



Super User

User Guide

Software Version 6.5

April 5, 2022

10026-01 EN Rev. A



©2022 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.



Table of Contents

OVERVIEW	4
MANAGING DATA IN ALL ORGANIZATIONS	4
Dashboard	4
The Dashboard Screen	4
Dashboard Card Configuration.....	5
TQL Queries.....	6
Posts	6
Threat Intelligence	6
Browse.....	7
Create	7
Import	8
Search and Analyze.....	9
The Details Screen.....	11
ThreatConnect Query Language.....	11
ThreatConnect Browser Extension	11
Workflow	13
Workflow Tasks.....	13
Workflow Templates.....	15
Workflow Cases	19
Playbooks.....	23
Playbook Templates	25
ADMINISTRATION AND CONFIGURATION OF ALL ORGANIZATIONS	27
Organization Settings.....	27
Viewing Organization Settings.....	27
Managing User Accounts.....	27
Organization Activity	28
Organization Configuration	28



Overview

A Super User account in ThreatConnect® enables users on multitenant instances to easily view and manage all of their customers' data from a single user account. Super Users do not have any access or permissions at the System level, but do have full data-level, administrative, and configuration permission at the Organization level for all Organizations on the ThreatConnect instance. Super Users may view, create, edit, and delete data (dashboards, posts, threat intelligence, Workflow, and Playbooks) in all Organizations on the ThreatConnect instance. They also can administrate and configure all Organizations, including creating, deleting, and updating user accounts and adding, modifying, and deleting Organization-level variables, metrics, Attribute Types, Indicator exclusion lists, and Security Labels.

This guide covers all of the functionalities specific to your Super User account. It discusses all the areas of ThreatConnect in which you can access and modify data in all Organizations on your instance and the administrative and configuration functions available to you for those Organizations.

Managing Data in All Organizations

Your Super User account belongs to one Organization (your “home Organization”), but you can view, manage, and modify dashboard, posts, threat intelligence, Workflow, and Playbooks information in all Organizations on your ThreatConnect instance.

Dashboard

As a Super User, you can determine which Organizations' data you want to view on the [Dashboard](#) screen. You can also configure dashboard cards to show data from selected Organizations and, for query cards, enter [ThreatConnect Query Language \(TQL\)](#) queries to search for objects belonging to multiple Organizations.

The Dashboard Screen

The **My Intel Sources** selector on the **Dashboard** screen will display a **My Orgs** list from which you can select the Organizations whose data you want to view (Figure 1).

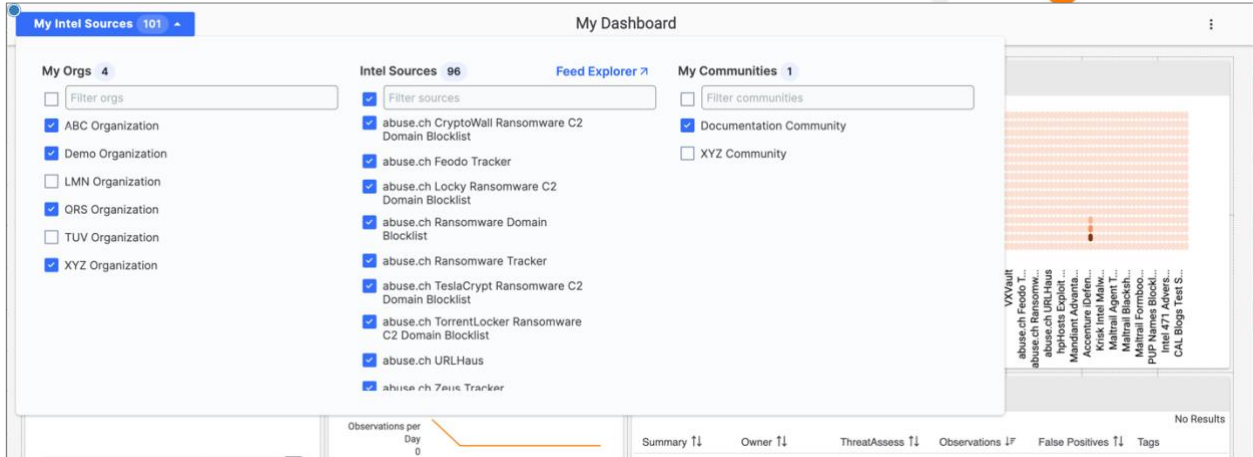


Figure 1

Dashboard Card Configuration

When configuring Metric and Query dashboard cards, you can use the **My Orgs** list to select Organizations whose data you want to include on the card (Figure 2).

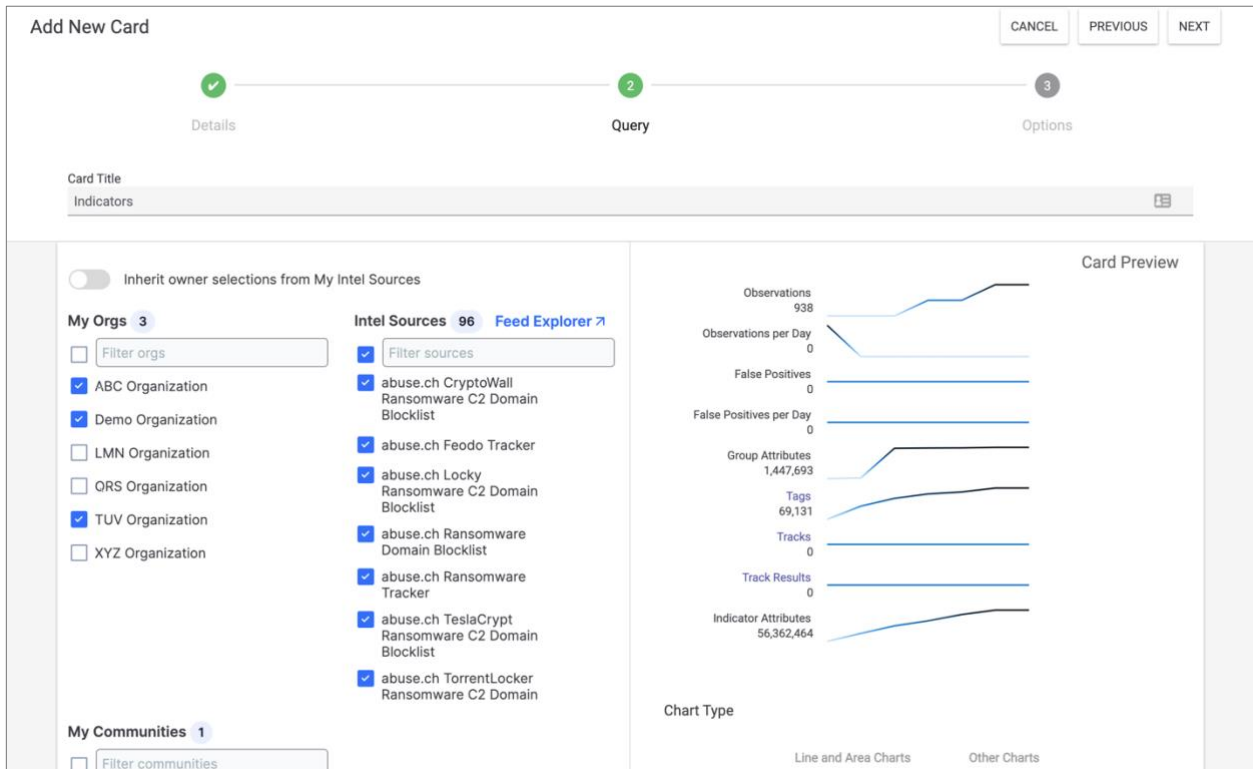


Figure 2



TQL Queries

When configuring Query dashboard cards, you can enter a TQL string to search for objects belonging to multiple Organizations in the **Advanced Query** field. See the “Query for Objects Belonging to Multiple Owners” section of [Using ThreatConnect Query Language \(TQL\)](#) for more information.

