ThreatQuotient

ThreatQ User Guide

Version 4.40

Wednesday, July 22, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Last Updated: Thursday, September 10, 2020

Contents

Introduction

The following provides an introduction to the ThreatQ platform.

ThreatQ Introduction

ThreatQ is a cyber threat intelligence platform that focuses on centralizing, structuring, and strengthening a security organization's intelligence-driven defensive posture against attacks.

Concept Overview

The following describes how ThreatQ helps organizations manage threat intelligence, allowing them to defend against sophisticated cyber-attacks.

Threat Library

A central repository combining global and local threat data to provide relevant and contextual intelligence that is customized for your unique environment. Over time, the library becomes more and more tuned to your environment and fills in the intelligence gaps created by different sources, all providing only some pieces of the puzzle.

Adaptive Workbench

An open and extensible work area for security experts across the organization to work within your processes and tools. A customizable workflow and customer-specific enrichment streamlines investigations and analysis, and automates the intelligence life cycle.

Open Exchange

ThreatQ is the only threat intelligence platform specifically designed for customization to meet the requirements of your unique environment. Get more from your existing security investments by integrating your tools, teams and workflows through standard interfaces and an SDK/API for customization.

Navigation Menu

The table below outlines the ThreatQ navigation menu and its related processes.

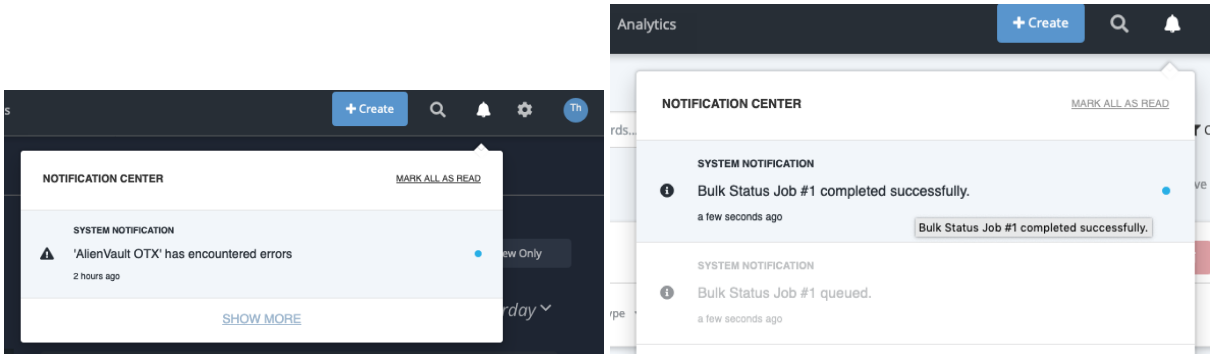
#	Name	Description	References
1	ThreatQ Icon	Clicking on the ThreatQ icon will navigate you back to the home page and dashboard.	N/A
2	Threat Library	Access and search the Threat Library and view system object details.	• Threat Library • Advanced Search • Object Details Page • System Objects
3	Investigations	Navigates to ThreatQ Investigations, a cyber-security situation room that enables col-laborative threat analysis, investigation, and coordinated response.	• ThreatQ Investigations User Guide
4	Analytics	Navigates to the Analytics section which provides a summary view of Adversary, Event, File, Indicator, and Signature Object Types.	• Analytics
5	Create Button	Create system objects.	• Adding Adversaries • Adding

#	Name	Description	References
			Events • Adding Files • Adding an Indicator • Parsing for an Indicator • Adding a Signature • Adding a Yara Signature
6	Search Icon	Perform a basic search for a system object or perform an Indicator Search.	• Search • Indicator Search
7	Message Center Icon	Receive in-app notifications of system job processes such as Bulk Actions. Administrator and Maintenance account users will also receive feed health notifications.	• Notification Center
8	Site Settings	Configure site settings such as user management, incoming feeds, TLP etc.	• User Management • Incoming Feeds Overview

#	Name	Description	References
			• Exports Overview • Operations Overview • Reports Overview • Licensing Overview
9	User Icon	Access your user profile.	• Managing your User Account

Notification Center

The Notification Center alerts you, via an in-app notification icon, when a Bulk Action job has been queued and/or completed. Administrator and maintenance accounts will also receive feed health notifications via the Notification Center. The icon is located on the navigation menu for the application. This allows you to monitor system processes while working within ThreatQ.



Related Topics:

- Bulk Actions
- Feed Health Notifications

System Access

The following describes how to log in and log out of the platform.

System Access Overview

To access the ThreatQ web UI, you must authenticate yourself with a username and password. You can use the main menu to access ThreatQ functionality.

Authentication Methods

There are three authentication methods that can used to access your ThreatQ platform:

Method	Description	Reference
Local Authentication	User accounts are created and maintained manually within in the platform. Username, passwords, and permission roles are configured within ThreatQ. Administrators can edit a user's profile including email, password, and permission role in ThreatQ. Local users will log in using the local user login	• User Management Overview

Method	Description	Reference
	method for the ThreatQ platform - see the Logging into ThreatQ topic.	
LDAP Authentication	User accounts are created and authenticated outside of the ThreatQ platform and user roles are mapped from the user's Active Directory. Due to this nature, user accounts cannot be modified within the ThreatQ platform (User Management page). LDAP users will log in using the local user login option for the ThreatQ platform - see the Logging into ThreatQ topic.	• LDAP Authentication
SAML Authentication	User accounts are created and authenticated outside of the ThreatQ platform and user roles are mapped from the user's Active Directory. Due to this nature, user accounts cannot be modified within the ThreatQ platform (User Management page). SAML does not allow user role mapping for maintenance accounts. SAML users will log in using the single sign-on (SSO) login option for the ThreatQ platform - see the Logging into ThreatQ topic.	• SAML Authentication

Transitioning Authentication Methods

The following scenarios will detail how authentication methods can be transitioned in the ThreatQ platform.

