document, E-mail, Event, Incident, Intrusion Set, Report, Signature, Threat, and Task) can be published. In order to publish a Group, it must first exist in, or be contributed to, a Community or Source. See [Contributing to a Community or Source](#) for more details.

The Publish feature is accessible by navigating to the **Browse** screen, and then selecting a Group object from the table that is displayed. In the following section, users will only view and download already-published JSON files.



## View and Download Published 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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Publishing** tab, and the **Publishing** screen will be displayed (Figure 46).



















Name	Date	Type	Created By	Status	Options
7.zip	11-28-2017	Group	test@threatconnect.com	Active	 
6.zip	11-28-2017	Group	test@threatconnect.com	Active	 
5.zip	11-28-2017	Group	test@threatconnect.com	Superseded	 
4.zip	11-28-2017	Group	test@threatconnect.com	Superseded	 
3.zip	11-28-2017	Group	test@threatconnect.com	Superseded	 
2.zip	11-28-2017	Group	test@threatconnect.com	Active	 
1.zip	09-21-2017	Group	test@threatconnect.com	Active	 

Figure 46

6. Determine the type of files to display by selecting the **Active**, **Superseded**, or **Deleted** checkboxes.
7. Click the **Download**  icon in the **Options** column for the published file that should be downloaded. The file will be saved to the computer's **Downloads** folder.

## Delete Published Files

1. Repeat Steps 1–6 in the “View and Download Published Files” section.
2. Click the **Delete**  icon in the **Options** column (Figure 46) for the file that should be deleted, and the **Delete Publication** window will be displayed (Figure 47).

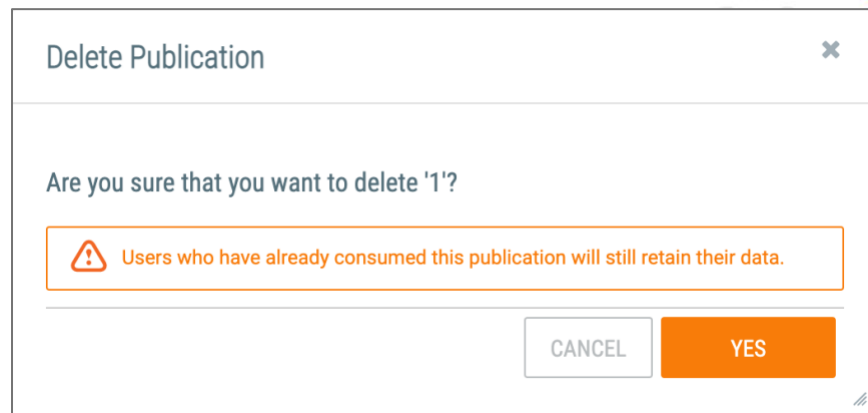


Figure 47

3. Click the **YES** button to delete the published file.

## 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, 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.

## 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. Log in with an Organization Administrator account, or higher, valid for the desired Community or Source.
2. On the top navigation bar (Figure 1), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).

