



Organization Administration

User Guide

Software Version 6.2

June 21, 2021

10012-10 EN Rev. A



ThreatConnect™

©2021 ThreatConnect, Inc.

Threat Connect® is a registered trademark of ThreatConnect, Inc.

TC Exchange™ is a trademark of ThreatConnect, Inc.

Farsight Security™ is a trademark of Farsight Security, Inc.

Google Authenticator™ is a trademark of Google LLC.





Table of Contents

OVERVIEW	6
THE ORGANIZATION SETTINGS SCREEN	6
Membership	7
Creating User Accounts	8
Editing User Accounts.....	8
Deleting User Accounts.....	8
Communities/Sources	9
View and Manage Community and Source Membership	9
Change Pseudonym	10
Groups	10
View and Manage Groups.....	10
Create a New Group.....	11
Edit a Group	11
Delete a Group	12
Invitations	13
Activity	14
Variables	15
Add a Variable	15
Edit a Variable	16
Delete a Variable	16
Metrics	16
Create a Metric	17
Edit a Metric.....	17
Delete a Metric	17
Clear Metric Data.....	17
Settings	18
Passive DNS	18
Reverse Whois	19
Login IP Filter.....	21
Playbook IP Filter	22
Email	23
View and Manage Mailboxes	23



Phishing Mailbox	24
Feed Mailbox	25
Apps.....	28
Jobs.....	28
App Delivery	32
Environments	32
API Token	33
Profiles.....	33
Styling.....	35
PDF Header.....	35
PDF Report Disclaimer	36
THE ORGANIZATION CONFIG SCREEN	37
Attribute Types.....	37
View Attribute Types	37
Create Attribute Type.....	38
Upload Attribute Type.....	39
Attribute Validation Rules.....	40
View Attribute Validation Rules	40
Create Attribute Validation Rule.....	41
Default Attributes.....	42
View Default Attribute Types.....	43
Create Default Attribute Type	43
Indicator Exclusions.....	44
View Indicator Exclusions.....	45
Create Indicator Exclusion List	45
Edit Indicator Exclusion List	46
Delete Indicator Exclusion List.....	47
Potential Associations Exclusions	47
View Potential Associations Exclusions	48
Create Potential Associations Exclusion List	48
Edit Potential Associations Exclusion List	50
Delete Potential Associations Exclusion List	50
Security Labels	51
View Security Labels	51



Create Security Label.....	52
Edit Security Label	52
Delete Security Label	52
Consolidate Security Label.....	53
Deprecation Rules.....	53
Create Deprecation Rule	54
Edit Deprecation Rule.....	54
Delete Deprecation Rule.....	55



Overview

An Organization, often referred to as an Org, is one of three owner types in ThreatConnect®. (The other two types are Community and Source. See the *ThreatConnect Community and Source Administration Guide* for more information.) It is where the majority of enriched, analyzed, actioned intelligence resides for a user and other members of their team. It is also a space where members can work on tasks and collaborate with each other.


Organization Administration is carried out in ThreatConnect by users with an [Organization role](#) of Organization Administrator. Organization Administrators have full administrative control for their Organization, allowing them to assign or delete user accounts, set permissions, set pseudonyms for individual users or for the Organization, and join Communities. See [ThreatConnect Owner Roles and Permissions](#) for more information on the specific permissions that Organization Administrators have with respect to intelligence access, threat intelligence, Workflow, and Playbooks in their Organization.

At least one Organization Administrator must exist per Organization account, and one is created at the same time as the Organization.

This guide covers the functionalities available to Organization Administrators on the **Organization Settings** and **Organization Config** screen.

The Organization Settings Screen

The **Organization Settings** screen provides a tabbed interface where Organization Administrators can manage their Organization's structure and capabilities in ThreatConnect. Follow these steps to view the **Organization Settings** screen:

1. Log in with an Organization Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon, and the **Settings** menu will be displayed (Figure 2).

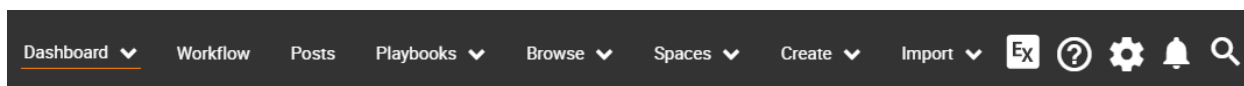


Figure 1

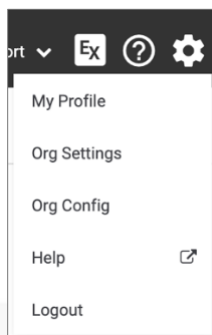


Figure 2



3. Select **Org Settings**, and the **Organization Settings** screen will be displayed with the **Membership** tab selected (Figure 3).

The screenshot shows the 'Demo Organization - Organization Settings' page with the 'Membership' tab selected. At the top right, there is a 'Demo Organization' dropdown menu. Below the navigation menu, there are four buttons: 'Create API User', 'Create TAXII User', 'Create User', and 'Create Read Only User'. Three informational boxes indicate remaining user limits: '5 more users can be created.', '1 more API user can be created.', and '3 more TAXII users can be created.'. A table lists user accounts with columns for Account, Name, System Role, Organization Role, Status, Last Login, and Options.

Account	Name	System Role	Organization Role	Status	Last Login	Options
9002283684460990288	Donna Noble	Api User	Standard User	OK		
66422015525627809171	Jack Harkness	Api User	Standard User	OK		
jsmith	John Smith	Operations Administrator	Organization Administrator	OK	06-04-2021 16:56 GMT	
apond	Amy Pond	Administrator	Organization Administrator	OK	06-04-2021 13:28 GMT	
rwilliams	Rory Williams	User	App Developer	OK	04-20-2021 15:14 GMT	
rytler	Rose Tyler	Administrator	Organization Administrator	OK	06-03-2021 17:04 GMT	

Figure 3

Membership

The **Membership** tab of the **Organization Settings** screen (Figure 3) displays all user accounts in the Organization. From this screen, Organization Administrators may create, edit, and delete users, including API Users, TAXII Users, and Read Only Users. The screen also displays the remaining number of users, API users, and TAXII users that can be created in the Organization.

NOTE: Users with a System role of Administrator, Operations Administrator, or Accounts Administrator can increase user limits. See [ThreatConnect System Roles and Permissions](#) for more information on System roles. See the [ThreatConnect Account Administration Guide](#) for instructions on increasing user limits in an Organization.

NOTE: The ability to create API users is determined by the terms of your ThreatConnect license. For more information, contact your Customer Success Manager.


NOTE: Users can enable two-step verification to increase the security of their ThreatConnect account via Google Authenticator™ or any other Time-based One-Time Password (TOTP)-compatible authentication service. An icon such as the Google Authenticator™ logo will be displayed in the Status column for such users. See [User Settings](#) for more information on enabling two-step verification.



Creating User Accounts

See [Creating User Accounts](#) for instructions on creating users, API users, and Read Only Users. See the “Creating a TAXII User” section of [Using the ThreatConnect TAXII Server](#) for instructions on creating TAXII users.

Editing User Accounts


From the **Membership** tab of the **Organization Settings** screen (Figure 3), click the pencil  icon in the **Options** column for the user to be edited. Depending on the type of user selected, the **API User Administration**, **TAXII User Administration**, or **User Administration** window will be displayed. For guidance on modifying the fields and options for each type of user accounts, see [Creating User Accounts](#) (for editing users and API users) and the “Creating a TAXII User” section of [Using the ThreatConnect TAXII Server](#) (for editing TAXII users).

NOTE: The Send Account Info Email checkbox in the User Administration window will not be displayed when editing a user. It is displayed only when creating a new user.

NOTE: When editing a user with a System role and Organization role of Read Only User, the only available Organization roles will be Read Only User and Read Only Commenter. To change the user's Organization role to any other value, change the System role of the user (e.g., to User) and click the SAVE button. Then edit the user again. The Organization Role dropdown menu will now display the rest of the Organization roles.

Deleting User Accounts

Follow these steps to delete a user account:

1. From the **Membership** tab of the **Organization Settings** screen (Figure 3), click the trash  icon in the **Options** column for the user to be deleted. The **User Deletion** window will be displayed (Figure 4).

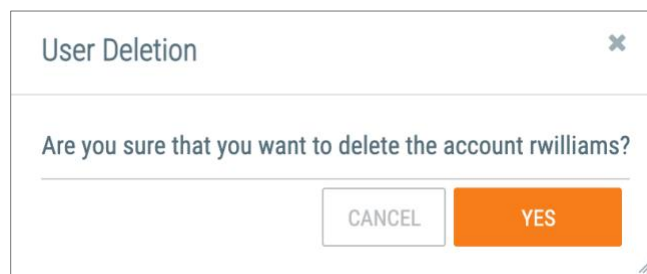


Figure 4

2. Click the **YES** button.



Communities/Sources

The **Communities/Sources** tab of the **Organization Settings** screen (Figure 5) displays the Organization's Community and Source memberships. From this screen, Organization Administrators can view and manage their Organization's membership in Communities and Sources and change their Organization's pseudonym.

Name	Type	Default Role	Anonymous	Joined	Options
A-Smoke-Source	Source	Director		03-26-2019	
Demo Community	Community	Director	Anonymous Profile	08-29-2018	
Demo Source	Source	Director		08-29-2018	
MITRE ATT&CK	Source	User		03-31-2021	
Sample Community	Community	Director	Anonymous Profile	08-29-2018	

Figure 5

View and Manage Community and Source Membership

The table on the **Communities/Sources** tab of the **Organization Settings** screen (Figure 5) displays an Organization's Community and Source memberships, providing the following information for each Community or Source:


- **Name:** This column displays the name of the Community or Source as a hyperlink that, when clicked on, displays the profile screen for the Community or Source. See the *ThreatConnect Community and Source Administration Guide* for more information.
- **Type:** This column indicates whether the object is a Community or a Source.
- **Default Role:** This column displays the default role of Organization members in the Community. See [ThreatConnect Owner Roles and Permissions](#) for more details on Community roles.

NOTE: User accounts with a Community role of Community Director may change the role of Organization members within a Community.

- **Anonymous:** This column displays "Anonymous Profile" if anonymous profiles are enabled for a Community. If anonymous profiles are not enabled (i.e., users' full profile information must be provided), the column is blank. See the *ThreatConnect Account Administration Guide* for more information on anonymous profiles.

NOTE: This column is always blank for Sources, even if they have an anonymous owner. Sources with anonymous owners act the same as Communities with anonymous profiles with respect to anonymous posting.




- **Joined:** This column provides the date on which the Organization joined the Community or Source.
- **Options:** Clicking on the trash  icon in this column provides the Organization Administrator with the option to have the Organization leave the Community or Source. This option will not be available for Communities and Sources owned by the Organization.

NOTE: This option will not be available to users whose owner role does not have permission to leave Communities and Sources. See [ThreatConnect Owner Roles and Permissions](#) for more information.

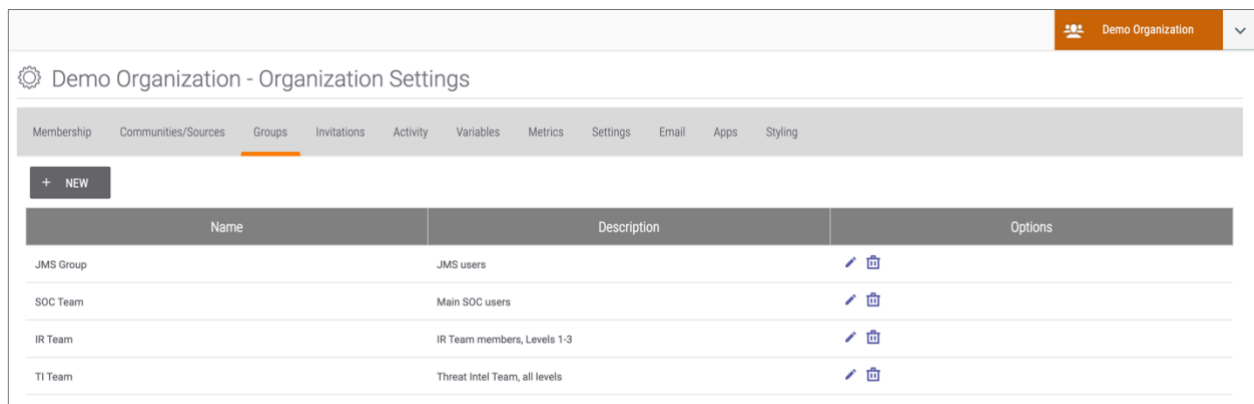
NOTE: This action does not delete a Community or Source. See the ThreatConnect Account Administration Guide for information on deleting owners.

Change Pseudonym

To change the pseudonym that an Organization uses in the Communities and Sources to which it belongs, click on the pencil  icon next to the current pseudonym, on the left side of the screen above the table (Figure 5).

Groups

The **Groups** tab of the **Organization Settings** screen (Figure 6) displays the Organization's user groups, which are teams of users to which [Workflow Cases](#) and [Workflow Tasks](#) may be assigned. From this screen, Organization Administrators can view and manage their Organization's groups and create new groups.











Name	Description	Options
JMS Group	JMS users	 
SOC Team	Main SOC users	 
IR Team	IR Team members, Levels 1-3	 
TI Team	Threat Intel Team, all levels	 

Figure 6

View and Manage Groups

The table on the **Groups** tab of the **Organization Settings** screen (Figure 6) provides the following information for each user group in the Organization:

- **Name:** This column displays the name of the user group.
- **Description:** This column displays a description of the user group.
- **Options:** This column provides options for editing and deleting the user group.



Create a New Group


Click the **+ NEW** button at the top left of the **Groups** tab (Figure 6) to create a new user group. The **Create Group** window will be displayed (Figure 7).