Current Method	New Method	Details
Local	SAML	Current ThreatQ accounts will be mapped using the user's email address and users will use SSO to log into the platform - see Logging into ThreatQ Local Maintenance Accounts will not be mapped in SAML and will continue to use the local login method. See the Configuring SAML topic for details on this setup process. ThreatQuotient strongly recommends that you perform a full backup before changing your authentication method.
SAML	Local	Contact ThreatQ Support.
Local	LDAP	Current ThreatQ accounts will be mapped using the user's email address and users will continue to use the local login method - see Logging into ThreatQ See the LDAP Authentication topic for details on this setup process. ThreatQuotient strongly recommends that you perform a full backup before changing your authentication method.
LDAP	Local	Contact ThreatQ Support.
LDAP	SAML	LDAP must be disabled before enabling SAML. No account updates are required if the unique account identifier for LDAP was the user's email address. The LDAP group that is mapped to the

Current Method	New Method	Details
		ThreatQ Maintenance role will have to be mapped to different user role as SAML does not allow maintenance account mapping.
SAML	LDAP	SAML must be disabled before enabling LDAP. No account updates are required if the unique account identifier for SAML was the user's email address.

System Login

When you installed ThreatQ, you set up the default user account, *Maintenance Account*, which you can use to log into the web UI.

Using this account, you can create additional user accounts.

Passwords must be 15 characters or longer. There is no limit on the character type.

Related Topics:

- Logging into ThreatQ
- Session Timeout

Logging into ThreatQ

When you installed ThreatQ, you defined an IP address for the web UI, and set up the *Maintenance Account* and password.

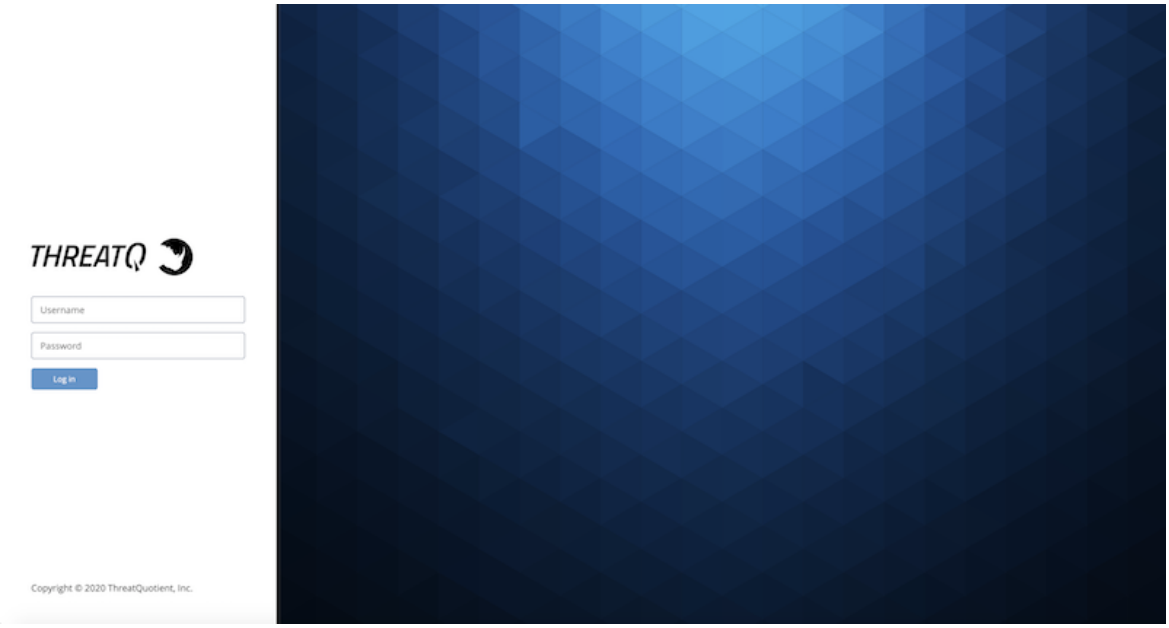
There are two methods that can be used to log into your ThreatQ instance:

- Local Log In
- Single Sign-On (SSO)

Local Log In

User accounts using local authentication and LDAP will log in using this method.

1. Navigate to your ThreatQ instance - `https://your-ThreatQ-web-ip-address`.



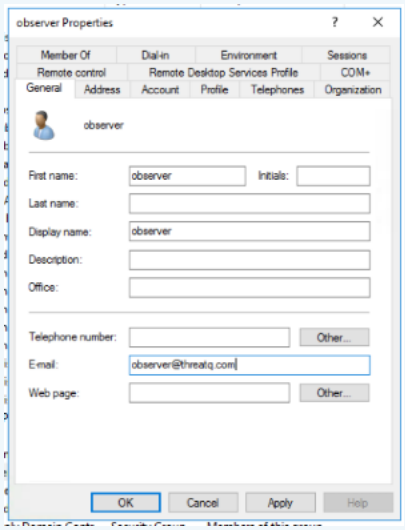
2. Enter your username (email address) and password.
3. Optionally, if you have 2-step verification enabled, complete the following steps:
   - Enter your verification code from Google Authenticator.
   - Optionally, choose to **Remember this computer for 30 days**.
4. Click **Login** or **Submit**.

Single Sign-On (SSO)

Users using SAML authentication will use this log in method.

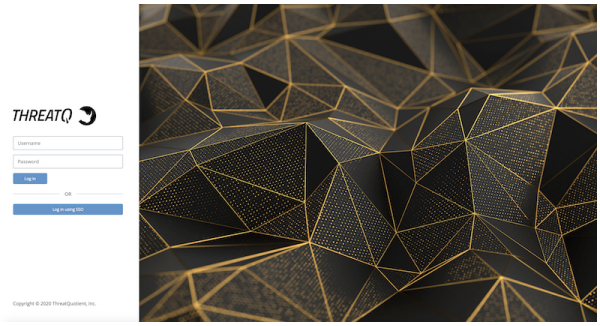
SAML users are required to add their email address to their user profiles in order to use the SSO. As part of the integration process, the ThreatQ platform expects that the user's email address has already been added to their IdP. See the Setting up LDAP Users/Groups for SAML topic for

more details.



1. Navigate to your ThreatQ instance - `https://your-ThreatQ-web-ip-address`.

   If SAML is enabled, you will see a Single Sign-On option.



2. Click on **Log in Using SSO**.

   You will navigate to your third-party authenticated site to log in. Once that has been completed, you will be automatically sent back to the ThreatQ instance.

Session Timeout

User sessions time out after 60 minutes of inactivity. Users with administrator and maintenance roles can update this setting or, disable session timeouts for that specific user, by

viewing the user's account profile. See the Editing a User topic for more details.