Posts

The **My Org** section of the [Posts](#) screen will display all Organizations on your ThreatConnect instance (Figure 3).

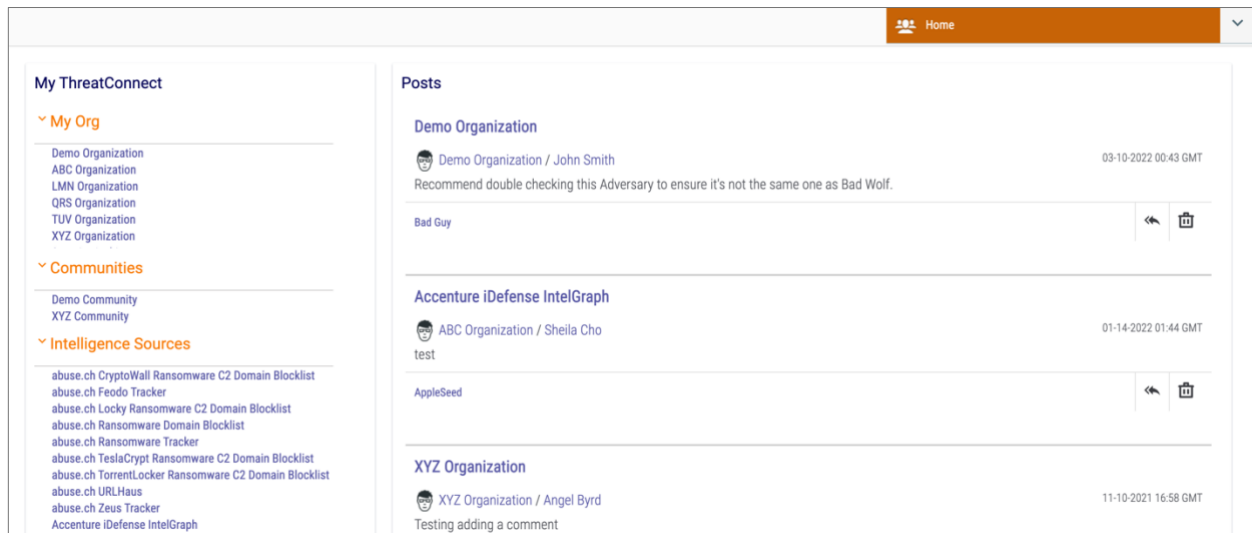


Figure 3

By default, the screen will display posts from your home Organization, and the name of your home Organization will be at the top of the **My Org** list. To view posts in another Organization, click on that Organization’s name in the list. You can also use the selector at the top right of the screen to navigate to the **Posts** screen for another Organization.

Threat Intelligence

As a Super User, you can view, create, import, filter, search for, modify, and delete threat intelligence in all Organizations on your ThreatConnect instance.



Browse

The **My Intel Sources** selector on the [Browse](#) screen will display a **My Orgs** list from which you can select the Organizations whose data you want to view (Figure 4).

The screenshot shows the ThreatConnect interface with the 'My Intel Sources' selector open. It displays three panels: 'My Orgs' (6 items), 'Intel Sources' (87 items), and 'My Communities' (1 item). The 'Intel Sources' panel is expanded, showing a list of sources with their addresses and threat intelligence counts.

Course of Action	Address	ThreatConnect Intelligence	F/P T1	Added T1	Modified T1
Document	52.71.57.184	318	--	10-08-2021	03-29-2022
E-mail	54.161.222.85	332	--	12-10-2021	03-29-2022
Event	34.205.242.146	336	--	12-10-2021	03-29-2022
Incident				10-08-2021	03-29-2022
Intrusion Set				10-21-2021	03-29-2022
Malware				10-22-2021	03-29-2022
Report				12-13-2021	03-29-2022

Figure 4

Create

When using the [Create](#) option on the top navigation bar to add an object (Indicator, Group, Track, or Victim) to ThreatConnect, you can select any Organization on the ThreatConnect instance from the **Owner** menu (Figure 5).

The screenshot shows the 'Create Campaign' screen with a three-step process: 1. Details, 2. Associations (Optional), and 3. Attachments (Optional). The 'Owner' dropdown menu is open, showing a list of organizations and communities.

Owner * Crypto

Organizations

- ABC Organization
- Demo Organization
- LMN Organization
- QRS Organization
- TUV Organization
- XYZ Organization

Communities

- Demo Community
- XYZ Community

Intelligence Sources

Figure 5



Import

When using the **Import** option on the top navigation bar to import objects ([Email import](#), [structured Indicator import](#), [unstructured Indicator import](#), or [Signature import](#)), you can select any Organization on the ThreatConnect instance from the **Owner** menu (Figure 6).

The screenshot shows the 'Import E-mail' interface. At the top, there is a breadcrumb trail: 'Import' (highlighted in orange), 'Score', 'Indicators', 'Victims', and 'Confirm'. Below this is a blue information bar with a question mark icon and the text: 'Select Import to automatically import an MSG or EML file, or copy and paste the required data from the originating e-mail into the fields below.' Below the information bar is a dark grey button labeled '+ IMPORT MSG OR EML FILE'. The main form area has a 'Owner' dropdown menu set to 'Documentation Team'. To the left of the form is a 'To' field with a search icon and a list of organizations: 'Demo Organization' (highlighted), 'ABC Organization', 'LMN Organization', and 'QRS Organization'. To the right of the 'To' field is a 'Header' text area. At the bottom right of the form is a '> Next' button. At the very bottom right of the interface are 'CANCEL' and 'SAVE' buttons.

Figure 6



Search and Analyze

The **OWNERS** selector in the [Search drawer](#) will display a **My Orgs** list from which you can select the Organizations in which to search for data (Figure 7).