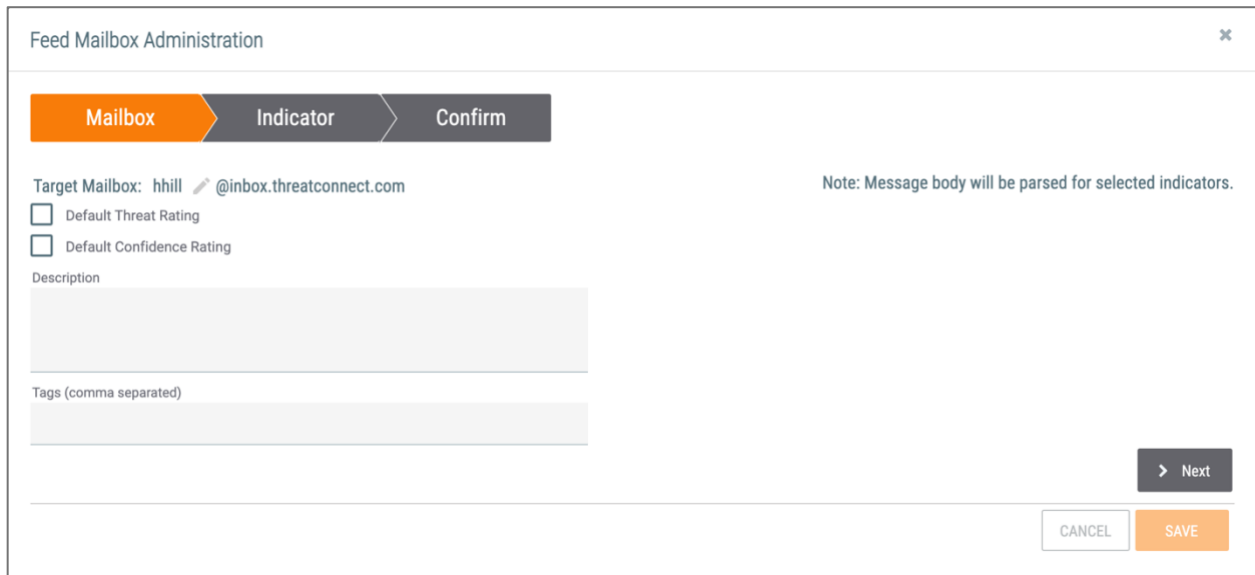


- Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
- Click the **Email** tab, and the **Email** screen will be displayed (Figure 48).



**Figure 48**

- Click the **Create Feed Mailbox** button. The **Feed Mailbox Administration** window will be displayed, with the **Mailbox** tab highlighted (Figure 49).



**Figure 49**

- 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, or use the plus and minus icons to add or subtract increments of 1, respectively.
- Description:** Enter a description for the Feed Mailbox.
- Tags:** Enter any Tags, separated by commas, for the Feed Mailbox.



7. Click the **Next** button, and the **Indicator** tab will be displayed (Figure 50).

Feed Mailbox Administration

Mailbox Indicator Confirm

Host

Enable Host  Use System Import Rules  
 Activate DNS  Activate Whois

Regex: Populate with Example

De-Sanitize Find Regex (Optional):

De-Sanitize Replace Regex (Optional):

1000 characters remaining.

< Back > Next

CANCEL SAVE

**Figure 50**

- **< 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, and the **Confirm** tab screen will be displayed (Figure 51).

Feed Mailbox Administration

Mailbox   Indicator   **Confirm**

Target Mailbox: dtorh@qa-101.int.tc-ops.com  
Mailbox Type: Feed  
Parse Type: Body

Host Regex Enabled: Yes      Using: System Import Regex  
Address Regex Enabled: No  
Email Address Regex Enabled: No  
URL Regex Enabled: No  
File Regex Enabled: No  
ASN Regex Enabled: No  
CIDR Regex Enabled: No  
Sample Regex Enabled: No  
Single Number Regex Enabled: No  
Single Text Case Regex Enabled: No  
Single Text Lower Regex Enabled: No  
Single Text Upper Regex Enabled: No

< Back      CANCEL      SAVE

**Figure 51**

- Review the selections, and then click the **SAVE** button to create the feed mailbox.

## 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.


For steps on how to create a phishing mailbox, see [Creating a Phishing Mailbox](#).



## Settings

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

### Enable 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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Settings** tab, and the **Settings** screen will be displayed (Figure 52).