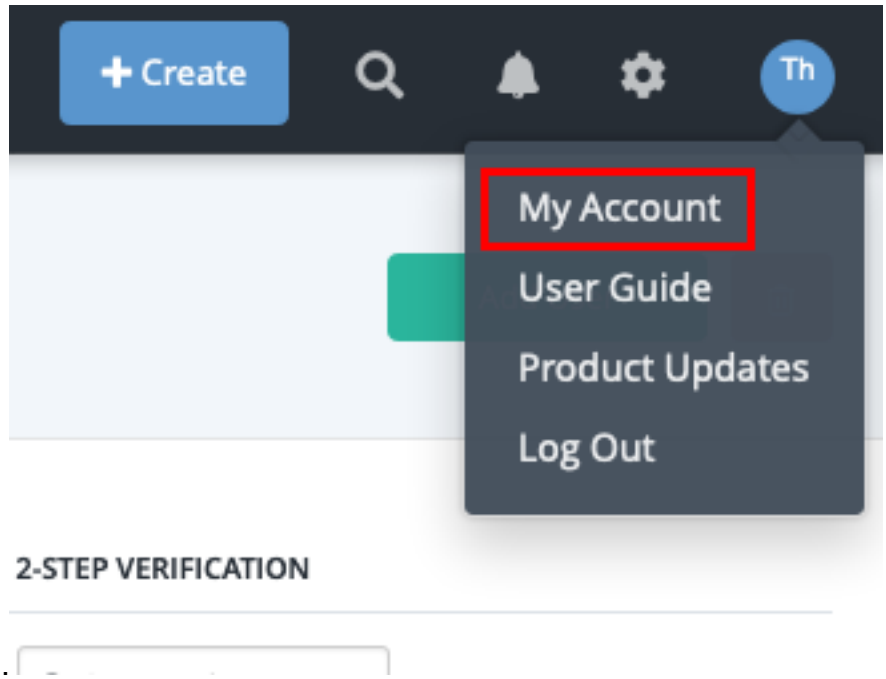
The initial account created when installing ThreatQ does not have a set session time by default. This setting can be updated as well from the user profile account.

Managing your User Account

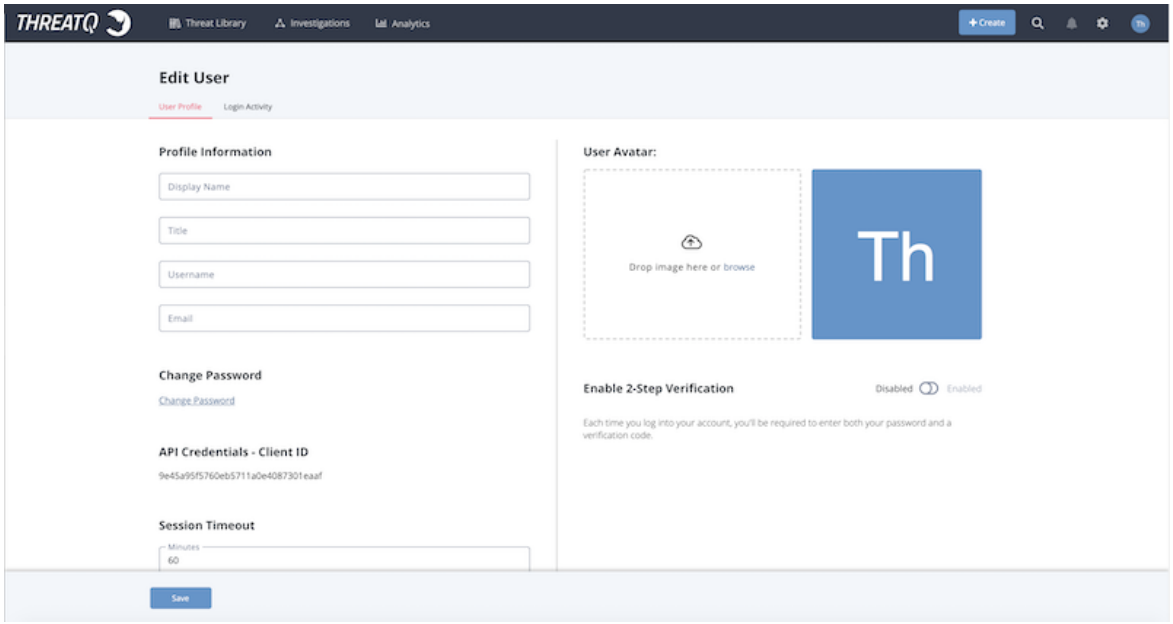
When you click on your **User Avatar** and select **My Account**, the system directs you to the Edit User page for your current login. From here, you can edit your user account, set up 2-step verification, view your API credentials, or view your login history.

Procedure

1. Click on your user avatar icon, located at the top-right of the screen, and select **My Account**



The User Profile page loads.

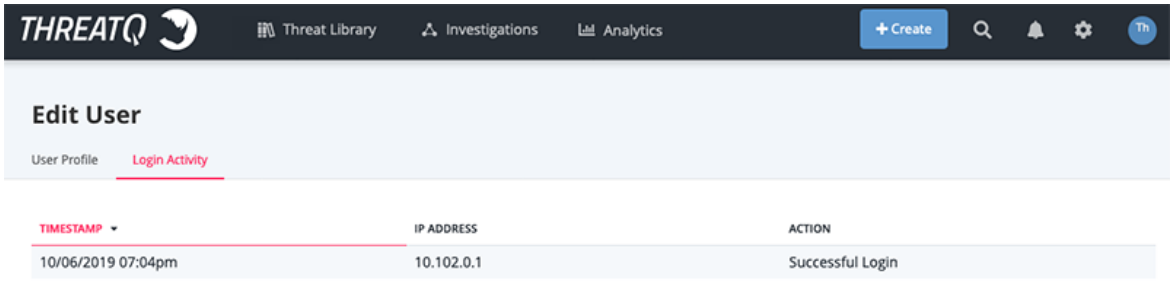


2. On the User Profile tab, you can view and/or edit the following settings of your user account:

Field	Description
Display Name	You can update your name.
Title	You can update your job title.
Username	You can update your username.
Email	You can update your email address.
Password	You can click on the **Change Password** link to update your password.
API Credentials	You can view your API credentials, a unique Client ID, which will allow you to connect with ThreatQ's API.
Session Timeout	You can update or disable your session timeouts.

Field	Description
User Avatar	You can update your user avatar; see Update User Avatar for more details.
2-Step Verification	Optionally, you can set up 2-step verification; see 2 Step Verification for more details.

3. Optionally, you can click on the **Login Activity** tab to view:



   - The last date and time you logged in.
   - The IP Address where you logged in.
   - Whether the login was successful or not.