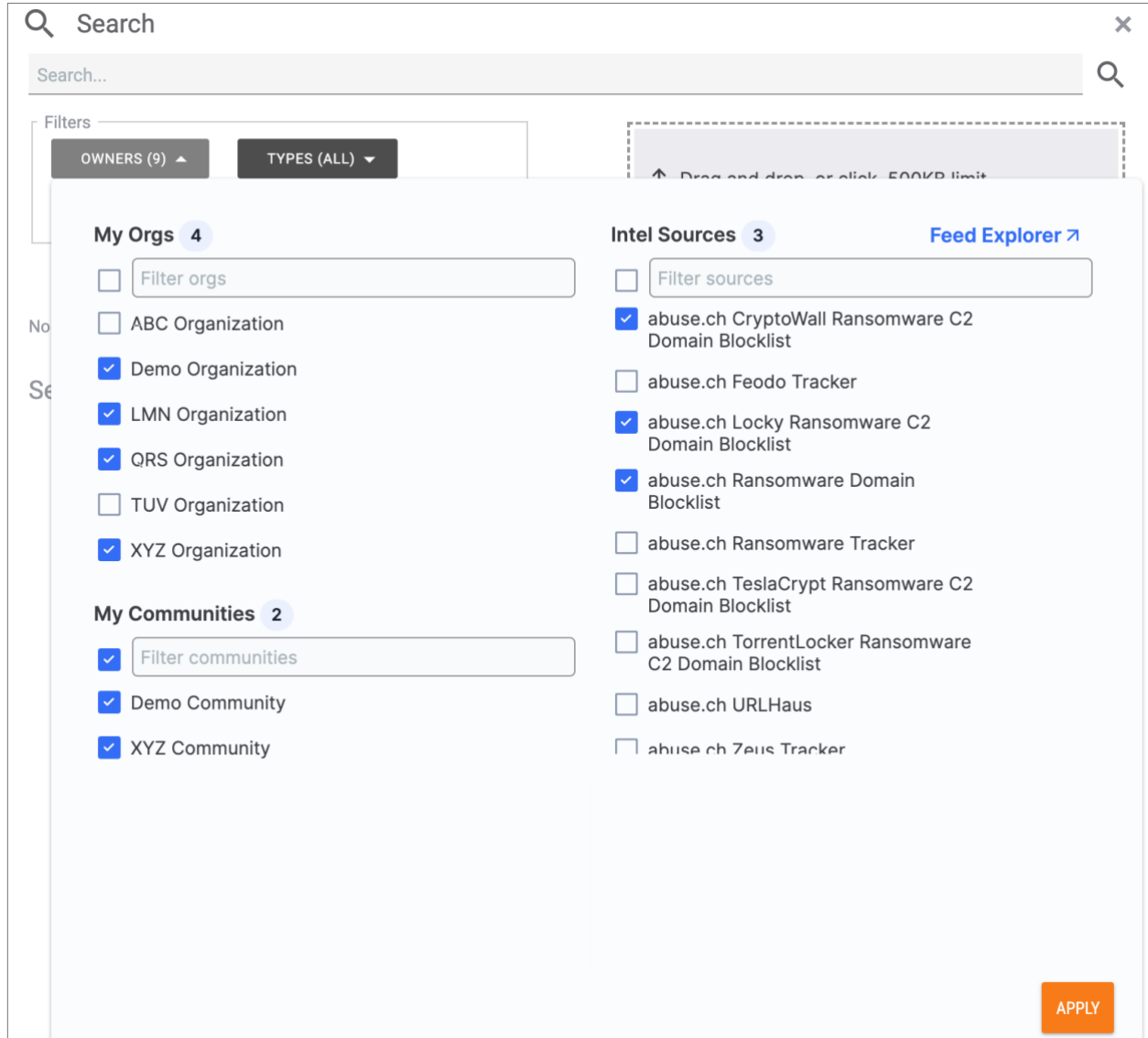


Figure 7

You can also add objects found during searches to any Organization on your instance (Figure 8).



Search

verybadguy

Filters

OWNERS (9) TYPES (ALL)

Local Matches Only

Drag and drop, or click. 500KB limit

Here's some intel we found relating to your search. Sort Exact Matches By Summary

Potentially Related Matches

Match	Type	Match on	Owner	Matched On
verybadguy.com	Host	Summary: verybadguy.com	Demo Community, Demo Organization, LMN On	
verybadguy@bad.com	EmailAddress	Summary: verybadguy@bad.com	Demo Community, Demo Organization	
Mark's Demo Case	Case	Artifact Name: verybadguy@badguyz.com	Demo Organization	
Demo Case Using a Workflow Template	Case		Demo Organization	Artifact Name

ADD TO OWNER

- abuse.ch CryptoWall Ransomware C2...
- abuse.ch Feodo Tracker
- abuse.ch Locky Ransomware C2 Dom...
- abuse.ch Ransomware Domain Blockl...
- abuse.ch Ransomware Tracker
- abuse.ch TeslaCrypt Ransomware C2 ...
- abuse.ch TorrentLocker Ransomware ...

Figure 8

NOTE: The ADD TO OWNER dropdown lists all owners in alphabetical order. It does not separate them by owner type (Organization, Community, and Source). Scroll down to find the owner to which you want to add an object found during a search.



The Details Screen

In addition to Communities and Sources, the **Additional Owners** card on the [Details screen](#) for an object will list all of the other Organizations that own the object (Figure 9).

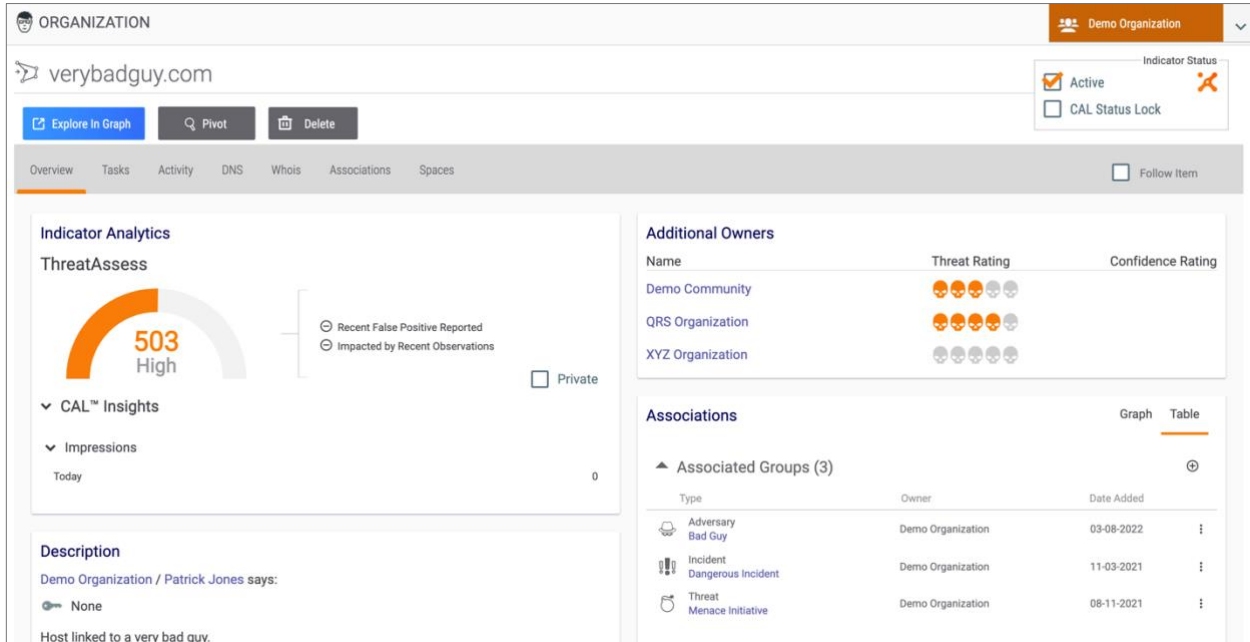


Figure 9

Click on the name of an Organization to view the object within that Organization. You can also use the selector at the upper-right corner of the screen to choose owners in which to view the object. When viewing the object in an Organization other than your home Organization, the label at the upper-left corner of the screen will be **SHARED** instead of **ORGANIZATION**.

ThreatConnect Query Language

You can write TQL queries that search for objects existing in multiple Organizations on your instance. See the “Query for Objects Belonging to Multiple Owners” section of [Using ThreatConnect Query Language \(TQL\)](#) for more information.

ThreatConnect Browser Extension

When selecting sources for the [ThreatConnect Browser Extension](#) to scan for potential Indicators and Groups, you can select multiple Organizations on your instance (Figure 10).

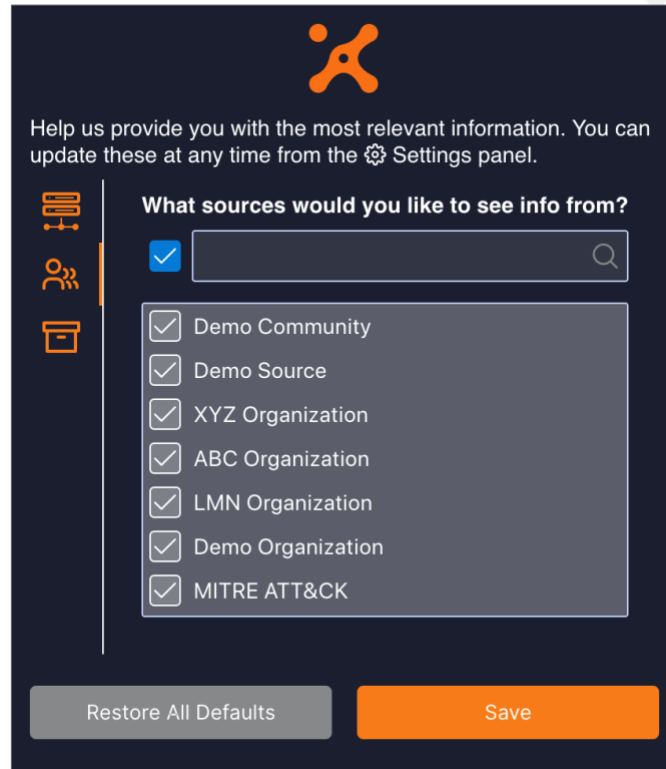


Figure 10

The Browser Extension will indicate when a scan finds objects that are known to exist in multiple Organizations on your instance (Figure 11).