<input type="checkbox"/>	User	Name	Status	Last Login
<input type="checkbox"/>	abernard	Andy Bernard	Active	06-14-2021 21:25 GMT
<input type="checkbox"/>	adwyer	Andy Dwyer	Active	06-11-2021 18:50 GMT
<input type="checkbox"/>	aludgate	April Ludgate	Active	06-11-2021 17:03 GMT
<input type="checkbox"/>	aperkins	Ann Perkins	Active	06-14-2021 14:16 GMT
<input type="checkbox"/>	apond	Amy Pond	Active	06-03-2021 17:04 GMT

Figure 7

- **Name:** Enter a name for the group.
- **Description:** Enter a description for the group.
- **Display Only Group Members:** Leave this checkbox unselected when creating a new group. Its functionality—displaying only members of the group in the table—applies only when editing an existing group.
- Select the checkboxes next to the users to be added to the group. Use the **Filter** box to search for a user by name.
- Click the **SAVE** button.

Edit a Group

Click the pencil  icon in the **Options** column for the group to be edited. The **Edit Group** window for that group will be displayed (Figure 8).




<input type="checkbox"/>	User	Name	Status	Last Login
<input checked="" type="checkbox"/>	abernard	Andy Bernard	Active	06-14-2021 21:25 GMT
<input checked="" type="checkbox"/>	adwyer	Andy Dwyer	Active	06-11-2021 18:50 GMT
<input type="checkbox"/>	aludgate	April Ludgate	Active	06-11-2021 17:03 GMT
<input checked="" type="checkbox"/>	aperkins	Ann Perkins	Active	06-14-2021 14:16 GMT
<input type="checkbox"/>	apond	Amy Pond	Active	06-03-2021 17:04 GMT

Figure 8

- **Name:** Modify the name of the group, if desired.
- **Description:** Modify the description of the group, if desired.
- **Display Only Group Members:** Select this checkbox to display only members of the group.
- Add users to the group, or remove users from the group, as desired.
- Click the **SAVE** button.

Delete a Group

Click the trash  icon in the **Options** column for the group to be deleted. The **Delete User Group** window for that group will be displayed (Figure 9).

Are you sure that you want to delete SOC Team?

Figure 9

Click the **YES** button to delete the group.



Invitations

The **Invitations** tab of the **Organization Settings** screen (Figure 10) displays the Organization's pending invitations to Communities.

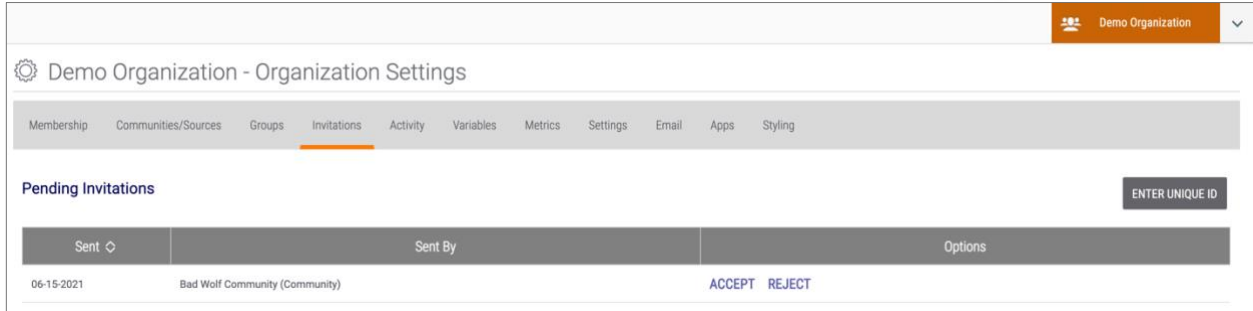


Figure 10

Invitations sent to an Organization Administrator's account will be displayed in the **Pending Invitations** table. The **Options** column provides options for accepting or rejecting an invitation. When accepting an invitation, the **Accept Invite** window will be displayed (Figure 11), explaining the Community's anonymity policy.

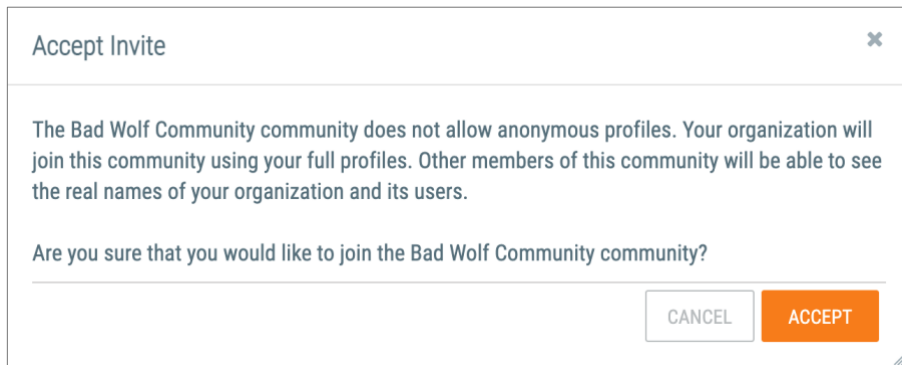


Figure 11

Click the **ACCEPT** button to join the Community.

Alternatively, click the **ENTER UNIQUE ID** button to use the invitation code from the email invitation. The **Accept Invite** window will be displayed (Figure 12).

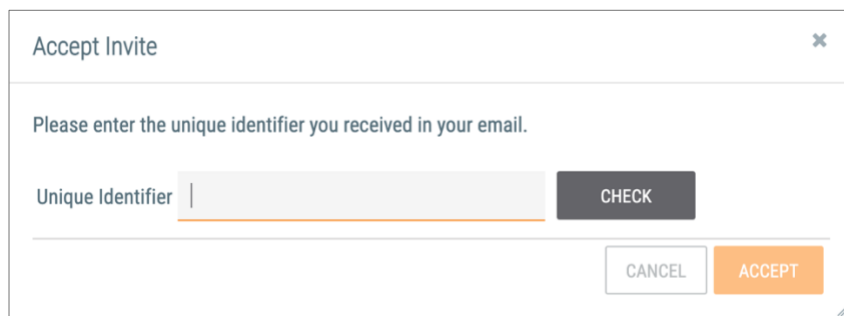
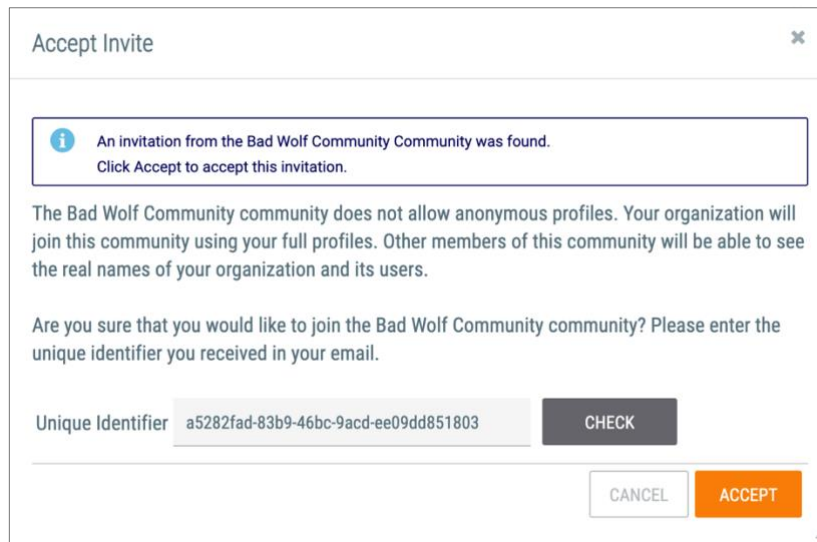


Figure 12



Enter the invitation code from the email in the **Unique Identifier** box, and then click the **CHECK** button. The **Accept Invite** window will confirm the invitation and display information about the Community's anonymity policy (Figure 13).



The dialog box titled "Accept Invite" contains the following information:

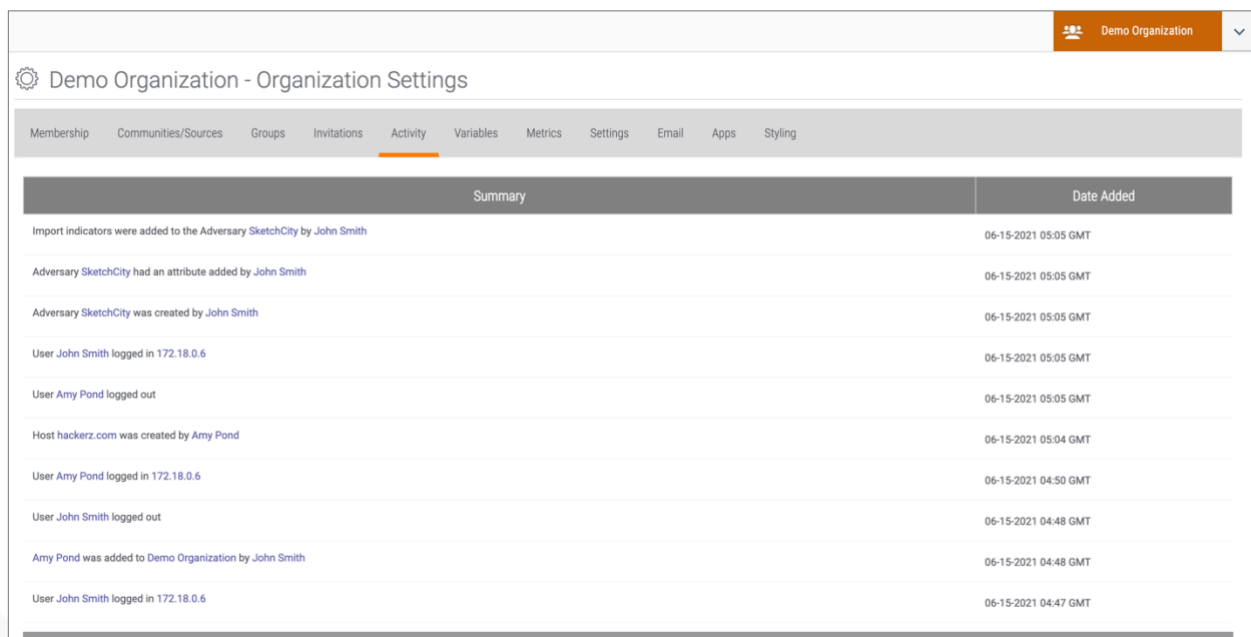
- An information icon followed by the text: "An invitation from the Bad Wolf Community Community was found. Click Accept to accept this invitation."
- A paragraph: "The Bad Wolf Community community does not allow anonymous profiles. Your organization will join this community using your full profiles. Other members of this community will be able to see the real names of your organization and its users."
- A question: "Are you sure that you would like to join the Bad Wolf Community community? Please enter the unique identifier you received in your email."
- A text input field labeled "Unique Identifier" containing the value "a5282fad-83b9-46bc-9acd-ee09dd851803".
- A "CHECK" button next to the input field.
- "CANCEL" and "ACCEPT" buttons at the bottom right.

Figure 13

Click the **ACCEPT** button to join the Community.

Activity

The **Activity** tab of the **Organization Settings** screen (Figure 14) displays a log of user activity in the Organization, including logins, logouts, creations, and deletions.



The screenshot shows the "Demo Organization - Organization Settings" page with the "Activity" tab selected. The activity log is as follows:

Summary	Date Added
Import indicators were added to the Adversary SketchCity by John Smith	06-15-2021 05:05 GMT
Adversary SketchCity had an attribute added by John Smith	06-15-2021 05:05 GMT
Adversary SketchCity was created by John Smith	06-15-2021 05:05 GMT
User John Smith logged in 172.18.0.6	06-15-2021 05:05 GMT
User Amy Pond logged out	06-15-2021 05:05 GMT
Host hackerz.com was created by Amy Pond	06-15-2021 05:04 GMT
User Amy Pond logged in 172.18.0.6	06-15-2021 04:50 GMT
User John Smith logged out	06-15-2021 04:48 GMT
Amy Pond was added to Demo Organization by John Smith	06-15-2021 04:48 GMT
User John Smith logged in 172.18.0.6	06-15-2021 04:47 GMT

Figure 14



Variables

The **Variables** tab of the **Organization Settings** screen (Figure 15) displays all variables in the Organization and allows Organization Administrators to create new variables. Variables can be preconfigured and used to populate certain fields, such as the ThreatConnect API Access ID or Secret Key, so that all users in the Organization can easily select them from a dropdown menu of possible variables rather than having to type out their values.

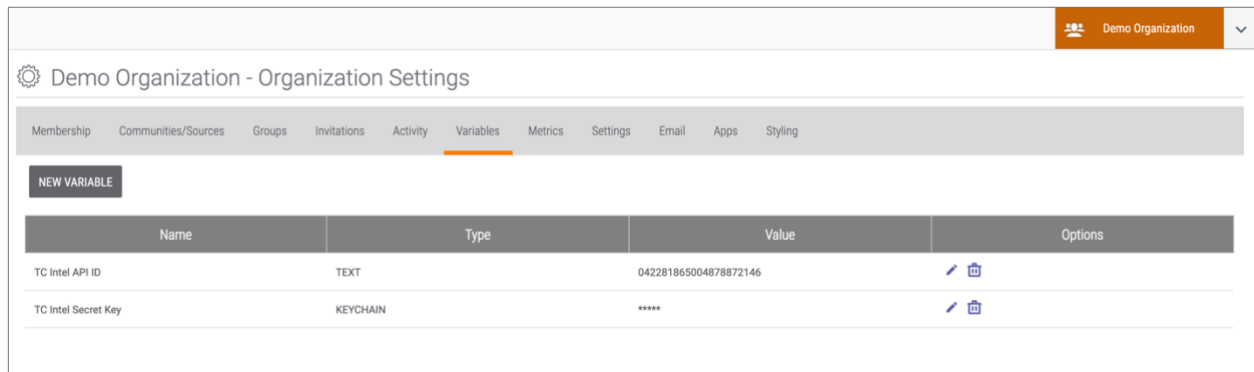


Figure 15

Add a Variable

Click the **NEW VARIABLE** button at the top left of the **Variables** tab (Figure 15), and the **Property** window will be displayed (Figure 16).