4. Click **Save**.

User Avatar Icons

User avatar icons provide a personalized look to your ThreatQ dashboard. Clicking on the avatar icon will reveal the **My Account** and **Log out** options.

Users can update their avatars by clicking on the avatar and selecting **My Account**.

- Update User Avatar Graphic

Update User Avatar Graphic

1. Click on avatar icon located to the top-right on the screen and select **My Account**.

   The *Edit User* form will load.

2. Select one of two options:
   - Click **browse** and select the icon graphic to upload.
   - Click and drag the new icon graphic onto the page.
3. Click **Save** at the bottom of the page.

2 Step Verification

When you enable 2-Step Verification (also known as two-factor authentication), you add an extra layer of security to your account. After 2-Step Verification is active, you sign in with your password and a code sent to your mobile device.

The 2-Step Verification option is not available for users using SAML Authentication and the Single Sign-On (SSO) process.

- Enabling 2 Step Verification

Enabling 2 Step Verification

Procedure:

1. Choose the **User Settings icon> My Account**.
2. Under Enable 2-Step Verification, click **Enabled**.
3. In the Enable 2 Step Verification dialog box, complete the following:
   - Scan the qr code using your Google Authenticator mobile app.
   - Enter the validation code delivered to your mobile device via Google

Authenticator.

- Click **Submit**.

4. Click **Save**.

What to do next

The next time you log in, you must use the newest verification code.

Licensing

The following provides an overview of licensing for the ThreatQ platform.

Licensing Overview

Your ThreatQ deployment requires a license to initialize the platform. ThreatQ Support provides the initial license and any subsequent licenses provided to maintain the platform. You apply the initial ThreatQ license during first boot, as described in the ThreatQ Getting Started Guide. Any subsequent license updates can be applied in the ThreatQ user interface.

Viewing the License Status

ThreatQ licenses are not perpetual. To view the license expiration date, complete the following steps:

Procedure

Choose the **Settings icon >About** .

Updating a License

If you receive a new license from Support, apply the new license by accessing the About page.

Procedure

1. Choose the **Settings icon > About**.
2. Choose **Update License**.
3. Enter the new license key.
4. Click **Submit**.

User Management

The following describes how to manage user accounts.

User Management Overview

ThreatQ uses role-based access control to manage user accounts. The system provides several user roles, each containing a set of permissions for accessing system functionality. You create user accounts, and assign them to a user role. The user role determines each account's set of permissions.

After you create a user account, you can modify the user role group, full name, and email address.

User Roles

The following details the user roles and their associated permissions.

User Role	Permissions
Maintenance Account	Members have access to the entire ThreatQ user interface and can edit all data. **Important Notes:**

User Role	Permissions
	• The initial local Maintenance Account, created when installing ThreatQ, can not be deleted • Local Maintenance Accounts (manually created within ThreatQ) cannot be migrated to SAML authentication groups.
Administrative Access	Members have access to the entire ThreatQ user interface and can edit all data.
Primary Contributor Access	Members have access to most of the ThreatQ user interface, except for: • User Management • Incoming Feeds • Exports • OAuth Management • System Configurations Members can edit: • Their own user info • Whitelist Management • Operations Management • Object meta data

User Role	Permissions
	• Saved Searches
Read Only Access	Members have access to most of the ThreatQ user interface, except for: • User Management • Incoming Feeds • Indicator Management • Whitelist Management • Exports • Operations Management • OAuth Management • System Configurations Members cannot edit any data. Members can export search results.

User Account Creation

When you first install ThreatQ, the system creates a default user account, the Maintenance Account. You cannot delete this account, and you can use it to initially create other user accounts. Each user account must have a unique username.

Only the Maintenance Account and Administrative Access user role have permissions to access user management functionality. You can only create new user accounts if logged in as one of these roles.

User Account Properties

Property	Description	Validation
Display Name	full name of the user associated with this account	any alphabetic character and spaces
Title	optional user title	any alphabetic character and spaces
Group	roles which this user account belongs to	at least one role selected
Username	username associated with this account	any alphabetic character and spaces
Email	email address associated with this account	valid email address, such as user-@domain.com
Password	initial password associated with the username	all characters

Adding a User

1. From the main menu, choose the **Settings icon > User Manangement**.
2. Click **Add User**.
3. Enter the user's **Display Name**.
4. Optionally, enter the user's **Title**.

5. Select the level of access for the user from the **Group** drop-down menu.

   Choose from the following options:

   - Maintenance Account
   - Administrative Access
   - Primary Contributor Access
   - Read Only Access
6. Enter the user's **Username**.
7. Enter the user's **Email** address.
8. Enter a password for the user.
9. Retype the password.
10. Click **Add User**.

User Account Modification

After you create a user account, you can modify the account's display name, title, role group, username, email address, and password.

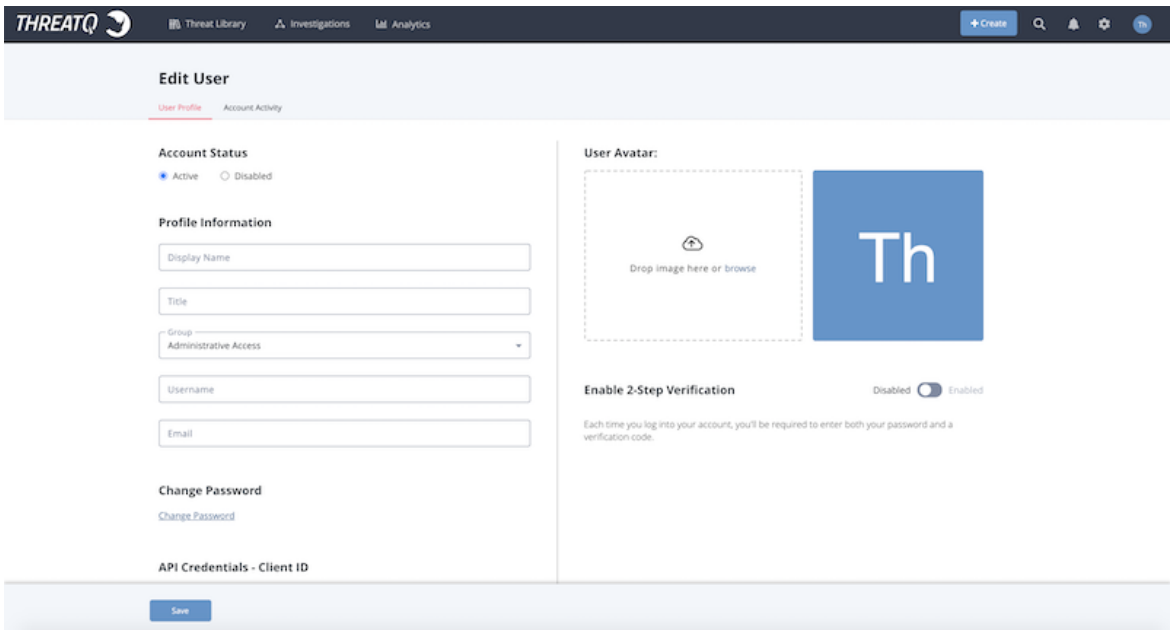
- Editing a User
- Resetting User Passwords from the Command Line
- Deleting a User

Editing a User

You cannot edit the user details for SAML nor LDAP users from the User Management page.