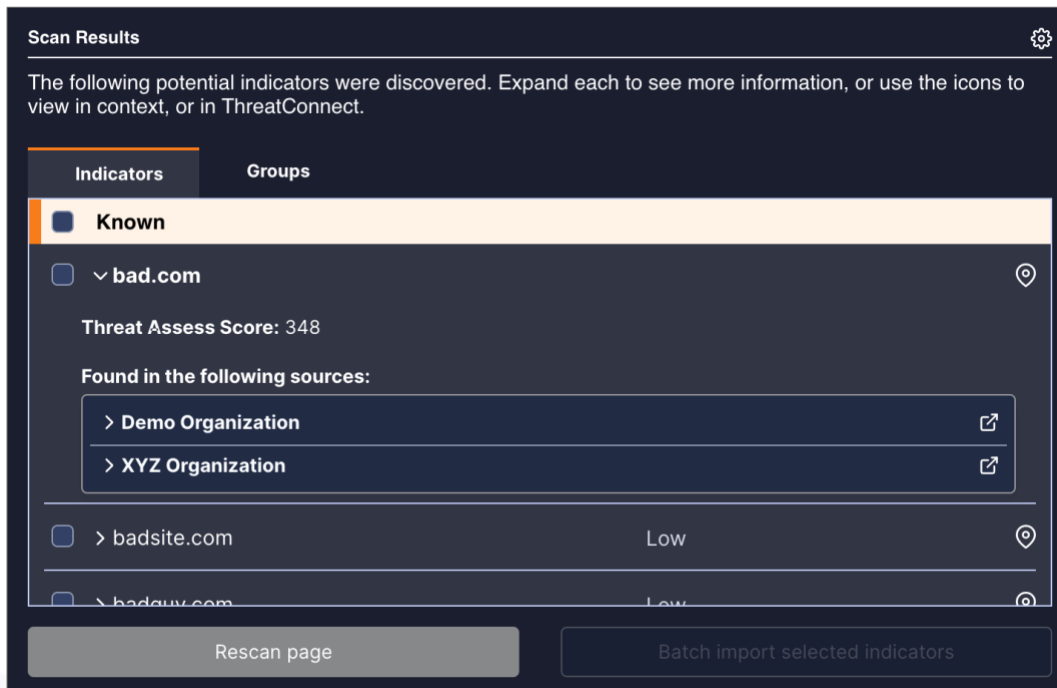


Figure 11



When importing scanned Indicators into ThreatConnect, you can select any Organization on your ThreatConnect instance as the destination owner (Figure 12).

Figure 12

Workflow

As a Super User, you can view, create, modify, assign, and delete Workflow Tasks, Templates, and Cases in all Organizations on your ThreatConnect instance.

Workflow Tasks

The Workflow [Tasks screen](#) will display all Tasks in all Cases in all Organizations on your instance, with the **Org** column indicating the Organization to which each Task belongs (Figure 13).



Type	Required	Case ID	Name	Org	Assignee	Due Date	Status	Case Severity	Missing Required Artifacts
		268	Capture Email Case: Email Investigation	Demo Organization			Open	Low	5
		9359	Capture Email Case: Demo Case Using a Workflow Template	ABC Organization			Open	Medium	5
		24	Investigate Embedded Links Case: File Backup Scam Phishing Alert	XYZ Organization	John Smith		Pending	High	3
		24	Capture Email Case: File Backup Scam Phishing Alert	XYZ Organization	SOC Team	2022-03-28 20:30:00 GMT	Open	High	2
	✓	268	Escalate to Supervisor Case: Email Investigation	Demo Organization			Pending	Low	2
		268	Submit Block Case: Email Investigation	Demo Organization			Pending	Low	2
	✓	9359	Escalate to Supervisor Case: Demo Case Using a Workflow Template	ABC Organization			Pending	Medium	2
		9359	Submit Block Case: Demo Case Using a Workflow Template	ABC Organization			Pending	Medium	2
		24	Research Sender Email Address Case: File Backup Scam Phishing Alert	XYZ Organization	John Smith		Pending	High	1
		24	Investigate Sender Domain Case: File Backup Scam Phishing Alert	XYZ Organization	John Smith		Pending	High	1

Figure 13

You can use the **Owner(s)** dropdown menu in the **FILTERS** selector to select the Organizations you want to include in the **Tasks** table (Figure 14).

The screenshot shows the 'FILTERS' dropdown menu with the 'Owner(s)' dropdown menu open. The 'Owner(s)' menu lists the following organizations with checkboxes:

- ABC Organization
- Demo Organization
- LMN Organization
- QRS Organization
- TUV Organization

Figure 14



NOTE: If the Tasks table is blank when you first use your Super User account to access the Tasks screen, this may be because there are no Organizations selected in the Owner(s) menu. Selecting at least one Organization will cause the table to populate (as long as the selected owners contain at least one Case with at least one Task in it).

You can select an assignee for any Task in any Case, but the assignee must belong to the Organization that owns the Case.

Workflow Templates

The Templates Screen

The Workflow [Templates screen](#) will display all Templates in all Organizations on your instance, with the text at the top left of each Template card indicating the Organization to which the Template belongs (Figure 15).

The screenshot shows the 'Workflow Templates' screen with a navigation bar at the top containing 'Cases', 'Tasks', and 'Templates'. Below the navigation bar, there is a search bar labeled 'Filter Templates by Name' and a 'FILTERS' dropdown menu. The main content area displays a grid of eight template cards, each representing a different organization and template type. Each card includes the organization name, the template title, a status indicator, and a table showing the number of Phases and Tasks. The cards are as follows:

Organization	Template Title	Status	Phases	Tasks
Demo Organization	Cyber Mission Assurance (CMA)	Inactive	3	9
QRS Organization	Collection Plan	Inactive	4	13
QRS Organization	Cyber Mission Assurance (CMA)	Active	3	9
LMN Organization	Dashboard Card Development	Active	5	16
Demo Organization	Email Investigation	Active	4	9
ABC Organization	Indicator Analysis with Automation	Active	4	9
Demo Organization	Cyber Mission Assurance (CMA)	Inactive	3	9
ABC Organization	API Template	Inactive	0	0

Figure 15

You can use the **Owner(s)** dropdown menu in the **FILTERS** selector to select the Organizations you want to include in the **Templates** table (Figure 16).