Property

Type
KEYCHAIN

Name

Value

CANCEL SAVE


Figure 16

- **Type:** Use the dropdown menu to select a variable type (**KEYCHAIN**, **TEXT**, or **FILE**). Keychain variables are used to store passwords and other secret data. Text variables are used to hold text values (e.g., user names, URLs). File variables are used to store files (e.g., certificates, private keys).
- **Name:** Enter a name for the variable.




- **Value:** Type in a value for a keychain or text variable. For a file variable, use the **+ SELECT FILE** button to browse to and select a file.
- Click the **SAVE** button.

Edit a Variable

Click the pencil  icon in the **Options** column for the variable to be edited. The **Property** window for that variable will be displayed (Figure 16). Modify as desired, and then click the **SAVE** button.

Delete a Variable

Click the trash  icon in the **Options** column for the variable to be deleted. The **Variable Deletion** window for that variable will be displayed (Figure 17).

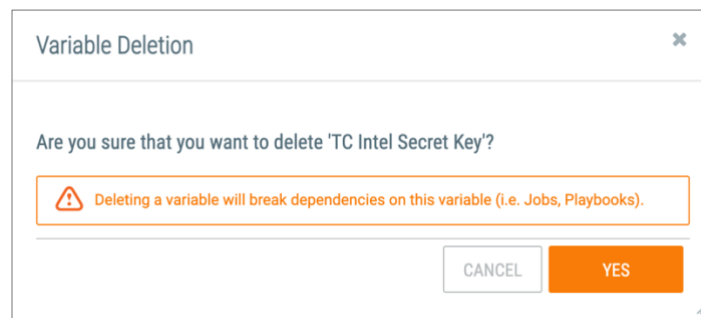


Figure 17

Click the **YES** button to delete the variable. Note that deleting a variable will break any dependencies on that variable, such as Jobs and Playbooks for which the variable has been selected as a parameter.

Metrics

The **Metrics** tab of the **Organization Settings** screen (Figure 18) displays the Organization's metrics, which allow users to track data not available through other functionalities. Metrics can be defined further as custom metrics through [API calls](#), allowing users to generate more specific data, such as the number of times a particular Playbook was run.

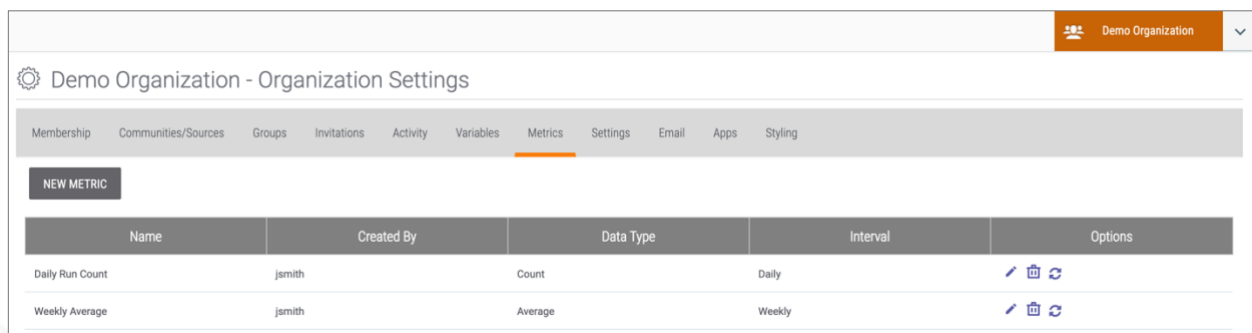



Figure 18




Create a Metric

See *Custom Metrics* for instructions on how to create metrics and define custom metrics.

Edit a Metric

Click the pencil  icon in the **Options** column for the metric to be edited. The **Configure Metric** window for that metric will be displayed. See *Custom Metrics* for more information.

Delete a Metric

Click the trash  icon in the **Options** column for the metric to be deleted. The **Delete Metric** window for that metric will be displayed (Figure 19).

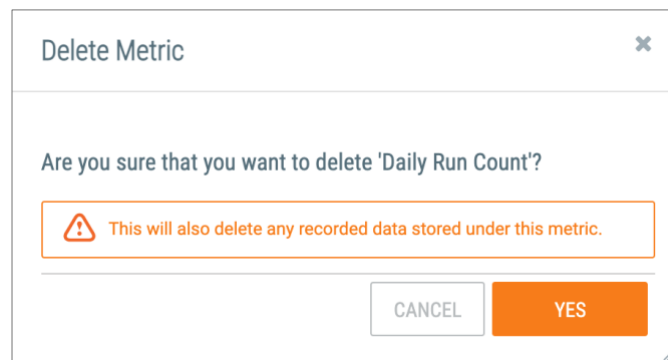



Figure 19

Click the **YES** button to delete the metric.

NOTE: Deleting a metric deletes all data stored under the metric.

Clear Metric Data

Click the clear metric  icon to clear all data stored under the metric. The **Clear Metric Data** window will be displayed (Figure 20).

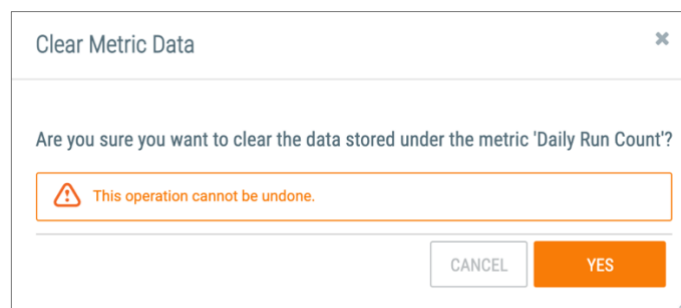


Figure 20

Click the **YES** button to clear the data stored under the metric. The metric itself will remain, but all of its data will be cleared.



Settings

The **Settings** tab of the **Organization Settings** screen (**Error! Reference source not found.**) allows Organization Administrators to enable the following settings: passive DNS (via a Farsight Security™ API key), Reverse Whois tracking (via a DomainTools API key), login IP filter, and Playbook IP filter.

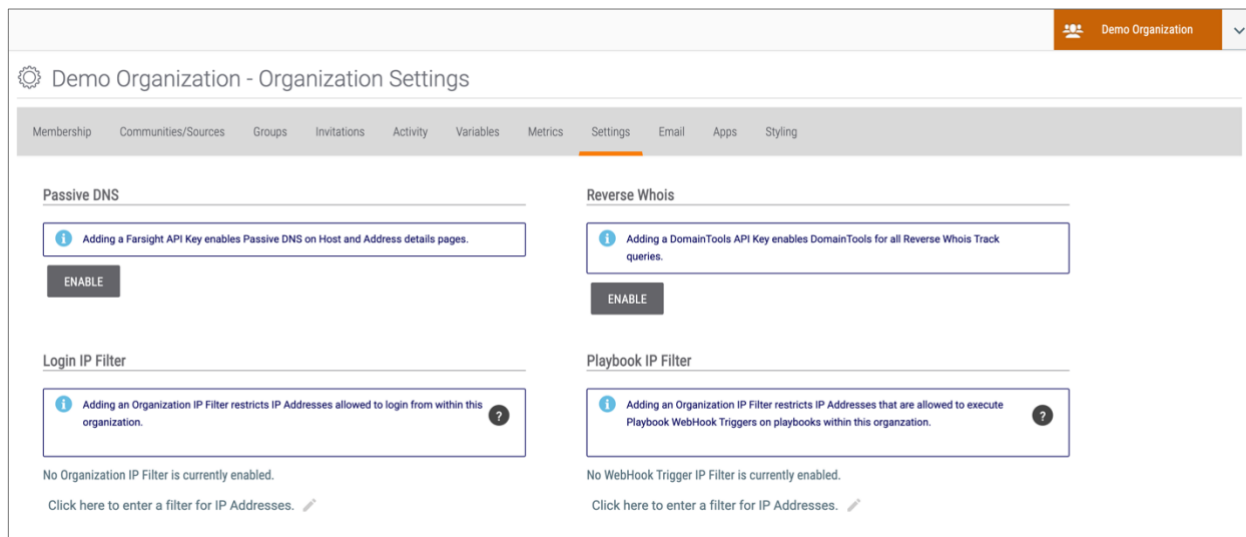


Figure 21

Passive DNS

Organizations with access to Farsight Security's passive DNS service may elect to enter an API key for that service in order to use that provider's data, as opposed to ThreatConnect's current provider's data, for Passive DNS lookups.

Enable Passive DNS

To enable the Farsight passive DNS service, click the **ENABLE** button on the **Reverse Whois** section of the **Settings** tab of the **Organization Settings** screen (Figure 21). The **Setup Farsight Passive DNS** window will be displayed (Figure 22).

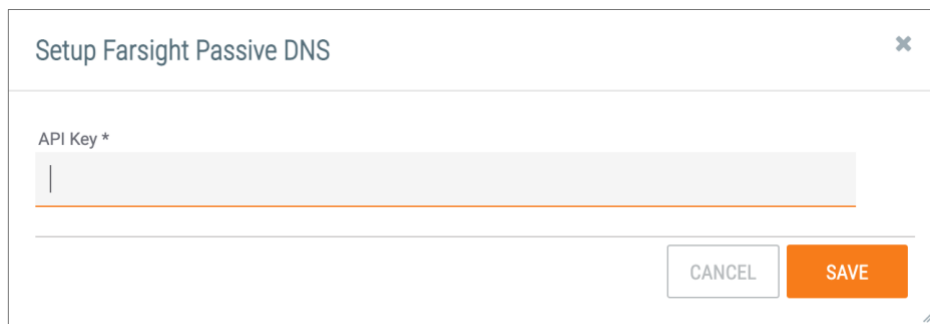


Figure 22



- **API Key:** Enter the Farsight passive DNS API key.
- Click the **SAVE** button.

The **Passive DNS** section will now show that a Farsight passive DNS API key has been enabled (Figure 23).

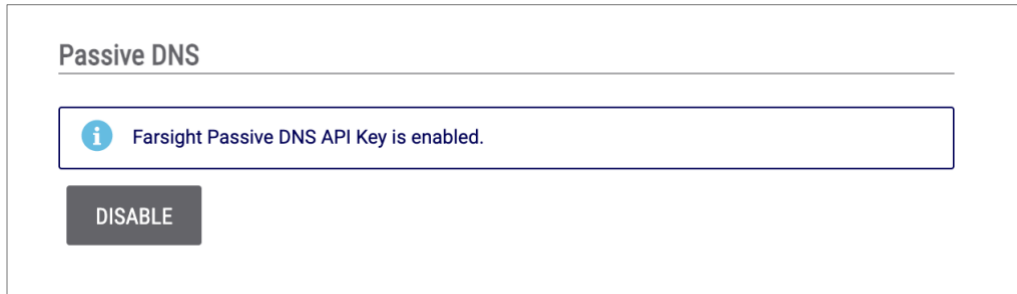


Figure 23

Disable Passive DNS

To disable the Farsight passive DNS service, click the **DISABLE** button on the **Passive DNS** section of the **Settings** tab of the **Organization Settings** screen (Figure 23). The **Remove API Key** window will be displayed (Figure 24).

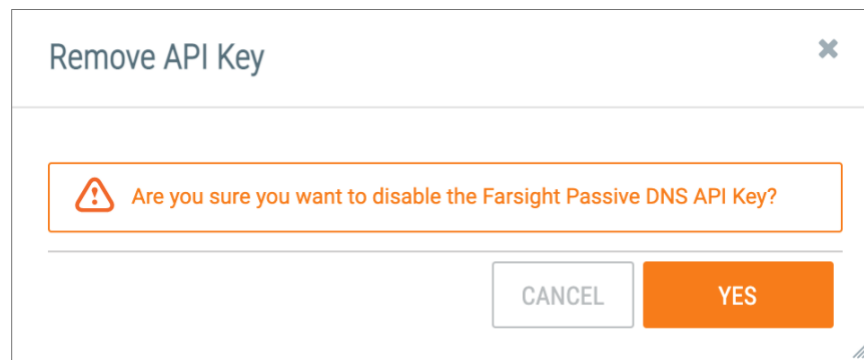


Figure 24

Click the **YES** button to disable the Farsight passive DNS API key.

Reverse Whois

Organization Administrators can enable Reverse Whois tracking by entering a DomainTools API key, allowing users to access and create [Tracks](#). Depending on the terms of the API key, users may be able to create and run an unlimited number of Tracks.



Enable Reverse Whois

To enable Reverse Whois tracking, click the **ENABLE** button on the **Reverse Whois** section of the **Settings** tab of the **Organization Settings** screen (Figure 21). The **Setup DomainTools** window will be displayed (Figure 25).

Setup DomainTools

User Name *

API Key *

CANCEL SAVE

Figure 25

- **User Name:** Enter the user name associated with the DomainTools API key.
- **API Key:** Enter the DomainTools API key.
- Click the **SAVE** button.

The **Reverse Whois** section will now show that a DomainTools API key has been enabled (Figure 26).

Reverse Whois

DomainTools API Key is enabled.

DISABLE

Figure 26

Disable Reverse Whois

To disable Reverse Whois tracking, click the **DISABLE** button on the **Reverse Whois** section of the **Settings** tab of the **Organization Settings** screen (Figure 26). The **Remove DomainTools API Key** window will be displayed (Figure 27).