1. From the main menu, choose the **Settings icon > User Management**.
2. Click the name of the user whose profile you wish to edit.

   The User Profile page loads.

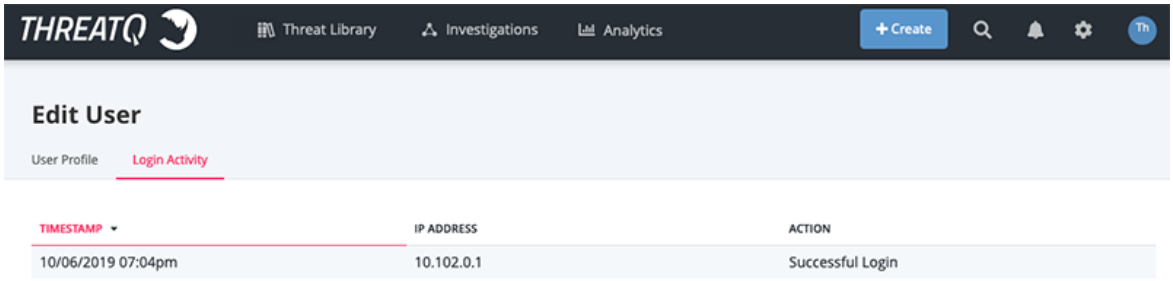


3. On the User Profile tab, you can view and/or edit the following settings:

Field	Description
Account Status	You can update a user's account. Select either: • **Active** • **Disabled** If the user's account is locked, you will see a third option for **Locked**. Selecting **Active** resets the user's account.
Display Name	You can update the user's name.
Title	You can update the user's job title.
Group	You can update the user's role group.

Field	Description
Username	You can update the user's username.
Email	You can update the user's email address.
Password	You can click on the **Change Password** link to update the user's password.
API Credentials	You can view the user's API credentials, a unique Client ID, which will allow him/her to connect with ThreatQ's API.
Session Timeout	You can update or disable the user's session timeouts.
User Avatar	You can update the user's user avatar; see Update User Avatar for more details.
2-Step Verification	Optionally, you can disable 2-step verification; see 2 Step Verification for more details.

4. Optionally, you can click on the **Login Activity** tab to view:



   - The last date and time the user logged in.
   - The IP Address where the user logged in.
   - Whether the login was successful or not.

5. Click **Save**.

Resetting User Passwords from the Command Line

You cannot reset a SAML nor LDAP user's password from the command line.

If you have root access to your ThreatQ installation, you can reset any user's password from the command line.

1. SSH to your ThreatQ installation as root.
2. Navigate to the api directory:

```
cd /var/www/api
```

3. Run the following command:

```
php artisan threatq:password-reset
```

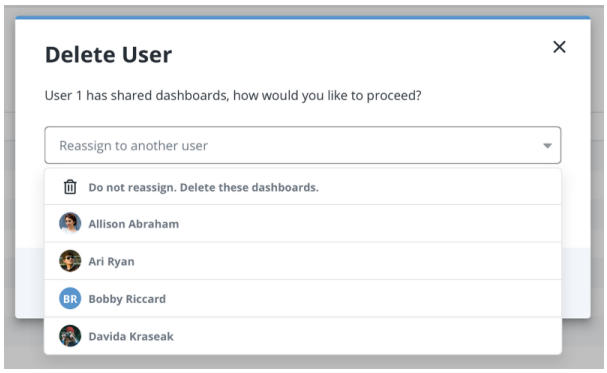
4. At the prompt, enter the email address for the user whose password you are resetting.
5. At the prompt, enter the new password.
6. At the prompt, re-enter the new password to confirm.

Deleting a User

Deleting a user cannot be undone.

1. From the main menu, choose the **Settings icon > User Management**.
2. Select the user(s) you wish to delete.
3. Click the **Delete** icon.

4. Confirm the deletion when prompted. If the user has any shared custom dashboards, select whether to delete the dashboards or reassign them to another user.



5. Click **Delete User**.

System Configurations

The following describes how to manage various system configurations in ThreatQ.

- Indicator Statuses
- Indicator Types
- Event Types
- Proxy
- Account Security
- LDAP Authentication
- SAML Authentication
- Date and Time Format

Indicator Statuses

Indicator Statuses page allows you to view, duplicate, add, edit, and delete available system-wide indicator statuses. You cannot edit nor delete indicator statuses provided by ThreatQ (Active, Expired, Indirect, Review, Whitelisted), but you can add, edit, and delete your own custom statuses.

Enabling the **Protect from Feed Override** option for a status, via the toggle switch, will prevent feeds from automatically updating the status of indicators. This can be useful for indicators with a specific status, such as **Whitelisted**, which you may want to prevent from being automatically updated to Active by a feed.

Related Topics:

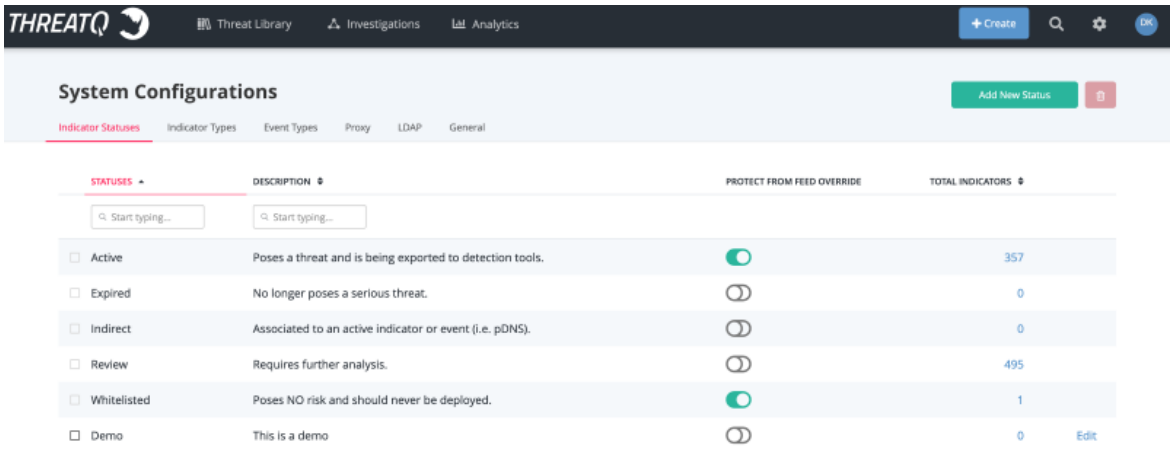
Viewing Indicator Statuses

To view existing indicator statuses, complete the following procedure.