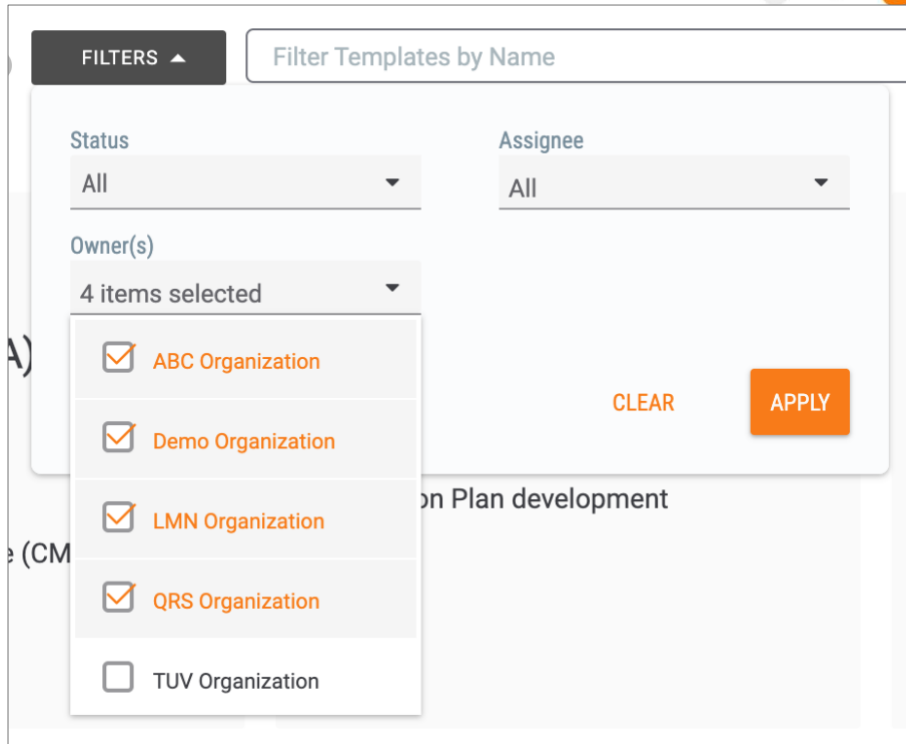


Figure 16

NOTE: If the Templates table is blank when you first use your Super User account to access the Templates screen, this may be because there are no Organizations selected in the Owner(s) menu. Selecting at least one Organization will cause the table to populate (as long as the selected owners contain at least one Template).

Creating a Template

When creating a new Template, you must select the Organization that will own the Template (Figure 17).



Workflow Templates New Workflow

Name: My New Template (15 / 255)

Description: Description (0 / 1500)

Owner *: Select an Owner

- Filter Owners by Name
- ABC Organization
- Demo Organization
- LMN Organization
- QRS Organization
- TUV Organization
- XYZ Organization

Default Assignee: No Default Assignee

Active:

Attributes

Attribute	Description	Actions
No attributes in this template. Click to add an attribute.		

Tasks

Tasks	Type	Name	Assignee	Artifacts	Required	Dependency	Actions
No tasks in this phase. Click to add tasks to create this phase.							

Figure 17

NOTE: The Default Assignee menu will not populate until you select an owner, because the default assignee must belong to the Organization that owns the Template. Similarly, when you assign a Task in the Template, the Default Assignee dropdown menu will list only users who are in the Organization that owns the Template.

Importing a Template

When importing a Template, you must select the Organization that will own the Template (Figure 18).

Import Workflow

Validating Workflow: Phishing Investigation Template.wf

Select Owner

Please select the Owner of this Workflow

Select an Owner

CANCEL NEW FILE IMPORT

Figure 18



NOTE: In addition to the *Validating Workflow* and *Select Owner* steps, you may see steps called *Variables* or *Missing Apps*. See the [“Importing a Template”](#) section of [Workflow Templates](#) for more information.

Sharing a Template across Organizations

As a Super User, you can easily share Templates across Organizations. On the **Templates** screen, select the **Duplicate** option from the vertical ellipsis menu for a Template. Enter a name for the Template, and then select the destination Organization from the **Select Owner** menu (Figure 19).

Duplicate Workflow Template

Name for New Template
Phishing Investigation Template

Select Owner
Select an Owner

Filter Owners by Name

- ABC Organization
- Demo Organization
- LMN Organization
- QRS Organization
- TUV Organization
- XYZ Organization

Figure 19

Copying a TC Exchange Template to an Organization

When copying a TC Exchange Template, you must select the destination Organization (Figure 20).

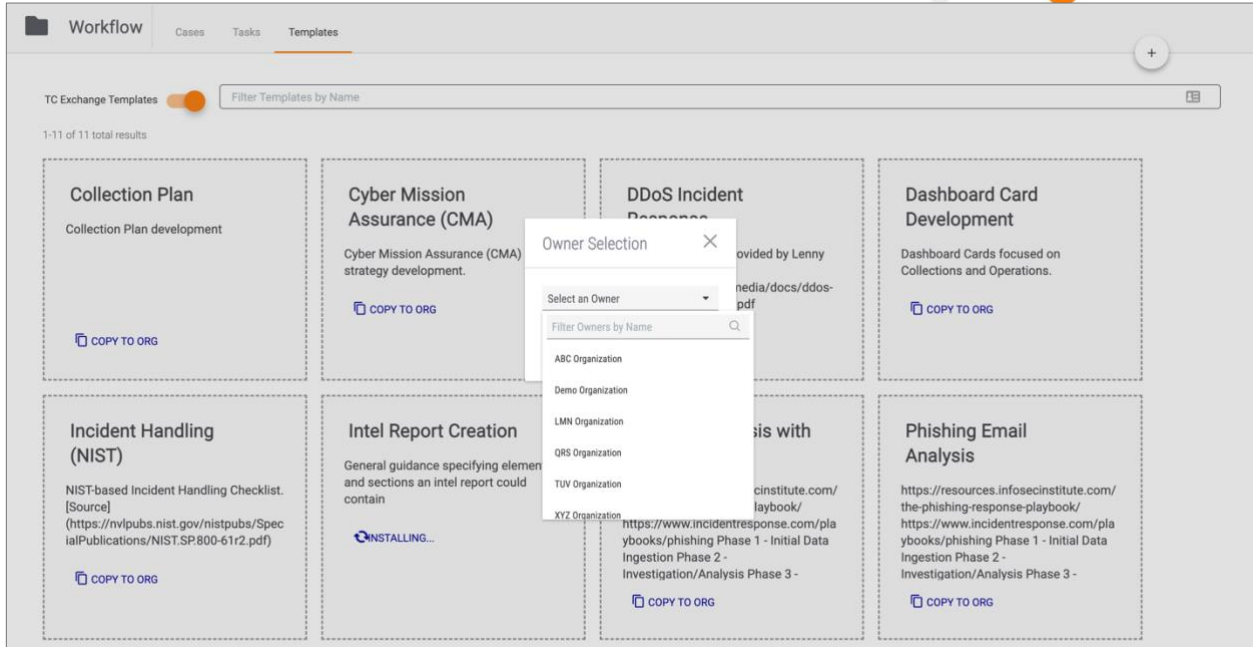


Figure 20

Workflow Cases

The Cases Screen

The Workflow [Cases screen](#) will display all [Cases](#) in all Organizations on your instance, with the **Org** column indicating the Organization to which each Case belongs (Figure 21).

ID	Name	Org	Severity	Missing Required Artifacts	Remaining Tasks	Assignee	Status	Created By	Created Date	Closed Date
25	Suspicious C2 Traffic	Demo Organization	Medium	0		Athena Jackson	Closed	Patrick Jones	2021-08-16 11:14:40	2022-03-16 12:48:24
27	Spearphishing Procedure	Demo Organization	Medium	0	2 / 5	John Smith	Open	API User	2021-08-19 13:44:07	
9359	Demo Case Using a Workflow Template hacker demo	Demo Organization	Medium	10	9 / 9	John Smith	Open	Patrick Jones	2022-02-15 15:14:21	
9401	Demo Case 03	LMN Organization	Medium	0		Patrick Jones	Closed	Patrick Jones	2022-03-22 17:19:31	2022-03-22 17:20:18
223	IOC Case Testing 001	ABC Organization	Low	0			Open	Andrew Lopez	2021-10-28 11:26:02	
268	Email Investigation	Demo Organization	Low	10	9 / 9		Open	Selena Chang	2021-11-23 16:00:07	
269	Patrick's Demo Case phishing	Demo Organization	Low	0	1 / 6	John Smith	Open	Patrick Jones	2021-11-24 08:57:07	
9396	Demo Case	Demo Organization	Low	0	3 / 3	John Smith	Open	Patrick Jones	2022-03-18 16:08:00	
9398	Hacker Triage	LMN Organization	Low	0		Patrick Jones	Closed	Patrick Jones	2022-03-22 15:19:15	2022-03-17 15:19:21
9399	Malware Transfer	QRS Organization	Low	0		Herschel Hodges	Closed	John Smith	2022-03-22 15:45:37	2022-03-18 15:22:45

Figure 21



In card view, the Organization that owns the Case is displayed at the top of the Case's card (Figure 22).