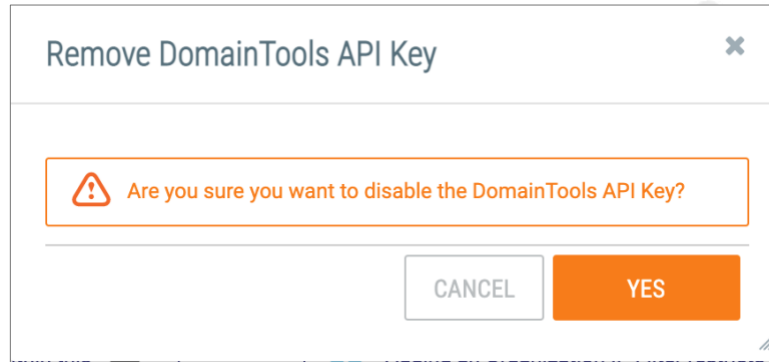



Figure 27

Click the **YES** button to disable the DomainTools API key.

Login IP Filter

Organization Administrators can use the login IP filter to limit logins to the Organization to a single IP address or a set of IP addresses, including IP address ranges.

To add IP addresses to the login IP filter, click the pencil  icon next to the **Click here to enter a filter for IP addresses** text on the **Login IP Filter** section of the **Settings** tab of the **Organization Settings** screen (Figure 21). A text box for entering IP addresses will be displayed (Figure 28).

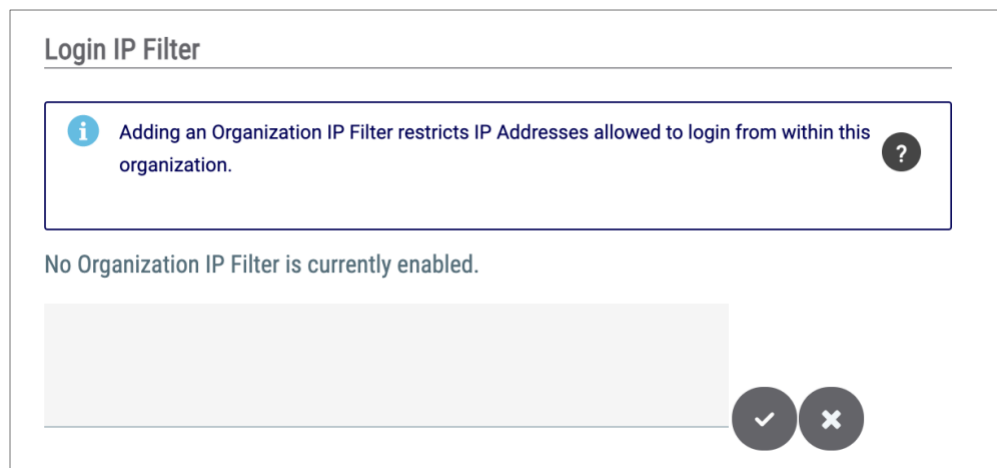


Figure 28

Enter one or more IP addresses that will be allowed to log into user accounts within the Organization. Separate multiple values with commas, and use a dash (-) to denote ranges (e.g., 192.168.1.8-192.168.1.12). Then click the checkmark icon to save the additions or changes. The **Login IP Filter** section will now show the address(es) to which Organization logins are restricted (Figure 29).

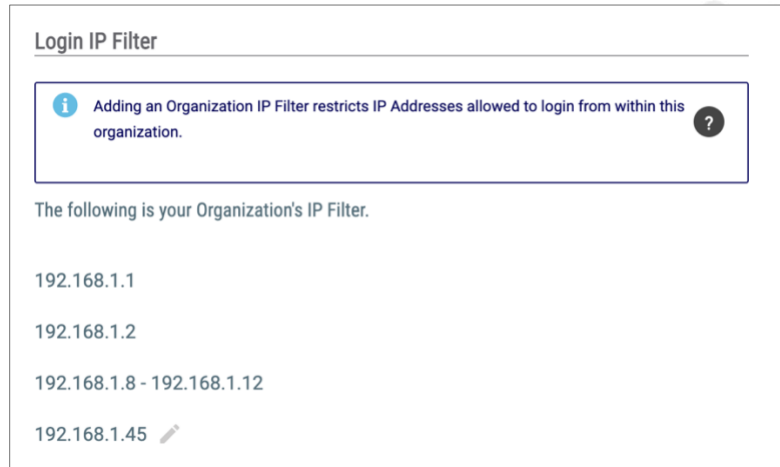



Figure 29

Playbook IP Filter

Organization Administrators can use the Playbook IP filter to specify the IP addresses that are allowed to send requests to [WebHook Triggers](#) in Playbooks.

To add IP addresses to the Playbook IP filter, click the pencil  icon next to the **Click here to enter a filter for IP addresses** text on the **Playbook IP Filter** section of the **Settings** tab of the **Organization Settings** screen (Figure 21). A text box for entering IP addresses will be displayed (Figure 30).

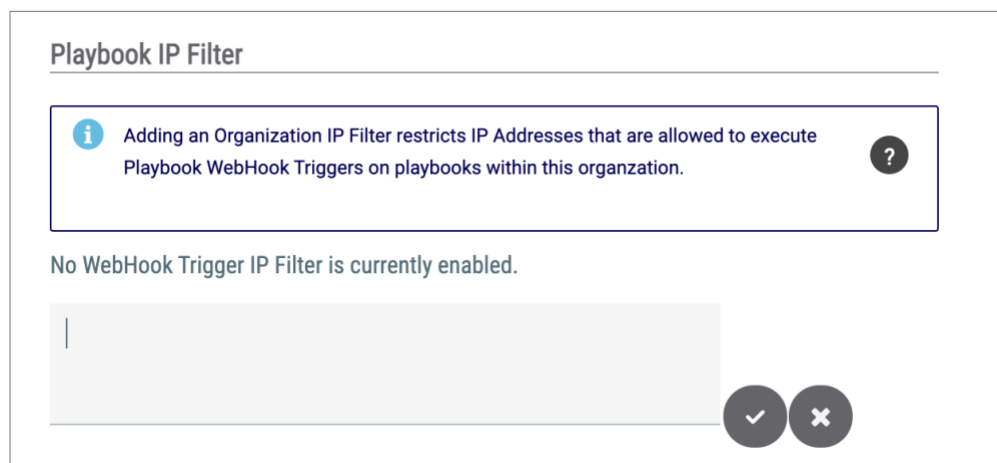


Figure 30

Enter one or more IP addresses that will be allowed to send requests to WebHook Triggers in Playbooks. Separate multiple values with commas, and use a dash (-) to denote ranges (e.g., 192.168.1.8-192.168.1.12). Then click the checkmark icon to save the additions or changes. The **Playbook IP Filter** section will now show the address(es) that are allowed to execute WebHook Triggers in Playbooks (Figure 31).



Playbook IP Filter

i Adding an Organization IP Filter restricts IP Addresses that are allowed to execute Playbook WebHook Triggers on playbooks within this organization. ?

The following is your Organization's WebHook Trigger IP Filter.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.8 - 192.168.1.12
- 192.168.1.45 ✎

Figure 31

NOTE: Users trying to execute a WebHook Trigger from IP addresses not on the filter list will receive an error message.

Email

The **Email** tab of the **Organization Settings** screen (Figure 32) allows Organization Administrators to configure email ingestion. Email ingestion allows users to send cyberthreat-related emails to ThreatConnect, where they will be parsed and imported for further analysis. Emails are ingested via phishing mailboxes and feed mailboxes.

Demo Organization

Demo Organization - Organization Settings

Membership
Communities/Sources
Groups
Invitations
Activity
Variables
Metrics
Settings
Email
Apps
Styling

Create Phishing Mailbox
Create Feed Mailbox

Type	Address	Description	Parse Type	Score Threshold	Default Threat Rating	Default Confidence Rating	Options
Feed	ovmpodzmy@app.threatconnect.com	Code Purple Threats	Body	N/A	3	85	✎ 🗑
Phishing	zirkqbtkyn@app.threatconnect.com	Level 5 Threat Phishing Mailbox	Body	70	N/A	N/A	✎ 🗑

Figure 32

View and Manage Mailboxes

The table on the **Email** tab of the **Organization Settings** screen (Figure 32) provides the following information for the phishing and feed mailboxes used by the Organization:

- **Type:** This column displays the type of mailbox: phishing or feed.
- **Address:** This column displays the email address of the mailbox.
- **Description:** This column displays a description of the mailbox.



- **Parse Type:** This column indicates whether the mailbox receives emails directly from network devices as **.eml** files (**Body**) or as email headers in the form of **.msg** attachments (**Attachment**).
NOTE: Only phishing mailboxes can parse attachments. This column will always display a value of Body for feed mailboxes.
- **Score Threshold:** This column displays the minimum score that an email must meet in order to be processed by a phishing mailbox. See [Email Import](#) for more information about email scoring.
NOTE: This column applies only to phishing mailboxes.
- **Default Threat Rating:** This column displays the default Threat Rating the mailbox applies to ingested Indicators.
NOTE: This column applies only to feed mailboxes.
- **Default Confidence Rating:** This column displays the default Confidence Rating the mailbox applies to ingested Indicators.
NOTE: This column applies only to feed mailboxes.
- **Options:** This column provides options for editing and deleting the mailbox.

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 Organization Administrator specifies whether 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 Group object containing the email's header and body;
- create a Task Group object signaling that the email is ready for additional processing;
- link previously existing Indicators to the Email Group, if they are found in the email header or body;
- link previously existing Victim email addresses to the Email Group, if they are found in the header.

Create Phishing Mailbox


To create a new phishing mailbox, click the **Create Phishing Mailbox** button at the top left of the table on the **Email** tab of the **Organization Settings** screen (Figure 32), and follow the steps in [Creating a Phishing Mailbox](#).



Edit Phishing Mailbox

Click the pencil  icon in the **Options** column for the phishing mailbox to be edited. The **Phishing Mailbox Administration** window for that mailbox will be displayed. See [Creating a Phishing Mailbox](#) for more information.

Delete Phishing Mailbox

Click the trash  icon in the **Options** column for the phishing mailbox to be deleted. The **Mailbox Deletion** window for that phishing mailbox will be displayed (Figure 33).

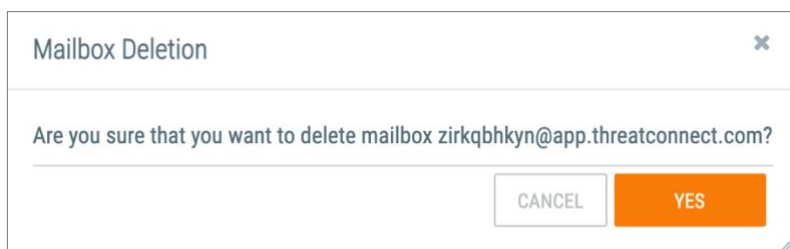


Figure 33

Click the **YES** button to delete the phishing mailbox.

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 a feed mailbox have only their bodies parsed for Indicators. When the parsing is complete, ThreatConnect will do the following:

- create a Document Group object from the email's body;
- create any Indicators that matched the pre-defined feed mailbox regular expressions;
- associate the Indicators with the Document.

Create Feed Mailbox

To create a new feed mailbox, click the **Create Feed Mailbox** button at the top left of the table on the **Email** tab of the **Organization Settings** screen (Figure 32). The **Feed Mailbox Administration** window will be displayed, with the **Mailbox** tab highlighted (Figure 34).



Feed Mailbox Administration

Mailbox Indicator Confirm

Target Mailbox: jmwpxdnwt @app.threatconnect.com

Default Threat Rating

Default Confidence Rating

Description

Tags (comma separated)

> Next

CANCEL SAVE

Note: Message body will be parsed for selected indicators.

Figure 34

- **Target Mailbox:** Click on the pencil icon to modify the name of the feed mailbox if desired.
- **Default Threat Rating:** To provide a default Threat Rating for ingested Indicators, select the **Default Threat Rating** checkbox. Five skulls will be displayed under the checkbox. Select the number of skulls representing the default Threat Rating.
- **Default Confidence Rating:** To provide a default Confidence Rating for ingested Indicators, select the **Default Confidence Rating** checkbox. A text box will be displayed to the right of the checkbox. Enter the default Confidence Rating or click the + and – signs to add and subtract increments of 1, respectively.
- **Description:** Enter a description for the feed mailbox.
- **Tags:** Enter Tags to be applied to ingested Indicators.

Click the **Next** button, and the **Indicator** tab will be displayed (Figure 35).



Figure 35

- **Indicator Selector:** Use the dropdown menu at the top left to select an Indicator type (Host, Address, E-mail Address, File, URL, ASN, CIDR, and any available custom Indicator types) for which to configure ingestion via the feed mailbox. All Indicator types may be configured, and selections made on the screen for one Indicator type will persist when another Indicator type is selected.
- **?** : Hover over the **?** icon at the top right to view explanations and examples that help define the criteria for each Indicator type.
- **Enable:** The **Enable** checkbox will display the selected Indicator type (e.g., **Enable Host**, **Enable Address**). Select the checkbox to enable the Indicator type for ingestion. Once an Indicator is enabled, the other fields in the window will become available for configuration.
- **Use System Import Rules:** Select this checkbox to use the standard import rules run by the system to import the Indicator. Selecting this checkbox disables the **Regex**, **De-Sanitize Regex**, and **De-Sanitize Replace Regex** fields.
- **Activate DNS:** Select this checkbox to activate DNS resolution tracking for a Host Indicator. This box is displayed only when configuring the Host Indicator type.
- **Activate Whois:** Select this checkbox to activate Whois lookups for a Host Indicator. This box is displayed only when configuring the Host Indicator type.
- **Regex:** Enter a regular expression (regex) to run against text in the email. The regex should handle sanitized Indicators.
- **Populate with example:** Click this text to populate the **Regex**, **De-Sanitize Find Regex**, and **De-Sanitize Replace Regex** fields with the example provided by the **?** icon.



- **De-Sanitize Find Regex:** Enter the regex to find the sanitized Indicator text. This field is optional.
- **De-Sanitize Replace Regex:** Enter the regex to replace the sanitized Indicator text. This field is optional.

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 will be displayed, showing a summary of the configuration (Figure 36).