Procedure:

1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



   Statuses found within ThreatQ are listed by status, number, and description within the Indicator Statuses table.

2. Optionally, to sort the table by a column, click the column header. To reverse the column sorting order, click the header a second time.

Indicator Statuses Table Functions:

Function	Description
Change the number of entries displayed in the table.	1. Click the dropdown menu at the top right of the table and select the desired option.
Sort the table by a column.	1. Click the column header. 2. To reverse the column sorting order, click the header a second time

Indirect Indicator Status

For feeds that set multiple statuses, A status of *Indirect* is assigned to indicators that meet the following criteria:

- Indicators created from the relations array are imported with a status of *Indirect*.
- If an indicator already exists, its original status value will remain the same. However, if the status is *Indirect*, and it is received as a parent indicator, its value will be updated as defined in the connector configuration.

Currently, this status only applies to CrowdStrike and iSight feeds, where:

- For CrowdStrike, *Indirect* indicates that ThreatQ received the indicator from the relations list for the parent indicator.
- For iSight Partners, *Indirect* indicates that ThreatQ received an indicator that does not have an attribute of *Attack* or *Compromised*.

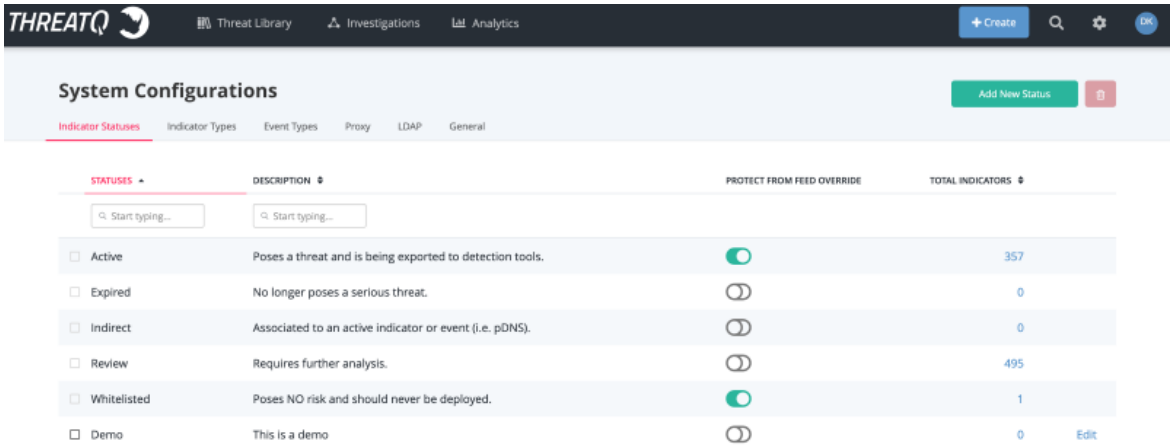
Adding an Indicator Status

To add an indicator status that can be applied to any system indicator, complete the following procedure.

Procedure:

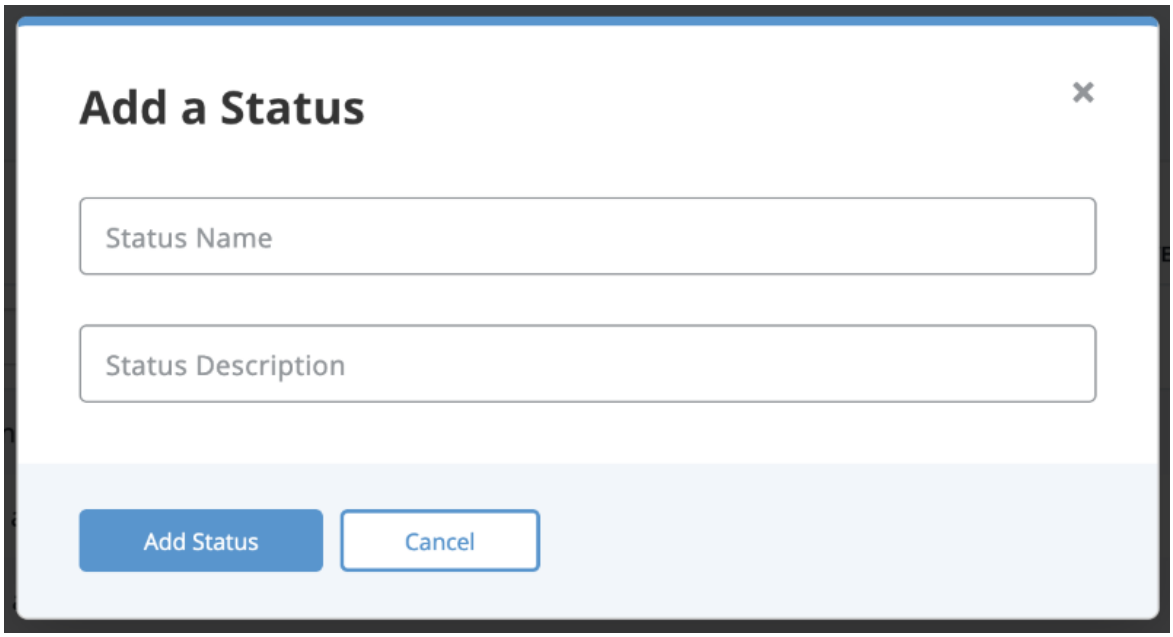
1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



2. Click **Add New Status**.

   The Add a Status dialog box opens.