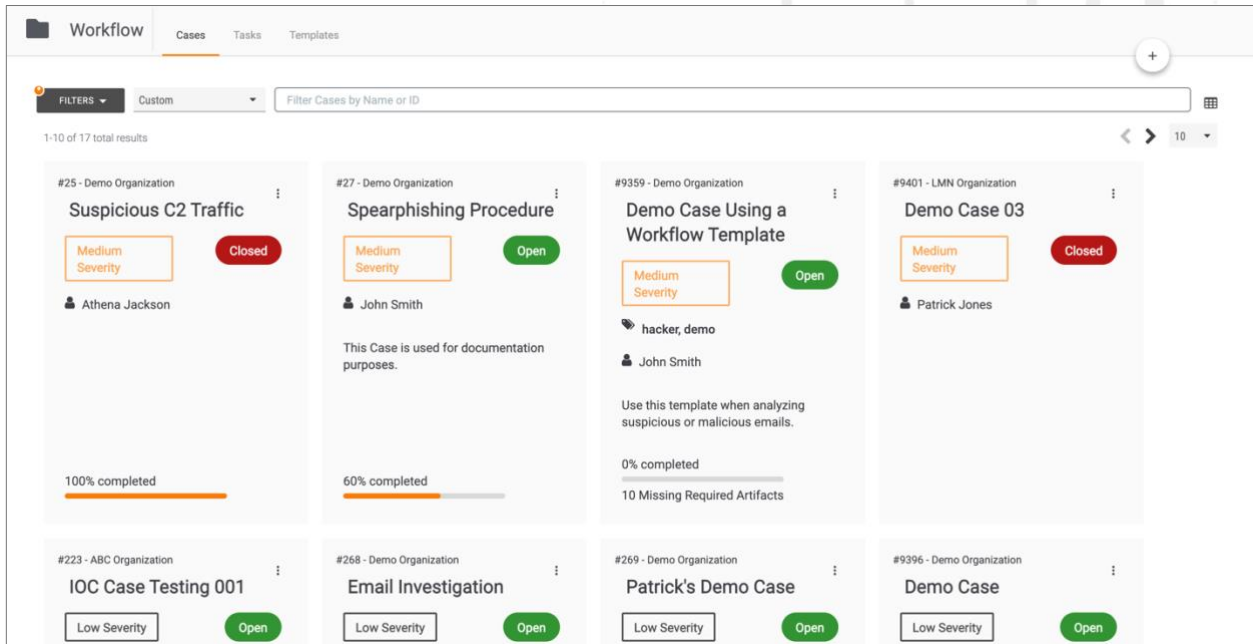


Figure 22

You can use the **Owner(s)** dropdown menu in the **FILTERS** selector to select the Organizations you want to include in the **Cases** table (Figure 23).

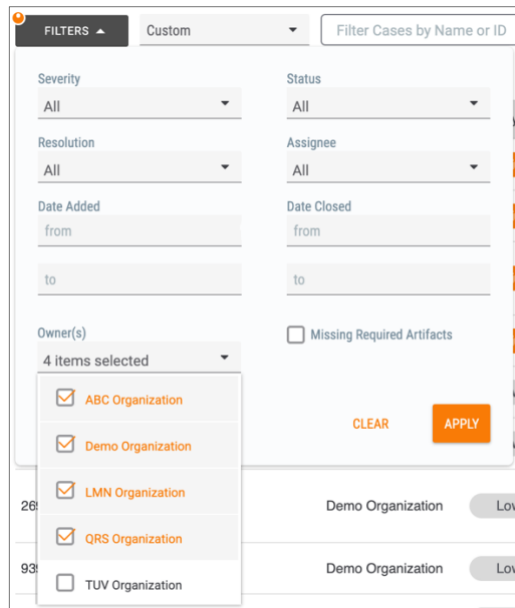


Figure 23

NOTE: If the Cases screen is blank when you first use your Super User account to access the Cases screen, this may be because there are no Organizations selected in the Owner(s) menu. Selecting at



least one Organization will cause the screen to populate (as long as the selected owners contain at least one Case).

Creating a Case

When creating a new Case, you must select the Organization that will own the Case (Figure 24).

New Case [Close]

Name *
[Text Input] 0 / 255

Owner *
Select an Owner [Dropdown]

Filter Owners by Name [Search]

- ABC Organization
- Demo Organization
- LMN Organization
- QRS Organization
- TUV Organization
- XYZ Organization

Severity: Low [Dropdown] Status: Open [Dropdown]

Assignee: Unassigned [Dropdown] Viewable By: Everyone [Dropdown]

Artifacts [ADD ARTIFACT]

No Artifacts Added

Figure 24

NOTE: The Assignee menu will not populate with any options besides Unassigned until you select an owner, because the assignee must belong to the Organization that owns the Case. Similarly, when you assign a Task in the Case, the Assignee dropdown menu will list only users who are in the Organization that owns the Case.

Viewing a Case

When you view a Case, you will see the Organization that owns the Case at the top left of the screen (Figure 25).

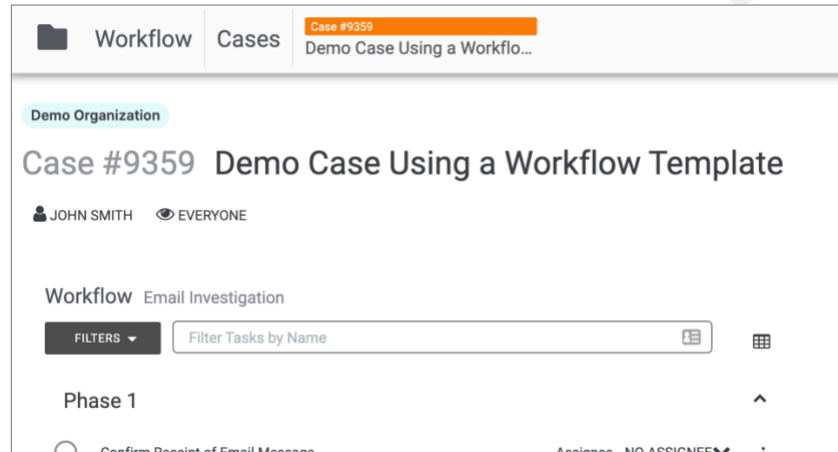


Figure 25

Viewing Artifact Owners

If an Artifact that is a ThreatConnect [Indicator type](#) exists in multiple Organizations on your instance, you can view the Organizations in the dropdown list in the **Summary** column (Figure 26).

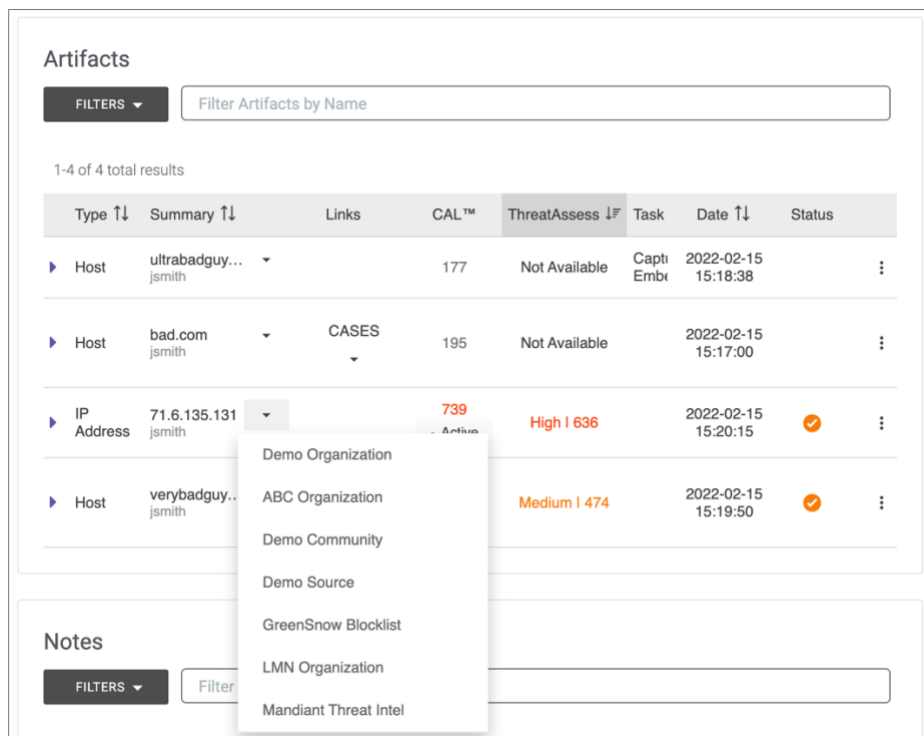


Figure 26

Click on an Organization's name in the list to view a **Details** drawer for the Indicator in that Organization.