Regex Type	Enabled	Using
Host Regex	Yes	System Import Regex
Address Regex	Yes	Custom Regex
Email Address Regex	Yes	System Import Regex
URL Regex	Yes	System Import Regex
File Regex	No	
ASN Regex	No	
CIDR Regex	Yes	Custom Regex


Figure 36

Click the **SAVE** button.

Edit Feed Mailbox

Click the pencil  icon in the **Options** column for the feed mailbox to be edited. The **Feed Mailbox Administration** window for that mailbox will be displayed. See the “Create Feed Mailbox” section for more information.

Delete Feed Mailbox

Click the trash  icon in the **Options** column for the feed mailbox to be deleted. The **Mailbox Deletion** window for that feed mailbox will be displayed (Figure 37).

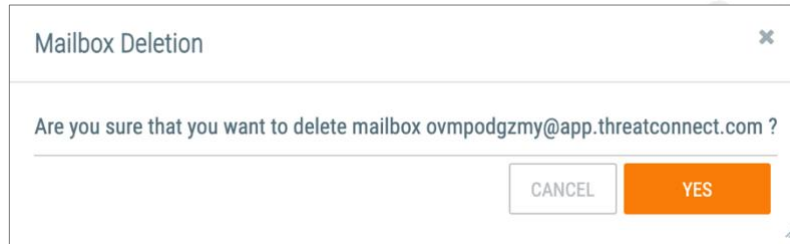


Figure 37

Click the **YES** button to delete the feed mailbox.

Apps

The **Apps** tab of the **Organization Settings** screen (Figure 38) allows Organization Administrators to administrate and run Job Apps, generate an App Delivery Token, view available Playbook Environments, generate a Developer Token, and administrate App Profiles.

Demo Organization - Organization Settings

Membership Communities/Sources Groups Invitations Activity Variables Metrics Settings Email **Apps** Styling

Jobs

Search... Clear

Job Name	Start Time	Last Execution	Next Execution	Active	
BAE Threat Intelligence v2	06-16-2021 00:00 GMT	Completed	06-17-2021 00:00 GMT	<input checked="" type="checkbox"/>	⊙ ✎ ⋮
BAE Threat Intelligence v2 (Deactivated by Feed Deployer)	05-21-2021 00:00 GMT	Completed	Off	<input type="checkbox"/>	⊙ ✎ ⋮
BAE Threat Intelligence v2 (Deactivated by Feed Deployer)	05-19-2021 00:00 GMT	Completed	Off	<input type="checkbox"/>	⊙ ✎ ⋮
OSINT Feed - Bambenek v1	06-16-2021 03:00 GMT	Completed	06-17-2021 03:00 GMT	<input checked="" type="checkbox"/>	⊙ ✎ ⋮
OSINT Feed - Blocklist.de Apache IPs v1	06-16-2021 04:00 GMT	Completed	06-17-2021 04:00 GMT	<input checked="" type="checkbox"/>	⊙ ✎ ⋮
OSINT Feed - Blocklist.de Bot IPs v1	06-16-2021 05:00 GMT	Completed	06-17-2021 05:00 GMT	<input checked="" type="checkbox"/>	⊙ ✎ ⋮
OSINT Feed - Blocklist.de Bruteforce IPs v1	06-16-2021 06:00 GMT	Completed	06-17-2021 06:00 GMT	<input checked="" type="checkbox"/>	⊙ ✎ ⋮
OSINT Feed - Blocklist.de FTP IPs v1	06-16-2021 07:00 GMT	Completed	06-17-2021 07:00 GMT	<input checked="" type="checkbox"/>	⊙ ✎ ⋮
Technical Blogs and Reports v1	06-16-2021 00:00 GMT	Completed	06-17-2021 00:00 GMT	<input checked="" type="checkbox"/>	⊙ ✎ ⋮

Figure 38

The **Apps** tab displays the **Jobs** view by default, but can be toggled to **Environments** and **Profiles** views as well.

Jobs


ThreatConnect is integrated with many third-party applications and services. ThreatConnect users may employ these product integrations as Apps via TC Exchange™ to further augment their analytic capabilities. Apps with feeds use [the Feed Deployer](#) to create Sources, which then run associated jobs.

When in **Jobs** view, the **Apps** tab of the **Organization Settings** screen displays a table with the following information about all jobs that are configured in the Organization (Figure 38):




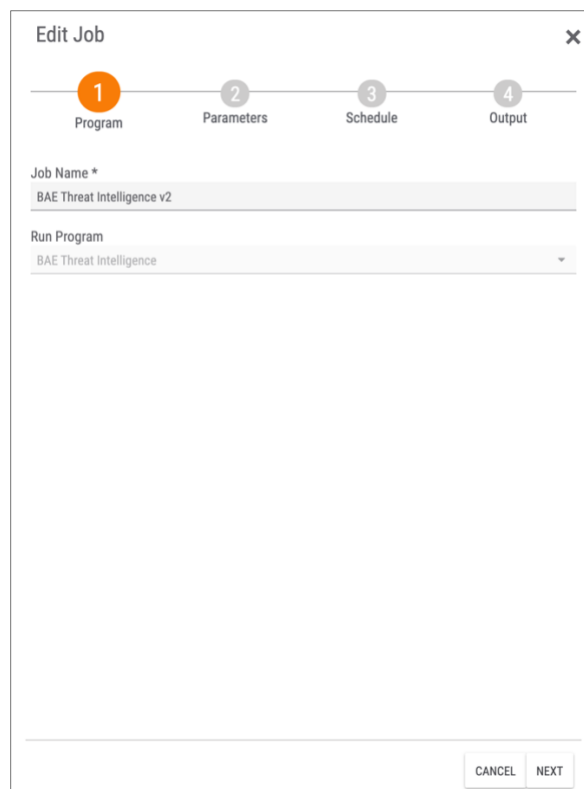
- **Job Name:** This column displays the name the job was given when it was added.
- **Start Time:** This column displays the time the most recent execution was started.
- **Last Execution:** This column displays the status of the most recent execution.
- **Next Execution:** This column displays the time of the next execution that is scheduled.
- **Active:** This column indicates whether the job is active or not and allows Organization Administrators to activate or deactivate it.

Create Job

Click the  button at the top right of the **Jobs** table to create a new job. See [Creating Jobs Using TC Exchange Apps](#) for further instruction.

Edit Job

Click the pencil  icon for a job on the right-hand side of the **Jobs** table to edit that job. The **Edit Job** drawer will be displayed (Figure 39).




The screenshot shows a modal window titled "Edit Job" with a close button (X) in the top right corner. At the top, there is a progress bar with four steps: 1. Program (highlighted in orange), 2. Parameters, 3. Schedule, and 4. Output. Below the progress bar, there is a "Job Name *" field with the value "BAE Threat Intelligence v2". Below that is a "Run Program" dropdown menu with the value "BAE Threat Intelligence". At the bottom right, there are "CANCEL" and "NEXT" buttons.

Figure 39

See [Creating Jobs Using TC Exchange Apps](#) for information on each screen.




Run Job

Click the **Run Job**  icon for a job on the right-hand side of the **Jobs** table to start a job on demand.

NOTE: *Jobs that may not be run on demand will not have this option enabled.*

Import Job

Click the **Import Job**  icon at the top right of the **Jobs** table to import a job file. The **Add Job** drawer will be displayed (Figure 40).

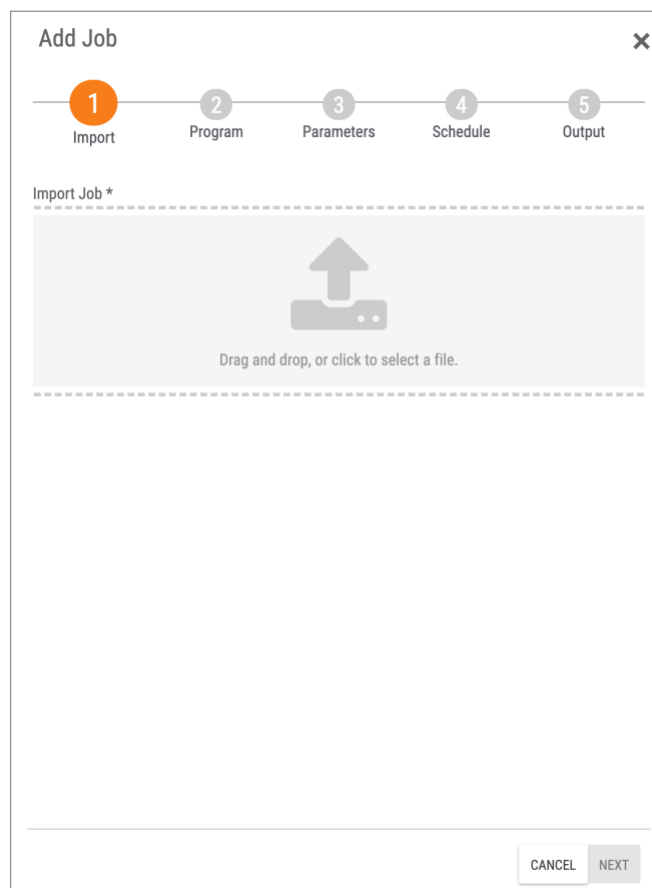


Figure 40

Drag and drop a Job file (**.json**) into the gray rectangle, or click the gray **Import** symbol in the middle of the screen in order to navigate to a directory from which to select a file.


Click the **NEXT** button, and navigate through the remaining screens following the instructions in [Creating Jobs Using TC Exchange Apps](#).



Refresh Jobs

Click the Refresh  icon at the top right of the **Jobs** table to reload the table.

Options Menu

Click on the vertical ellipsis  icon for a job on the right-hand side of the **Jobs** table to view a menu with a set of options for the job (Figure 41).

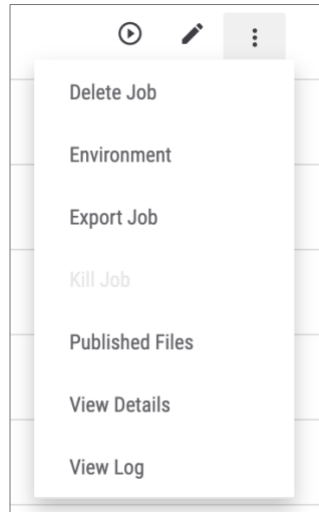



Figure 41

- **Delete Job:** Select this option to delete the job. A window will be displayed asking for confirmation.
- **Environment:** Select this option to choose an Environment Server on which to run the job remotely. See [Playbook Environments](#) for more information on Environment Servers.
- **Export Job:** Select to this option to download a `.json` file containing the job.
- **Kill Job:** Select this option to stop an ongoing run of the job.
- **Published Files:** Select this option to generate files that can be consumed by third-party services. The job must be configured for file generation.
- **View Details:** Select this option to view a drawer showing the last execution details for the job, including the name of the job, the name of the app, peak memory usage, peak CPU usage, queued date, start date, completed date, session id, server information, and exit message.
- **View Log:** Select this option to view run logs for the job.

NOTE: *Not all of these options will be available for every job.*

App Delivery

To generate an app delivery token, click the vertical ellipsis  menu at the top right and select **App Delivery** from the dropdown menu (Figure 42).

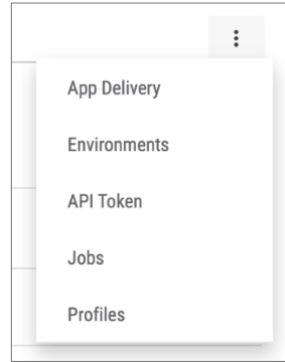


Figure 42

The current app delivery token will be provided (Figure 43).

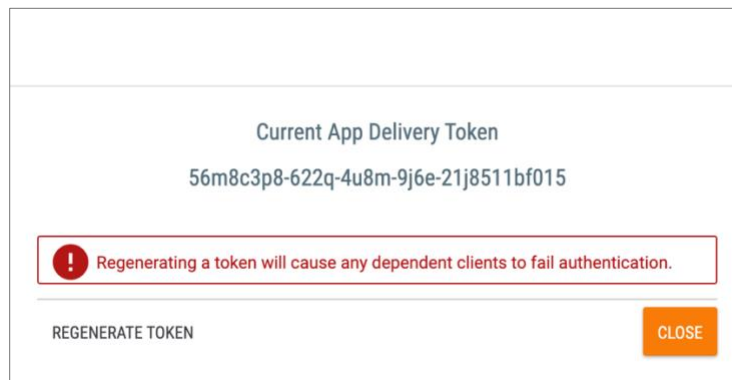


Figure 43

Click **REGENERATE TOKEN** to regenerate the token, but note that doing so will cause dependent clients to fail authentication.

Environments

To view all Environments available on the ThreatConnect instance, select the **Environments** option from the vertical ellipsis ⋮ menu (Figure 42). The screen will show all available Environments (Figure 44).