3. Enter a **Status Name**.
4. Optionally, enter a **Status Description**.
5. Click **Add Status**.

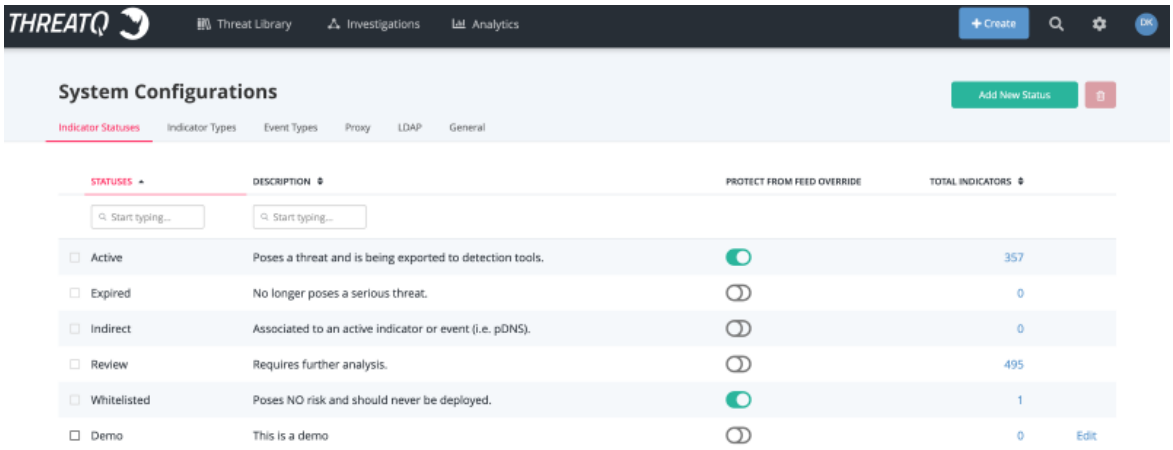
Editing an Indicator Status

To edit an existing indicator status, complete the following procedure. You cannot edit indicator statuses provided by ThreatQ.

Procedure:

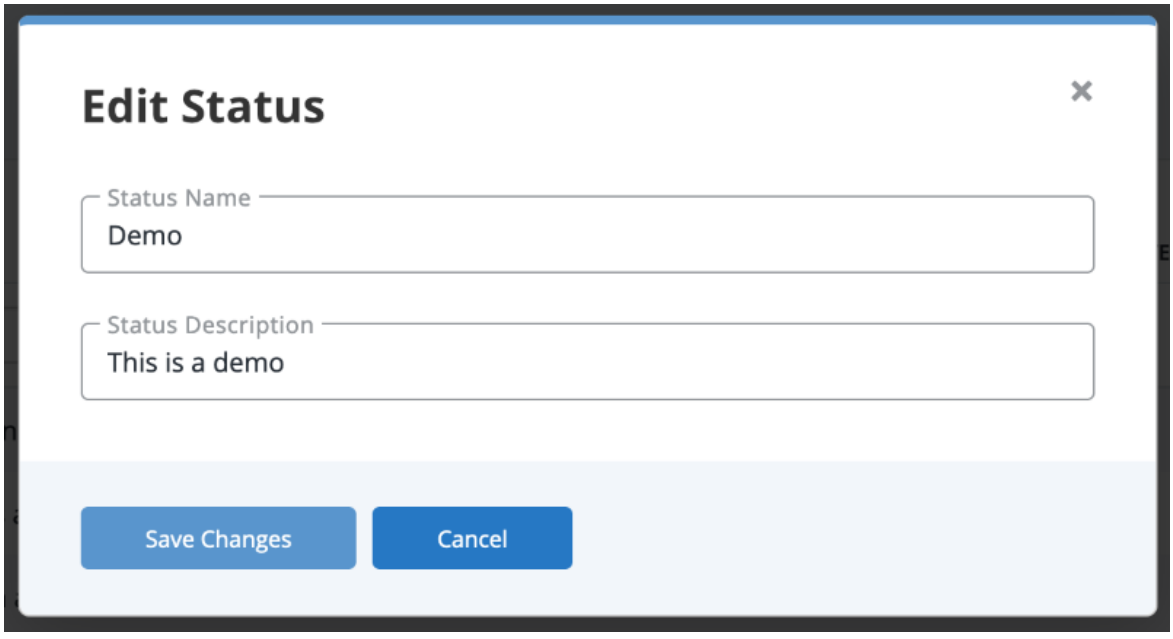
1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



2. Determine the indicator you want to edit and click **Edit** in the far right column.

   The Edit Status dialog box opens.



3. Optionally, enter a new **Status Name**.
4. Optionally, enter a new **Status Description**.

5. Click **Save Changes**.

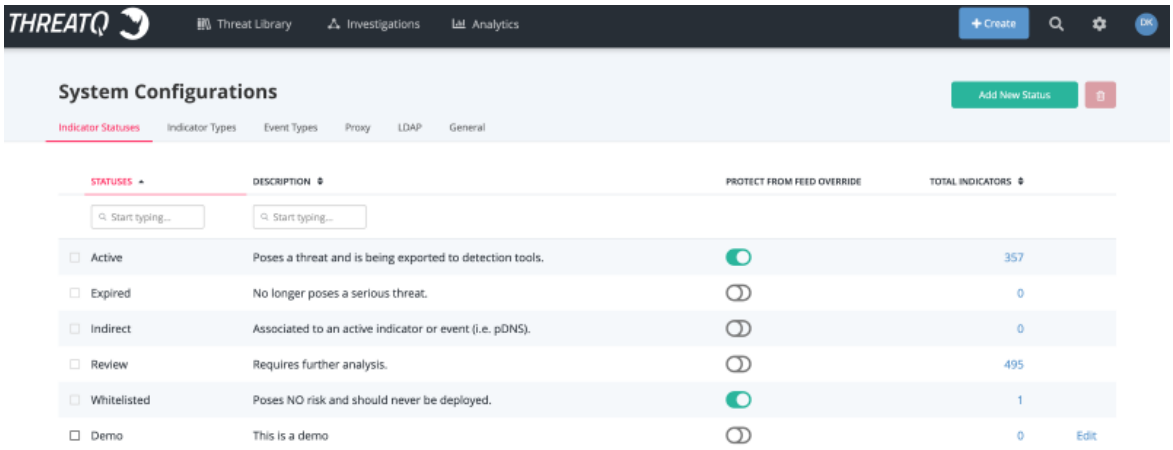
Deleting an Indicator Status

To delete an indicator status, complete the following procedure. You cannot edit and delete indicator statuses provided by ThreatQ. Custom statuses can only be deleted if there are no indicators using that status.