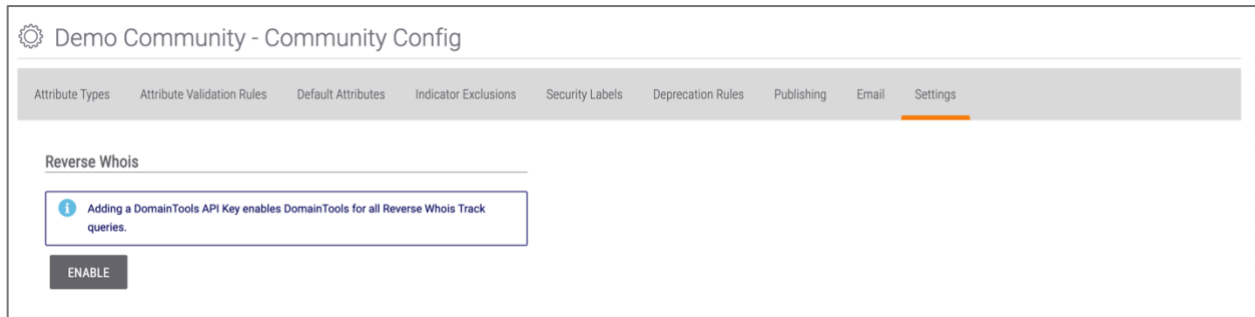


Figure 52

6. Click the **ENABLE** button, and the **Setup DomainTools** window will be displayed (Figure 53).

Figure 53

- **User Name:** Enter a username for the account.




- **API Key:** Enter a valid API key to enable DomainTools.

7. Click the **SAVE** button to enable DomainTools.

## Data

From the **Data** tab, users can create a variety of Source feeds, including HTTP Feeds, and inbound and outbound TAXII Exchange Feeds.

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), click **Posts**, and the **Posts** screen will be displayed (Figure 2).
3. Click on the desired Community or Source in the **My ThreatConnect** card, and its **Community** (Figure 12) or **Source** card (Figure 13) will be displayed at the upper-left corner of the **Community** (Figure 3) or **Source** screen (Figure 4).
4. Click on the **Community** (or **Source**) **Config**  icon, and the **Community Config** (Figure 5) or **Source Config** screen (Figure 6) will be displayed.
5. Click the **Data** tab, and the **Data** screen will be displayed (Figure 54).

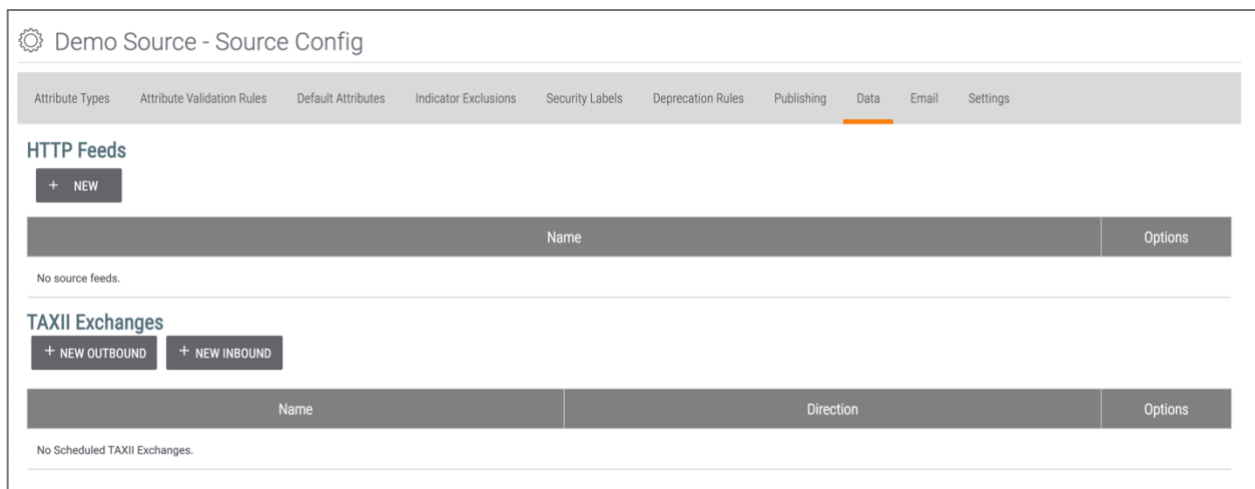


Figure 54

## 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](#).