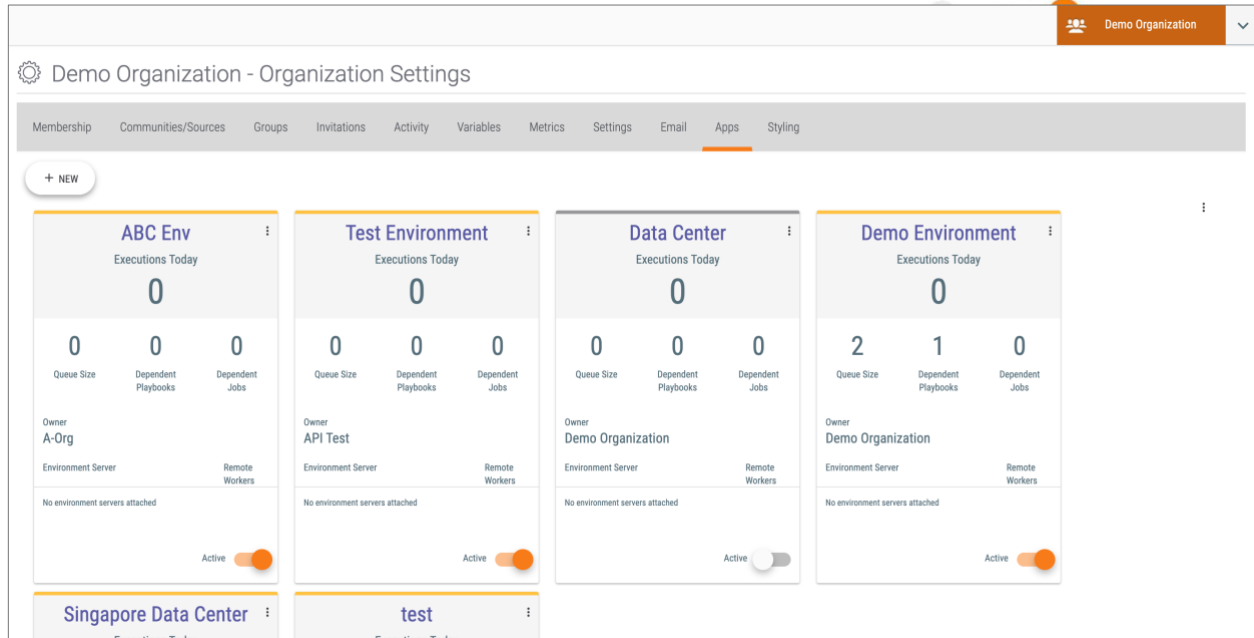


Figure 44

See [Playbook Environments](#) for more information.

API Token

To generate a temporary API token that developers can use to build Spaces, job, or Playbook Apps, select the **API Token** option from the vertical ellipsis ⋮ menu (Figure 42). The **Get Developer Token** window will be displayed (Figure 45).



Figure 45

Click the copy  icon to copy the token to the clipboard.

Profiles

A profile serves as a proxy for an App, and users interact directly with the profiled version of the installed App. Decoupling an app from a configuration profile allows Organization Administrators to configure multiple profiles of an app and, subsequently, give permissions to different users based on that profile. Moreover, this added level of abstraction allows the same app to be




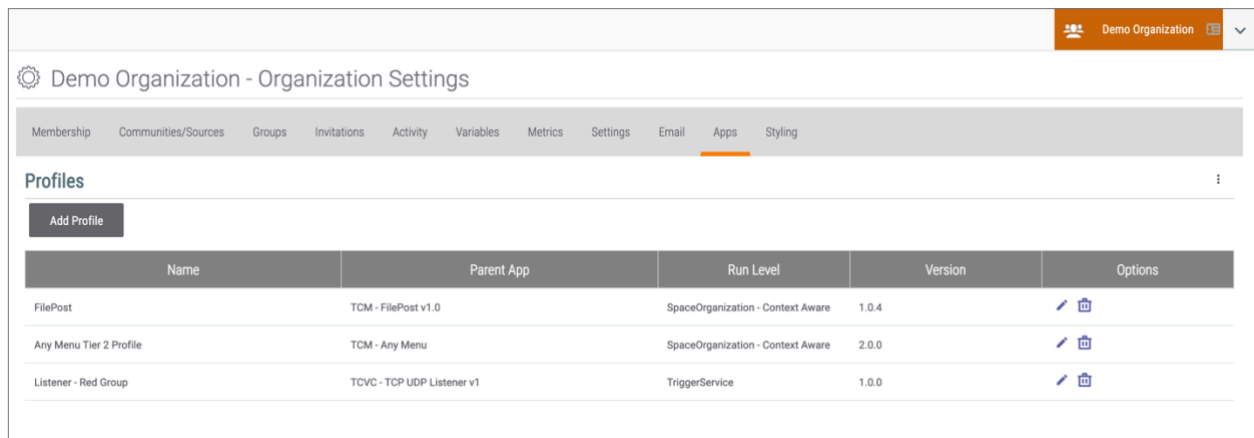
configured to work slightly differently at installation. App profiles allow administrators to customize installed apps in the following ways:

- set default parameter values for an app
- assign privileges to different profiles for the same app;
- define setup parameters required by an app.

App profiles are also necessary for configuring menu spaces, which are Apps listed in the **Spaces** menu on the top navigation bar. See the “Menu Spaces” section of [Spaces](#) for more information.

View App Profiles

To view all app profiles available in the Organization, select the **Profiles** option from the vertical ellipsis  menu (Figure 42). The screen will show all available app profiles (Figure 46).









Name	Parent App	Run Level	Version	Options
FilePost	TCM - FilePost v1.0	SpaceOrganization - Context Aware	1.0.4	 
Any Menu Tier 2 Profile	TCM - Any Menu	SpaceOrganization - Context Aware	2.0.0	 
Listener - Red Group	TCVC - TCP UDP Listener v1	TriggerService	1.0.0	 

Figure 46

The **Profiles** table displays the following information about the app profiles that are configured in the Organization:


- **Name:** This column displays the name the profile was given when it was added.
- **Parent App:** This column displays the name of the App selected for the profile.
- **Run Level:** This column displays the type of App selected for the profile.
- **Version:** This column displays the version of the App selected for the profile.
- **Options:** This column provides options for editing and deleting the app profile.

Add App Profiles

Click the **Add Profile** button at the top left of the **Profiles** table to create a new app profile. See [Adding App Profiles](#) for further instruction.



Edit App Profile

Click the pencil  icon for a profile on the right-hand side of the **Profiles** table to edit that profile. The **App Profile** window will be displayed. See [Adding App Profiles](#) for information on this window.

Delete App Profile

Click the trash  icon for a profile on the right-hand side of the **Profiles** table to delete that profile.

Styling

The **Styling** tab of the **Organization Settings** screen (Figure 47) allows Organization Administrators to upload a custom header and add disclaimer text for the top and bottom, respectively, of [report PDFs](#) downloaded from Groups.

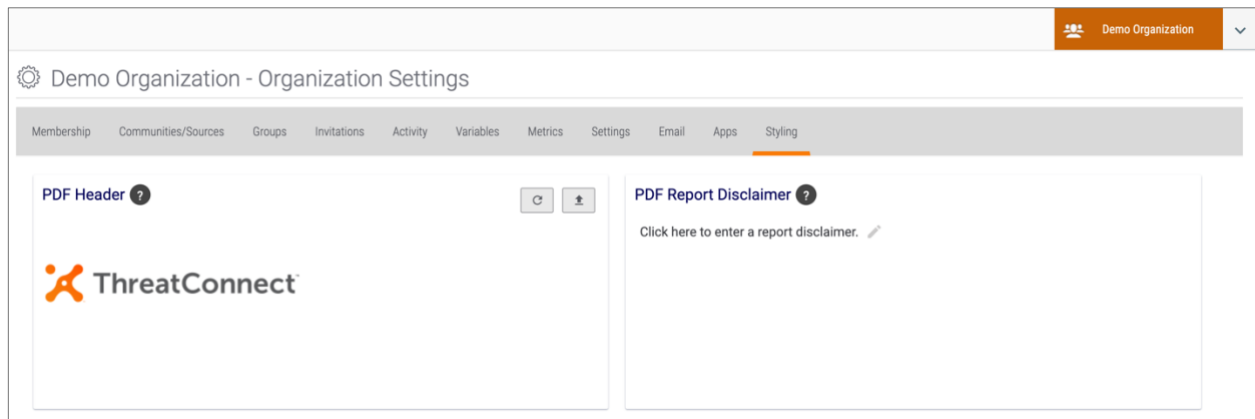


Figure 47

PDF Header



Click the **Upload**  icon at the top right of the **PDF Header** card, navigate to a directory, and select a JPEG or PNG image file. The new header image will be displayed in the **PDF Header** card (Figure 48).




Figure 48



NOTE: Hover over the question mark icon to view information on the maximum dimensions and size for the file.

To reset the header image back to the default ThreatConnect header, click the **Reset**  icon at the top right of the card.

PDF Report Disclaimer

Click the pencil  icon in the **PDF Report Disclaimer** card. A text box will be displayed (Figure 49).

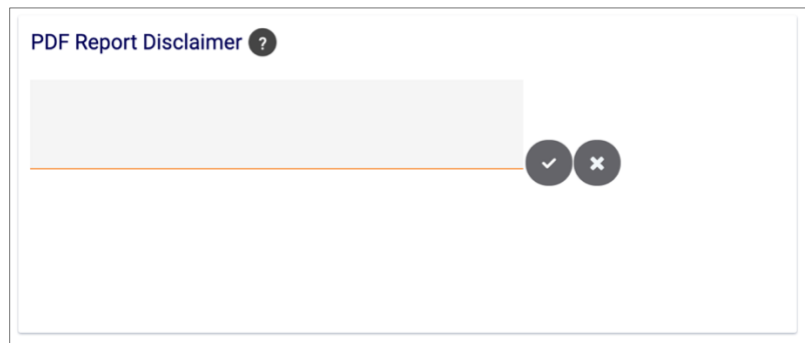



Figure 49

Enter the disclaimer text in the text box, and then click the checkmark  icon to accept it. The text will be displayed in the **PDF Report Disclaimer** card (Figure 50).

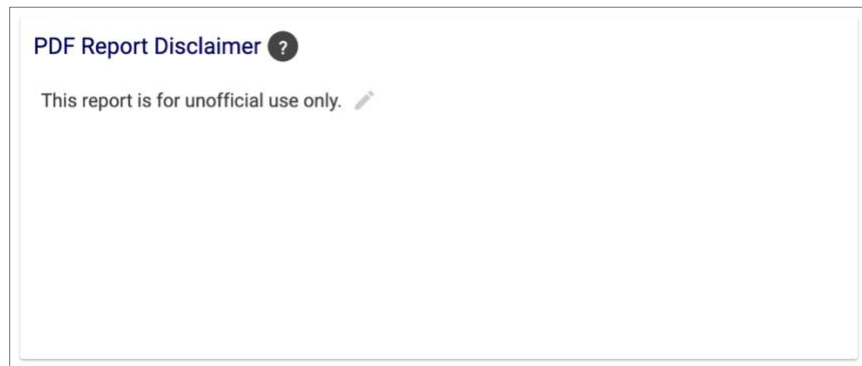



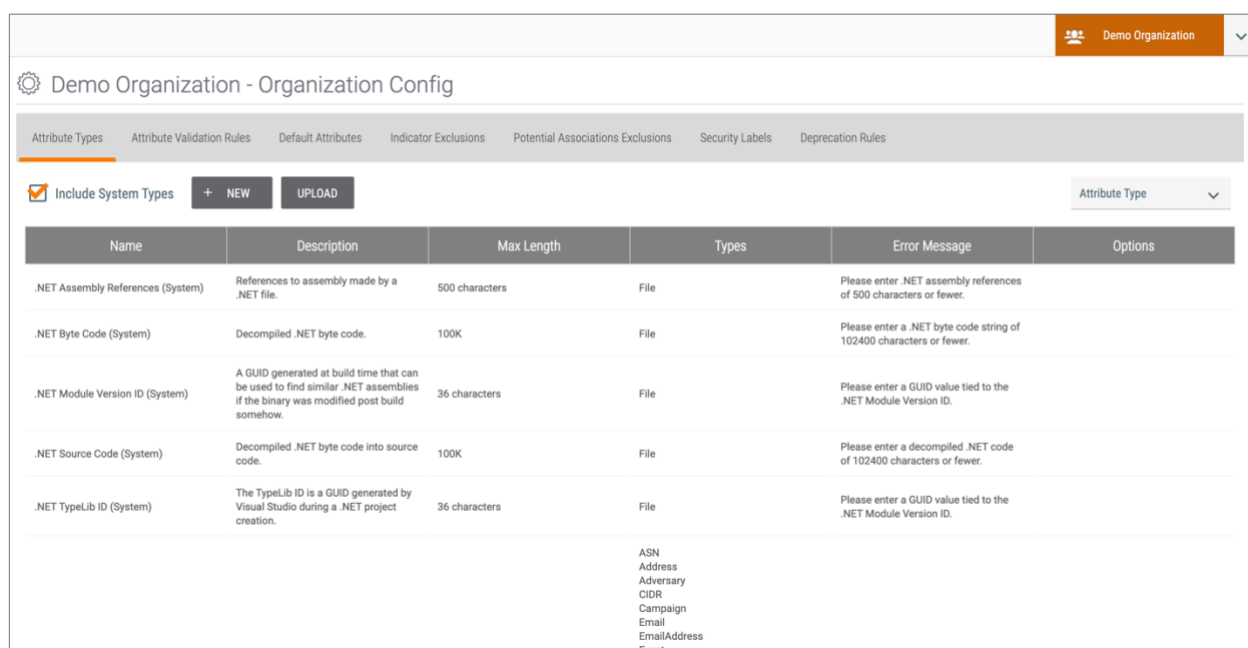
Figure 50



The Organization Config Screen

The **Organization Config** screen provides a tabbed interface where Organization Administrators can customize how data in their Organization are labeled and acted upon. Follow these steps to view the **Organization Config** screen:

1. Log in with an Organization Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon, and the **Settings** menu will be displayed (Figure 2).
3. Select **Org Config**, and the **Organization Config** screen will be displayed with the **Attribute Types** tab selected (Figure 51).



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.	

Figure 51

Attribute Types

Attributes are key/value sets that can be added to any Indicator or Group. The **Attribute Types** tab of the **Organization Config** screen (**Error! Reference source not found.**) displays the Attribute Types available to all Organizations on the ThreatConnect instance (that is, the System Attribute Types; see the *ThreatConnect System Administration Guide* for more information), as well as the Attribute Types specific to the Organization (i.e., custom Attribute Types).

View Attribute Types

The **Attribute Types** table displays the following information about the Attribute Types available to the Organization:

- **Name:** This column displays the name of the Attribute Type.
- **Description:** This column displays a description of the Attribute Type.



- **Max Length:** This column displays the maximum size of the value of the Attribute Type, in characters.
- **Types:** This column displays the object type(s) (Indicators, Groups, and Victim) to which the Attribute Type can be added.
- **Error Message:** This column provides the error message that will be presented to users if an incorrect value is entered.
- **Options:** This column provides options for editing and deleting the Attribute Type. These options are available only to custom Attribute Types.