Playbooks

The [Playbooks screen](#) will display all [Playbooks](#) in all Organizations on your instance, with the **Organization** column indicating the Organization to which each Playbook belongs (Figure 27).

Type	Name	Organization	Version	Trigger	Labels	Log Level	Updated	ROI
[ABC]	[ABC] Uncover Attacks	ABC Organization	1.0	Attack Pattern		WARN	08-06-21 10:19	⌵ ⋮
[ABC]	Analyst Workbench Endpoint: https://app.threatconnect.com/api/d34alea0-ea26-4q2e-81dc	QRS Organization	1.29	WebHook		WARN	08-11-21 12:38	⌵ ⋮
[ABC]	App Caching	Demo Organization	1.0	UserAction		WARN	03-07-22 17:40	⌵ ⋮
[ABC]	Basic Email Ingest As a starting point for a variety of Use Cases, this Playbook enables the ingestion and processing of basic emails.	TUV Organization	2.6	Custom Trigger	Email ingest Alert Processing	WARN	08-10-21 11:53	⌵ ⋮
[ABC]	Cache Store Training This Playbook will use the cache store that persists for 24 hours to prevent excess calls to CAL. When they are returned, they will be added as Tags to the Indicator in question.	Demo Organization	1.23	-		-	03-23-22 10:34	⋮

Figure 27

You can use the **Organization** dropdown menu along the top of the screen to select the Organizations you want to include in the **Playbooks** table (Figure 28).

Type	Name	Organization	Version	Trigger	Labels	Log Level	Updated	ROI
[ABC]	[ABC] Uncover Attacks	ABC Organization	1.0	Attack Pattern				
[ABC]	Analyst Workbench Endpoint: https://app.threatconnect.com/api/d34alea0-ea26-4q2e-81dc	QRS Organization	1.29	WebHook				

- ABC Organization
- Documentation Team
- LMN Organization
- QRS Organization
- TUV Organization

Figure 28

Creating a Playbook

When creating a new Playbook (including a [Playbook Component](#) or [Workflow Playbook](#)), you must select the Organization that will own the Playbook (Figure 29).



Create Playbook

Name *

Owner *

Select an Owner

Filter Owners by Name

- ABC Organization
- Demo Organization
- LMN Organization
- QRS Organization
- TUV Organization
- XYZ Organization

running workflow logic.

CANCEL SAVE

Figure 29

Importing a Playbook

When importing a Playbook, you must select the Organization that will own the Playbook (Figure 30).

Import Playbook

- Validating Playbook: Create Metrics.pbzx
- Playbook Preview
- 3 Select Owner

Please select the Owner of this Playbook

Select an Owner

Filter Owners by Name

- ABC Organization
- Demo Organization
- LMN Organization
- QRS Organization
- TUV Organization
- XYZ Organization

CANCEL PREV IMPORT

Figure 30



You can easily share a Playbook from one Organization to another by exporting the Playbook, or by [generating a Share Token](#), and then immediately importing it into another Organization.

Viewing a Playbook

When you view a Playbook, you will see the Organization that owns the Playbook at the upper-right corner of the [Playbook Designer](#) (Figure 31).

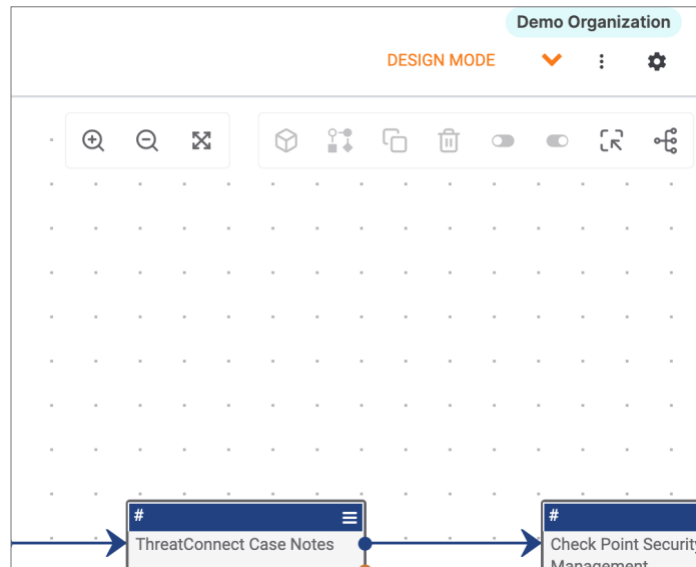


Figure 31

When you are working in a Playbook, the features of that Playbook will be specific to the Organization that owns the Playbook. For example, only the Apps that are available for use in the owning Organization will be available to the Playbook. Similarly, when using the **Run As App** menu option or the [Playbook settings menu option](#) to run an App or Playbook, respectively, as a different user, only users in the owning Organization will be available in those menus.

Playbook Templates

When importing a [Playbook Template](#) as a Playbook, you must select the Organization that will own the Playbook (Figure 32).