To view only custom Attribute Types, clear the **Include System Types** checkbox (Figure 52).

Demo Organization - Organization Config

Attribute Types | Attribute Validation Rules | Default Attributes | Indicator Exclusions | Potential Associations Exclusions | Security Labels | Deprecation Rules

Include System Types + NEW UPLOAD Attribute Type

Name	Description	Max Length	Types	Error Message	Options
Org Attribute Type - MOB Test (Old)	My second description	100 characters	Address Adversary Campaign Document Email EmailAddress File Host Incident Signature Uri	Enter a valid value.	

Figure 52

To filter the table to display only Attribute Types that apply to a particular object type, select the object type from the **Attribute Type** dropdown menu at the top right of the table. Only one object type may be selected at a time. To reset the table to display all Attribute Types, select **Attribute Type**.

Create Attribute Type

Click the **+ NEW** button at the top left of the **Attribute Types** table to create a new custom Attribute Type for the Organization. See [Creating Custom Attribute Types](#) for further instruction.

Figure 53 shows an example of a custom Attribute Type that uses the **Country** Validation Rule to track the suspected nationalities of those responsible for the specified types of Groups and Indicators.



Figure 53

Upload Attribute Type

Custom Attribute Types can be added in bulk by uploading a comma-separated value (CSV) file. To do so, click the **UPLOAD** button at the top left of the **Attribute Types** table. The **Upload Attributes** window will be displayed (Figure 54).

Figure 54

Click the **+ SELECT FILE** button, navigate to the desired directory, select a file, and click the **SAVE** button. The Attribute Types will be displayed in the **Attribute Types** table.



Attribute Validation Rules

Attribute validation rules ensure that Attribute Types conform to a valid input range and format. The **Attribute Validation Rules** tab of the **Organization Config** screen (Figure 55) displays the Attribute validation rules available to all Organizations on the ThreatConnect instance (that is, the System Attribute validation rules; see the *ThreatConnect System Administration Guide* for more information), as well as the Attribute validation rules specific to the Organization (i.e., custom Attribute validation rules).

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.	
Adversary Ownership (System)	SelectOne	[hidden]	Infrastructure Ownership Types	
Adversary Type (System)	SelectOne	[hidden]	The type of Adversary.	
Bitcoin Address (System)	Regex	[hidden]	Matches valid bitcoin addresses.	
Boolean (System)	SelectRadio	[hidden]	Valid boolean values: True, False.	
Campaign Status (System)	SelectOne	[hidden]	Valid Statuses: Ongoing, Historic, Future	
COA Effectiveness (System)	SelectOne	[hidden]	Values for COA Effectiveness	
COA Effects (System)	SelectOne	[hidden]	Course of Action Effects	

Figure 55

View Attribute Validation Rules

The **Attribute Validation Rules** table displays the following information about the Attribute validation rules available to the Organization:

- **Name:** This column displays the name of the Attribute validation rule.
- **Type:** This column displays the data format for the Attribute validation rule.
- **Rule:** This column defines the rule being used, but its contents are always hidden.
- **Description:** This column displays a description of the Attribute validation rule.
- **Options:** This column provides options for editing and deleting the Attribute validation rule. These options are available only to custom Attribute validation rules.

To view only custom Attribute validation rules, clear the **Include System Rules** checkbox (Figure 56).

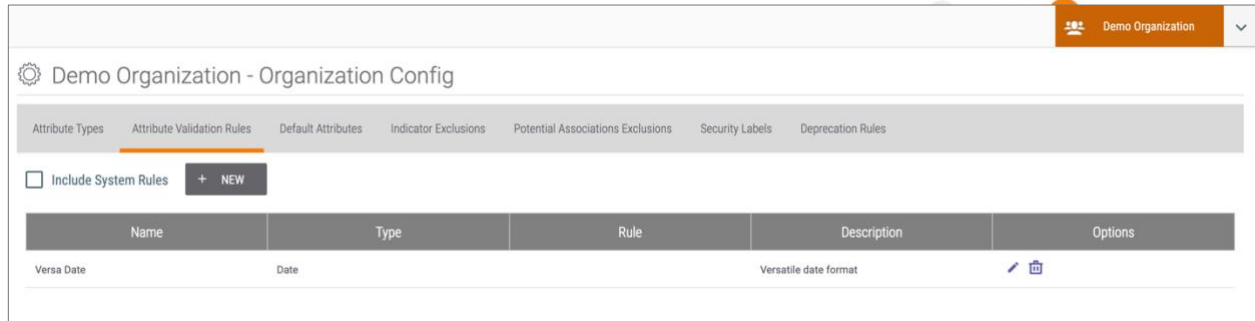


Figure 56

Create Attribute Validation Rule

Click the **+ NEW** button at the top left of the **Attribute Validation Rules** table to create a new custom Attribute validation rule for the Organization. The **Create Attribute Validation Rule** window will be displayed (Figure 57).

The dialog box contains the following elements:

- Type:** A dropdown menu currently showing 'Regex'.
- Name *:** A text input field.
- Description *:** A larger text area for description.
- Enter a valid Regular Expression *:** A text area for the regular expression.
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom right.

Figure 57

- **Type:** Use the dropdown menu to select the data format to use for the validation rule:
 - **Regex:** a regular expression that will consider only matching inputs to be valid (e.g., an IP address or email address on a certain domain)
 - **Xsd:** an XML Schema Definition used to validate input (useful for attaching logs from a vendor product)
 - **Select One Picklist:** a dropdown menu of options from which users may select only one value (e.g., high/medium/low priorities)
 - **Select One Radio:** similar to the **Select One Picklist**, but presented as a series of radio buttons



- **Date**
- **Date/Time**
- **Integer:** A whole number, valid in the specified range (e.g., 0:1440 for “minutes worked”)
- **Name:** Enter the name of the validation rule as it will be displayed when creating an Attribute Type (i.e., in the **Validation Rule** dropdown list in Figure 53).
- **Description:** Enter a description for the Attribute validation rule.
- **Parameters:** The label on the last field in this window will vary depending on the selected type (e.g., **Enter a valid Regular Expression** for the **Regex** type). Enter the parameters for the validation rule. This field is not displayed for the **Date** and **Date/Time** types.

Click the **SAVE** button to save the custom validation rule. Note that the rule will have to be attached to an actual Attribute Type in order to validate user input.

Figure 58 is an example of a completed Attribute validation rule that defines acceptable inputs as emails from the threatconnect.com domain.

The screenshot shows a dialog box titled "Create Attribute Validation Rule". It has a close button (X) in the top right corner. The "Type" dropdown menu is set to "Regex". The "Name *" field contains the text "ThreatConnect Email". The "Description *" field contains the text "An email address from the ThreatConnect domain". The "Enter a valid Regular Expression *" field contains the text "[A-Za-z0-9_-]+@threatconnect.com". At the bottom right, there are two buttons: "CANCEL" and "SAVE".

Figure 58

Default Attributes

To keep [Details screens](#) from becoming cluttered, only a few Attribute Types are pre-populated. However, an Organization Administrator may choose to set placeholder default Attribute Types for a Group or Indicator type to remind users to populate them as soon as the Group or Indicator is created. The **Default Attributes** tab of the **Organization Config** screen (Figure 59) displays the Attribute Types that will be displayed by default when opening the **Details** screen for particular Group and Indicator types in the Organization.



Type	Attribute	Message	Sort Index	Options
Adversary	Date of Discovery	Enter the date on which the object was discovered.	5	
Campaign	Date of Discovery	Enter the date on which the object was discovered.	5	
Email	Date of Discovery	Enter the date on which the object was discovered.	5	
Event	Date of Discovery	Enter the date on which the object was discovered.	5	
Incident	Date of Discovery	Enter the date on which the object was discovered.	5	
Report	Date of Discovery	Enter the date on which the object was discovered.	5	

Figure 59

View Default Attribute Types

The **Default Attributes** table displays the following information about the Attribute Types that will be displayed by default on the **Details** screen:

- **Type:** This column displays the Group or Indicator type that will display the default Attribute Type on its **Details** screen.
- **Attribute:** This column displays the Attribute Type that will be displayed by default on the **Details** screen.
- **Message:** This column displays the prompt to the user to enter data for the Attribute Type.
- **Sort Index:** This column displays enter the index number for the Attribute Type, which determines where it will be in the list of Attribute Types on the **Details** screen.
- **Options:** This column provides options for editing and deleting the default Attribute Type.

Create Default Attribute Type

Click the **+ NEW** button at the top left of the **Default Attributes** table to create a new default Attribute Type for the Organization. The **Create Default Attribute Type** window will be displayed (Figure 60).



Figure 60

- **Attribute Type:** Use the dropdown menu to select an Attribute Type to be displayed by default on the **Details** screen.
- **Type:** Use the dropdown menu to select one or more Groups or Indicators whose **Details** screen will display the Attribute Type by default. Only Groups or Indicators to which the Attribute Type applies will be listed in the dropdown menu.
- **Message:** Click in the box to enter text prompting users to populate the Attribute on the **Details** screen. The text will be a link that takes users to a window in which to enter the Attribute.
- **Sort Index:** Click in the box (or use the plus and minus signs) to enter 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 Attributes list, and the highest number will be at the bottom.

Click the **SAVE** button to save the default Attribute Type.

Indicator Exclusions

Indicator Exclusion Lists prevent the import of Indicators that may be deemed illegitimate or non-hostile by an Administrator. ThreatConnect allows the creation of Indicator Exclusion Lists at the System, Community, Source, and Organization levels. When a user attempts to create an Indicator that is on the Organization's Exclusion List, they will receive an error message warning that the Indicator is contained on an Organization-wide Exclusion List.

The **Indicator Exclusions** tab of the **Organization Config** screen (Figure 61) displays information on the Organization-wide Indicator Exclusion Lists—that is, the Indicators whose import into the Organization will be prevented.



Type	Exclusion Count	Options
Address-IPv4	Custom: 2 fixed, 1 variable	
Address-IPv6	None	
ASN-AS Number	None	
BadGirl-BadGirl	None	
BadGuy-BadGuy	None	
CIDR-Block	None	
Email Subject-Subject	Custom: 2 fixed	
Email Subjects-Subject	None	
EmailAddress	Custom: 1 fixed	
File-MD5	None	
File-SHA1	None	
File-SHA256	None	

Figure 61

View Indicator Exclusions

The **Indicator Exclusions** table displays the following information about the Organization's Indicator Exclusion Lists:

- **Type:** This column displays all Indicator types in the Organization, including custom Indicator types. See the *ThreatConnect System Administration Guide* for more information on custom Indicators.
- **Exclusion Count:** This column displays the number of exclusions on the Indicator Exclusion List for the Indicator type. Fixed exclusions refer to specific Indicators (e.g., **www.xyz.com**), whereas variable exclusions refer to Indicators with wildcards (***www.xyz.com***).
- **Options:** This column provides the option to edit the Indicator Exclusion List for an Indicator type.

Create Indicator Exclusion List

Click the pencil icon for an Indicator type that does not yet have an Exclusion List. The **Exclusion Details** window for the Indicator type will be displayed (Figure 62).



URL Exclusion Details

Custom

<No exclusions specified.>

+ UPLOAD FILE

CANCEL SAVE

Figure 62

Delete the **<No exclusions specified.>** text. Then enter each Indicator to be excluded into the **Custom** box, one per line, or click the **+ UPLOAD FILE** button to navigate to a directory and select a **.txt** file listing the exclusions in that format. Use the asterisk (*) as a wildcard before and after an Indicator to exclude all results containing that Indicator. For example, ***xyz.com*** in the URL Exclusion list would exclude any URL that contains the string **xyz.com**.

Figure 63 shows an example of a newly created Exclusion List for the URL Indicator type.

URL Exclusion Details

Custom

www.goodurl.com
www.anothergoodurl.com
www.xyz.com


+ UPLOAD FILE

CANCEL SAVE

Figure 63

After all exclusions have been entered, click the **SAVE** button. The row for the Indicator type in the **Indicator Exclusions** table will display the number of fixed and variable exclusions.

Edit Indicator Exclusion List

To edit an existing Exclusion List for an Indicator type, click the pencil  icon for that Indicator type. The **Exclusion Details** window will be displayed (Figure 64).

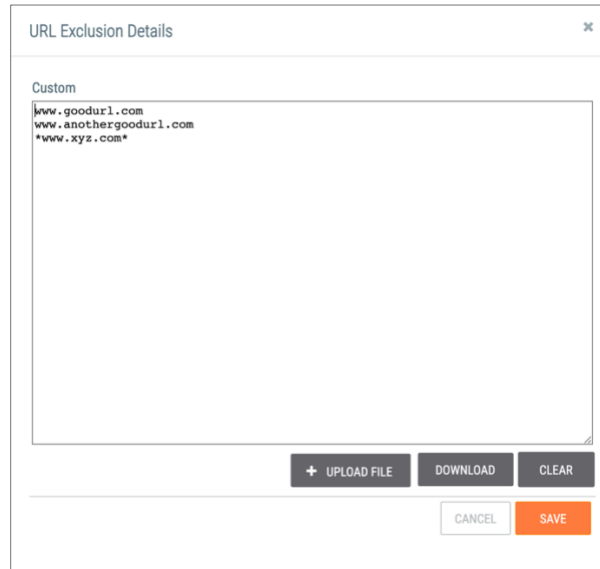



Figure 64

To modify the Exclusion List, edit it directly in the **Custom** box. Otherwise, click the **DOWNLOAD** button to download and edit a **.txt** file, and then click the **+ UPLOAD FILE** button to upload the edited file. Click the **SAVE** button to save the changes to the Exclusion List.

Delete Indicator Exclusion List

To delete an existing Exclusion List for an Indicator type, click the pencil  icon for that Indicator type. The **Exclusion Details** window will be displayed (Figure 64). Click the **CLEAR** button. The **Remove Exclusions** window will be displayed (Figure 65).

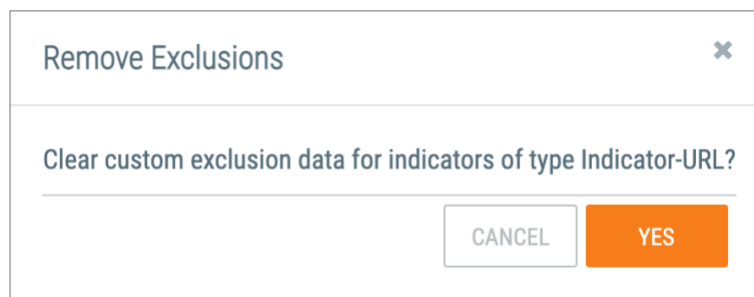


Figure 65

Click the **YES** button to clear the Exclusion List for the Indicator type.

Potential Associations Exclusions

Potential Associations Exclusion Lists prevent specific [Artifact](#) values in [Workflow Cases](#) from suggesting any potential [Associations](#). ThreatConnect allows the creation of Potential Associations Exclusion Lists at the System and Organization levels.



The **Potential Associations Exclusions** tab of the **Organization Config** screen (Figure 66) displays information on the Organization-wide Potential Associations Exclusion Lists—that is, the Artifacts whose creation of potential associations will be prevented.

Type	Exclusion Count	Options
Address	Custom: 1 fixed, 1 variable	
ASN	None	
ASN (Old)	None	
Asset Group ID	None	
Asset Group ID (Old)	None	
Bitcoin Wallet Address	None	
Blackberry Address	None	
Certificate File	None	
CIDR	None	
CIDR (Old)	None	
Command	None	
Credential ID	None	

Figure 66

View Potential Associations Exclusions

The **Potential Associations Exclusions** table displays the following information about the Organization’s Potential Associations Exclusion Lists:

- **Type:** This column displays all Artifact types in the Organization, including custom Artifact types. See the *ThreatConnect System Administration Guide* for more information on custom Artifacts.
- **Exclusion Count:** This column displays the number of exclusions on the Potential Associations Exclusion List for the Artifact type. Fixed exclusions refer to specific Artifacts (e.g., **www.xyz.com**), whereas variable exclusions refer to Artifacts with wildcards (***www.xyz.com***).
- **Options:** This column provides the option to edit the Potential Associations Exclusion List for an Artifact type.

Create Potential Associations Exclusion List

Click the pencil icon for an Artifact type that does not yet have an Exclusion List. The **Exclusion Details** window for the Artifact type will be displayed (Figure 67).



URL Exclusion Details

Custom

<No exclusions specified.>

+ UPLOAD FILE

CANCEL SAVE

Figure 67

Delete the **<No exclusions specified.>** text. Then enter each Artifact to be excluded into the **Custom** box, one per line, or click the **+ UPLOAD FILE** button to navigate to a directory and select a **.txt** file listing the exclusions in that format. Use the asterisk (*) as a wildcard before and after an Artifact to exclude all results containing that Artifact. For example, ***xyz.com*** in the URL Exclusion list would exclude any URL that contains the string **xyz.com**.

Figure 68 shows an example of a newly created Exclusion List for the URL Artifact type.

URL Exclusion Details

Custom

www.goodurl.com
www.anothergoodurl.com
www.xyz.com

+ UPLOAD FILE


CANCEL SAVE

Figure 68

After all exclusions have been entered, click the **SAVE** button. The row for the Artifact type in the **Potential Associations Exclusions** table will display the number of fixed and variable exclusions.



Edit Potential Associations Exclusion List

To edit an existing Exclusion List for an Artifact type, click the pencil  icon for that Artifact type. The **Exclusion Details** window will be displayed (Figure 69).

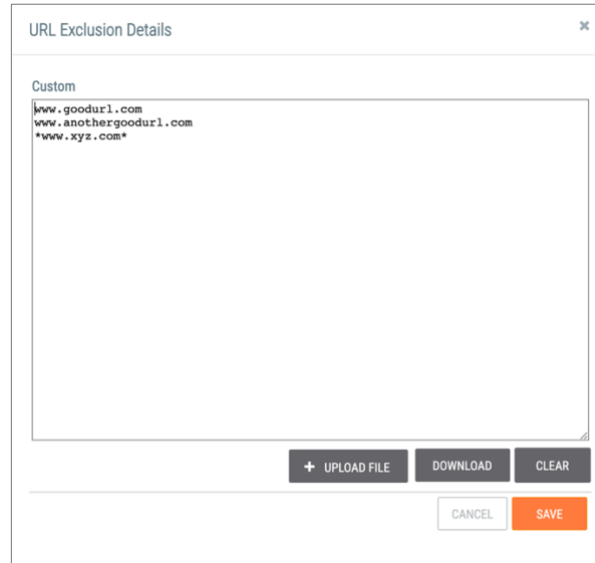



Figure 69

To modify the Exclusion List, edit it directly in the **Custom** box. Otherwise, click the **DOWNLOAD** button to download and edit a **.txt** file, and then click the **+ UPLOAD FILE** button to upload the edited file. Click the **SAVE** button to save the changes to the Exclusion List.

Delete Potential Associations Exclusion List

To delete an existing Exclusion List for an Artifact type, click the pencil  icon for that Artifact type. The **Exclusion Details** window will be displayed (Figure 69). Click the **CLEAR** button. The **Remove Exclusions** window will be displayed (Figure 70).

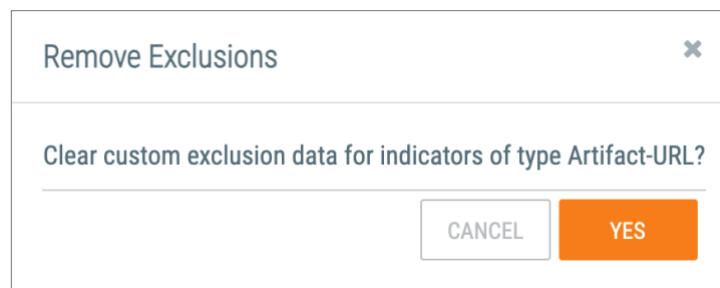


Figure 70

Click the **YES** button to clear the Exclusion List for the Artifact type.



Security Labels

An Organization may use custom Security Labels to determine how to treat Groups and Indicators in bulk. On the System level, ThreatConnect uses the [Traffic Light Protocol](#) (TLP) system developed by the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). Organization Administrators can define their own Security Labels based on their Organization's needs.

Security Labels are most effective when users share or contribute information within ThreatConnect. Security Labels allow users to withhold or divulge information, depending on their Organization's policies, based on the Security Label applied to each piece of data.

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

The **Security Labels** tab of the **Organization Config** screen (Figure 71) displays the Security Labels available to all Organizations on the ThreatConnect instance (that is, the System-wide Security Labels; see the *ThreatConnect System Administration Guide* for more information), as well as the Security Labels specific to the Organization (i.e., custom Security Labels).

Name	Description	Options
Purple	This security label designates information that can be shared freely with partner groups, but must not be shared outside of those groups.	
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 71

View Security Labels

The **Security Labels** table displays the following information about the Security Labels available to the Organization:

- **Name:** This column displays the name of the Security Label.
- **Description:** This column displays a description of the Security Label.



- **Options:** This column provides options for editing, deleting, and consolidating the Security Label. These options are available only to custom Security Labels.

To view only custom Security Labels, clear the **Include System Labels** checkbox (Figure 72).

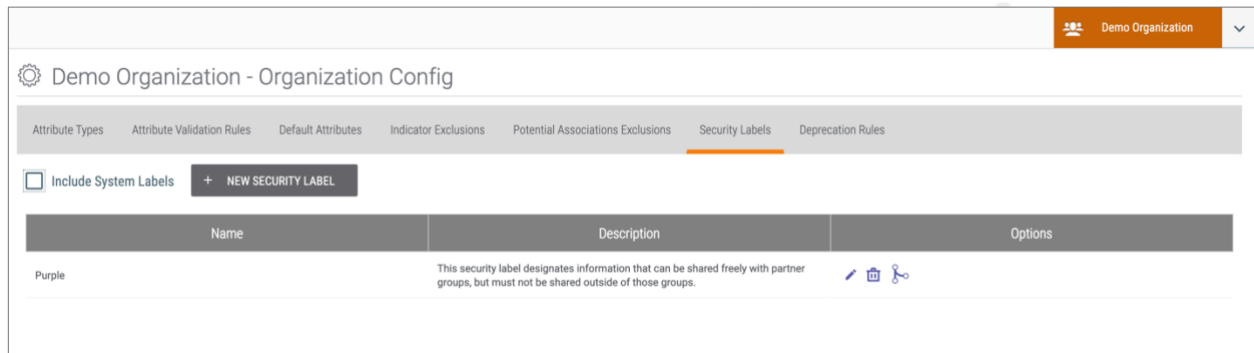


Figure 72

Create Security Label

Click the + **NEW SECURITY LABEL** button at the top left of the **Security Labels** table to create a new custom Security Label for the Organization. See [Creating Security Labels](#) for further instruction.

Edit Security Label


To edit a custom Security Label, click the pencil  icon for that Security Label. The **Create Security Label** window will be displayed (Figure 73).

Figure 73

See [Creating Security Labels](#) for further instruction on the fields in this window.

Delete Security Label



To delete a custom Security Label, click the trash  icon for that Security Label. The **Delete Security Label** window will be displayed (Figure 74).



Figure 74

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

Consolidate Security Label

Custom Security Labels can be consolidated with System-wide Security Labels, causing all data that have the custom Security Label to be re-labeled with a System-wide Security Label. To consolidate a Security Label, click the **Consolidate**  icon for that Security Label. The **Consolidate Security Label** window will be displayed (Figure 75).

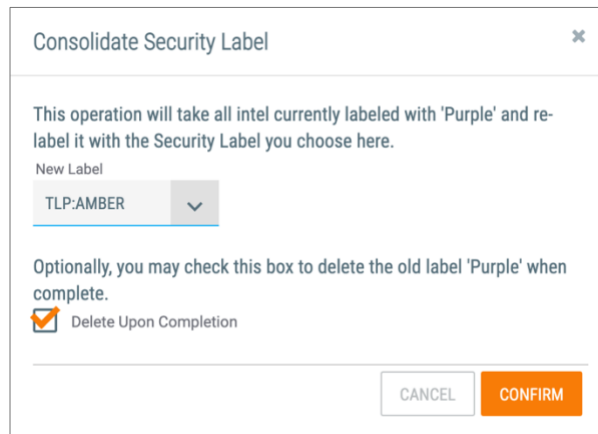


Figure 75

- **New Label:** Select the System-wide Security Label into which to consolidate the custom Security Label,
NOTE: The Include System Labels checkbox on the Security Labels tab of the Organization Config screen must be selected for options to be provided in the New Label dropdown menu.
- **Delete Upon Completion:** Select this checkbox to delete the custom Security Label after the consolidation has completed.

Click the **CONFIRM** button to complete the consolidation.

Deprecation Rules

Indicator Confidence deprecation is a great way to allow Indicators to drop in [Confidence Rating](#) over time or be deleted if the Confidence Rating is not being maintained and updated. Confidence deprecation is used in the case of an Indicator, such as an IP Address, that is no longer being used for any malicious activity for a certain amount of time. Depending on the Confidence deprecation rule, ThreatConnect will drop the Confidence Rating or delete the Indicator, assuming that the



Indicator is dormant or that the threat actor has ceased using it. ThreatConnect allows the creation of Confidence deprecation rules at the System, Community, Source, and Organization levels.

The **Deprecation Rules** tab of the **Organization Config** screen (Figure 76) displays the Confidence deprecation rules that have been set for the Organization.

Indicator Type	Interval	Amount	Percentage	Recurring	Action At Minimum	Options
Address	2 days	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inactive	
Host	3 days	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Delete	
URL	3 days	5	<input type="checkbox"/>	<input type="checkbox"/>	None	

Figure 76

Create Deprecation Rule

See [Configuring Indicator Confidence Deprecation](#) for instruction on how to create a new Confidence deprecation rule for the Organization.

Edit Deprecation Rule

To edit an existing Confidence deprecation rule for the Organization, click the pencil icon for the rule. The **Create/Edit Deprecation Rule** window will be displayed (Figure 77). See [Configuring Indicator Confidence Deprecation](#) for further instruction.

Create/Edit Deprecation Rule

Indicator Type: Address

Action At Minimum: Set Inactive

Confidence: 2

Percentage:

Lock Status:

Interval: 2 days

Recurring:

CANCEL SAVE


Figure 77

NOTE: The *Indicator Type* selection cannot be changed. To set a deprecation rule for a different *Indicator type*, create a new deprecation rule or edit the existing deprecation rule for that type.



NOTE: Each Indicator type may have only one Confidence deprecation rule. Attempts to create a second rule for an Indicator type will result in an error.

Delete Deprecation Rule

To delete a Confidence deprecation rule for the Organization, click the trash  icon for the rule. The **Delete Deprecation Rule** window will be displayed (Figure 78).

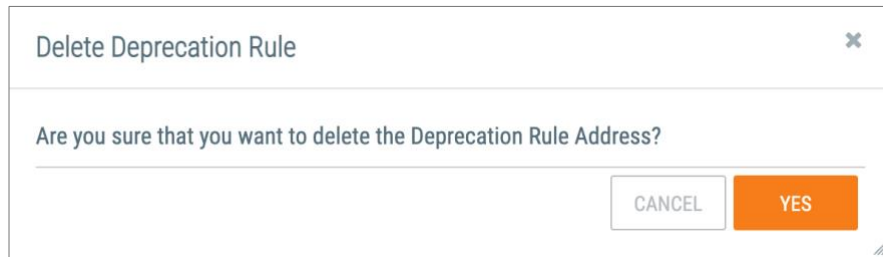


Figure 78

Click the **YES** button to delete the deprecation rule.