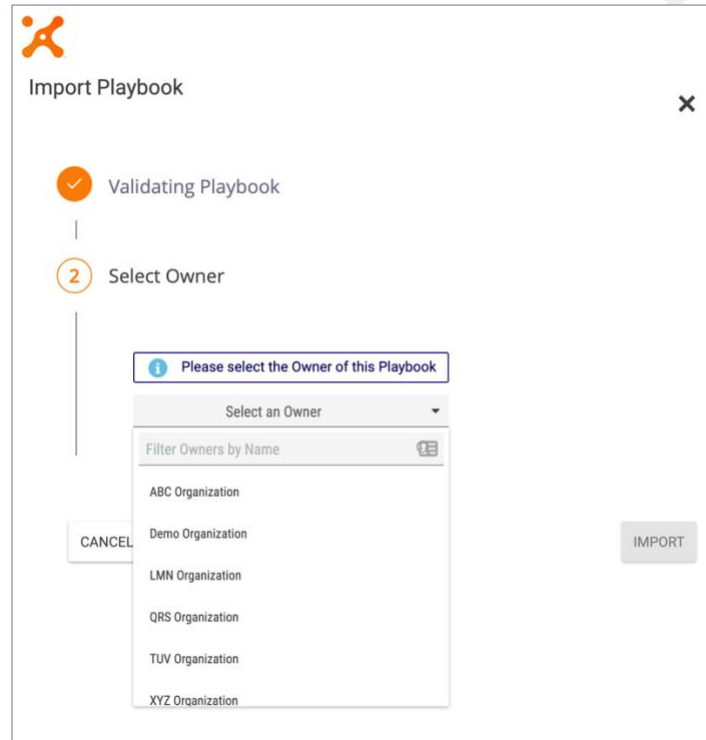


Figure 32




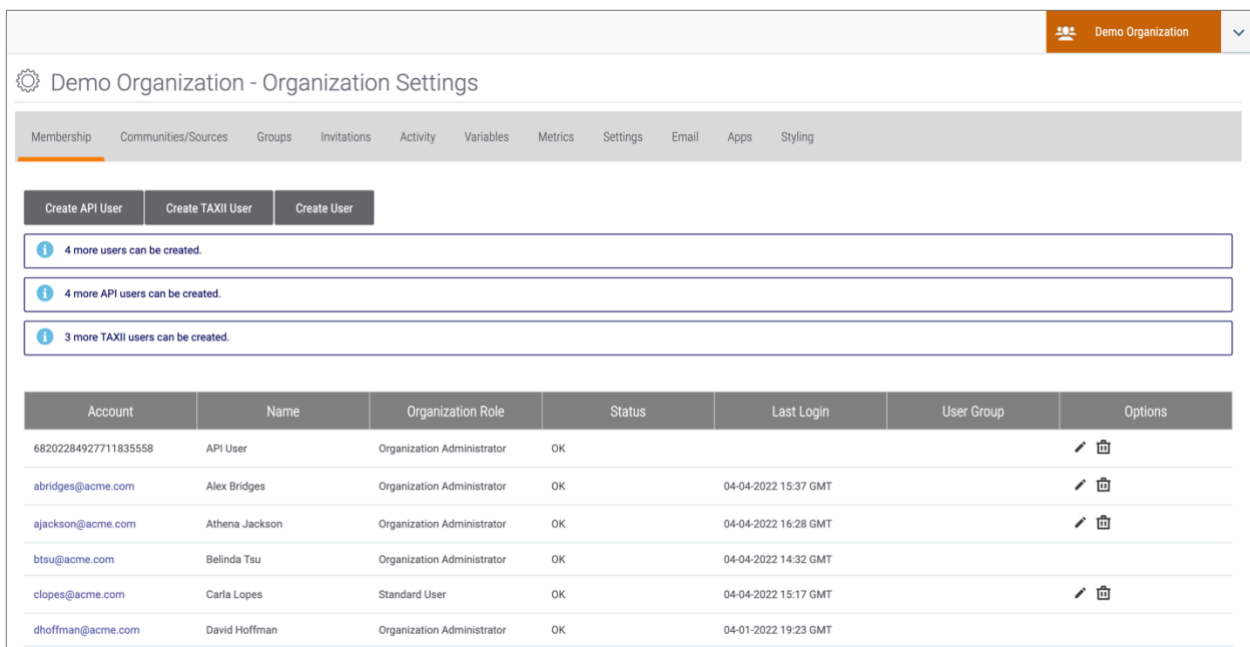
Administration and Configuration of All Organizations

Your Super User account has a [System role](#) of Super User and an [Organization role](#) of Organization Administrator. This combination of roles means that you are an Organization Administrator for every Organization on your ThreatConnect instance, allowing you to view, modify, and manage the **Organization Settings** and **Organization Config** screens for all Organizations. See the *ThreatConnect Organization Administration Guide* for more information on the functionalities and permissions available to Organization Administrators.

Organization Settings

Viewing Organization Settings

When you click the **Org Settings** option in the **Settings**  menu, the **Membership** tab of the **Organization Settings** screen for your home Organization will be displayed (Figure 33).











Account	Name	Organization Role	Status	Last Login	User Group	Options
68202284927711835558	API User	Organization Administrator	OK			 
abridges@acme.com	Alex Bridges	Organization Administrator	OK	04-04-2022 15:37 GMT		 
ajackson@acme.com	Athena Jackson	Organization Administrator	OK	04-04-2022 16:28 GMT		 
btsu@acme.com	Belinda Tsu	Organization Administrator	OK	04-04-2022 14:32 GMT		
clopes@acme.com	Carla Lopes	Standard User	OK	04-04-2022 15:17 GMT		 
dhoffman@acme.com	David Hoffman	Organization Administrator	OK	04-01-2022 19:23 GMT		

Figure 33

You have full access to all tabs of this screen for every Organization on your instance. To view this screen for a different Organization, choose the desired Organization from the selector at the upper-right corner of the screen.

Managing User Accounts

When [creating a user account](#), the System role for the account will automatically be **User**, and you will not have a menu to select a different System role, nor will you be able to view user




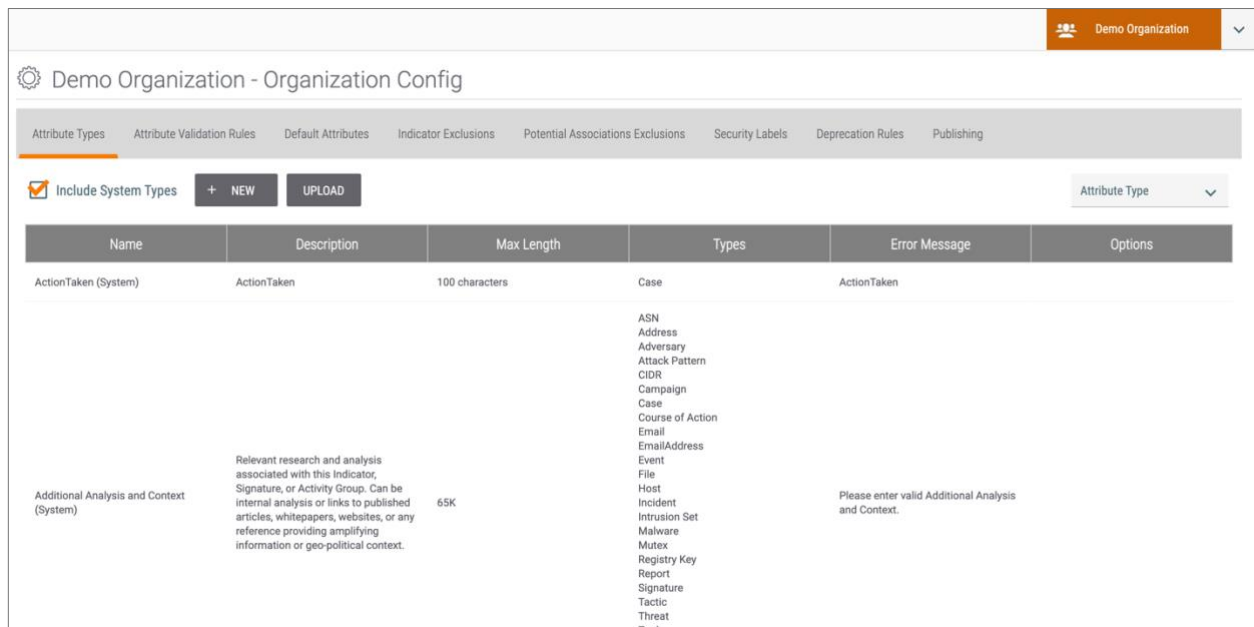
System roles in the table on the **Membership** tab of the **Organization Settings** screen. You also will not be able to modify or delete users with a System role that is higher than yours.

Organization Activity

The **Activity** tab of the **Organization Settings** screen logs all user activity in an Organization. When you perform an activity (e.g., create an Indicator) in an Organization other than your home Organization, other members of that will not see your name as part of the log entry. Instead, the activity will be attributed to your Organization (e.g., **Host bad.com was created by Demo Organization**).

Organization Configuration

When you click the **Org Config** option in the **Settings**  menu, the **Attribute Types** tab of the **Organization Config** screen for your home Organization will be displayed (Figure 34).



Name	Description	Max Length	Types	Error Message	Options
ActionTaken (System)	ActionTaken	100 characters	Case	ActionTaken	
Additional Analysis and Context (System)	Relevant research and analysis associated with this Indicator, Signature, or Activity Group. Can be internal analysis or links to published articles, whitepapers, websites, or any reference providing amplifying information or geo-political context.	65K	ASN Address Adversary Attack Pattern CIDR Campaign Case Course of Action Email EmailAddress Event File Host Incident Intrusion Set Malware Mutex Registry Key Report Signature Tactic Threat Tool	Please enter valid Additional Analysis and Context.	

Figure 34

You have full access to all tabs of this screen for every Organization on your instance. To view this screen for a different Organization, choose the desired Organization from the selector at the upper-right corner of the screen.