Procedure:

1. Navigate to **Settings** > **System Configurations**.

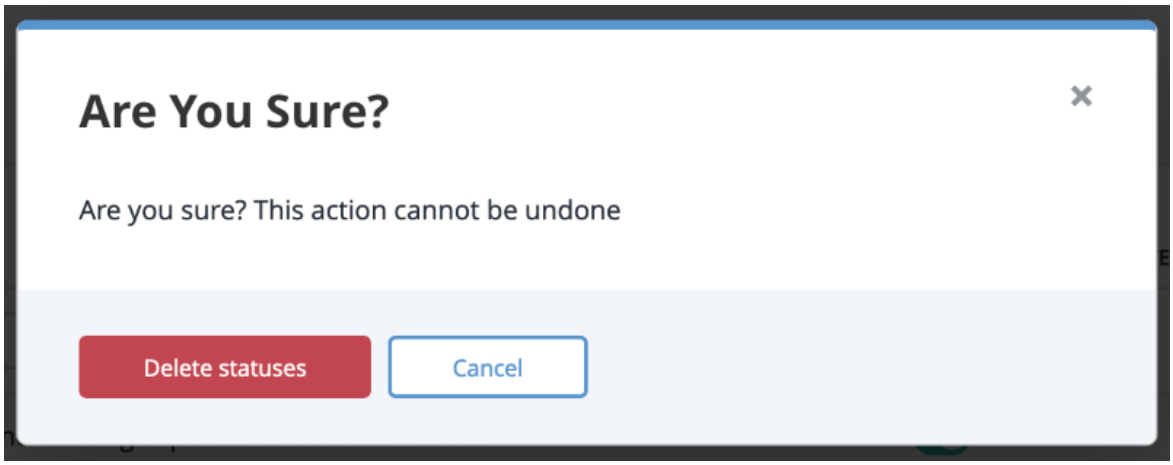
   The System Configurations page opens to the Indicator Statuses tab.



2. Determine the indicator you want to delete and select the corresponding checkbox in the first column.

3. Click the **Delete icon** in the upper right hand corner.

   A confirmation dialog box appears.



4. Click **Delete Statuses**.

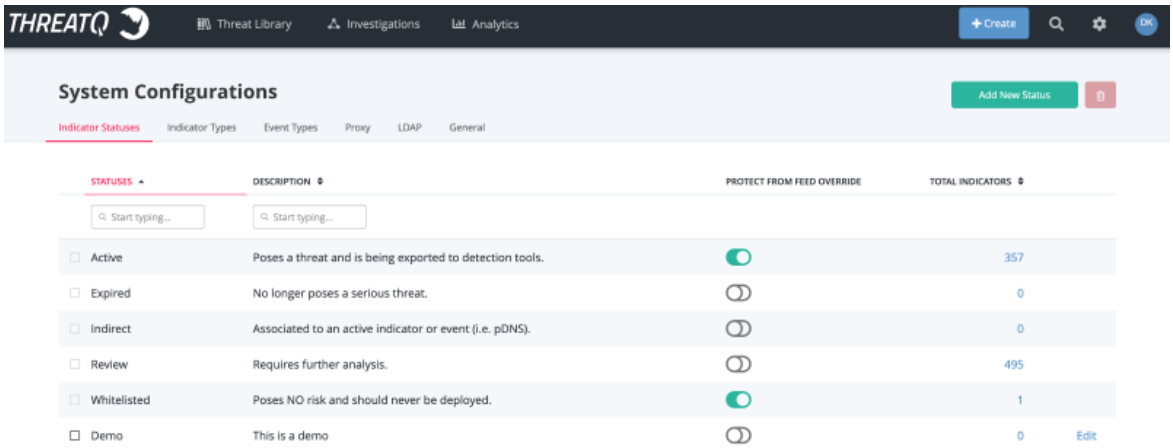
Indicator Types

The Indicator Types table allows you to view a list of indicator types found in ThreatQ and the total number of indicators associated with each type.

To view Indicator Types found within ThreatQ:

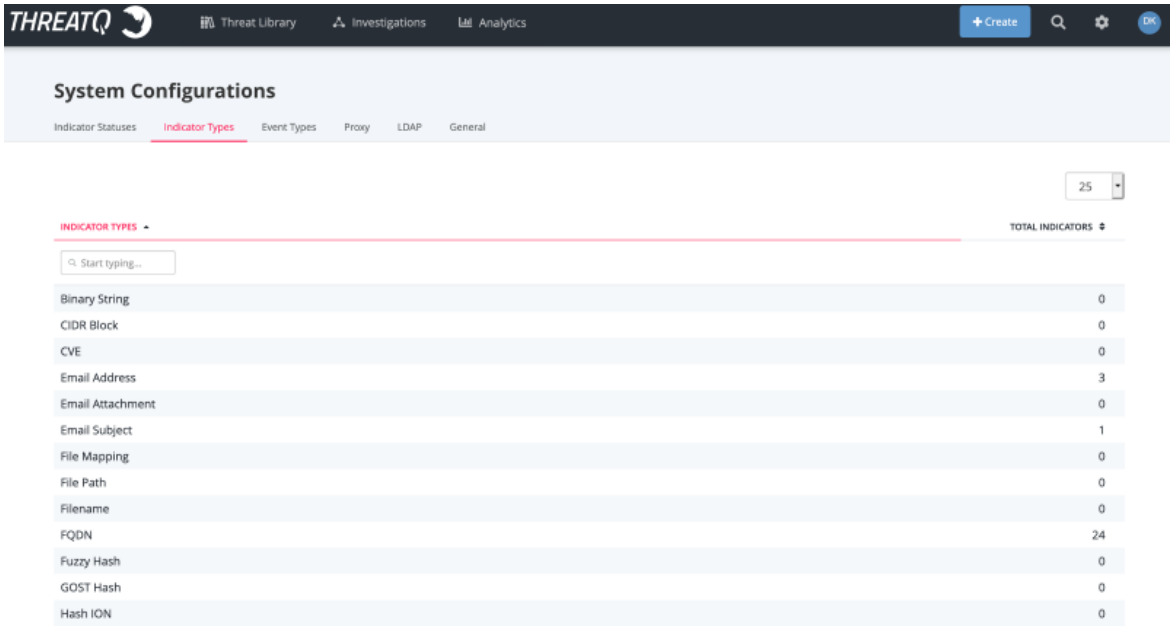
1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens.



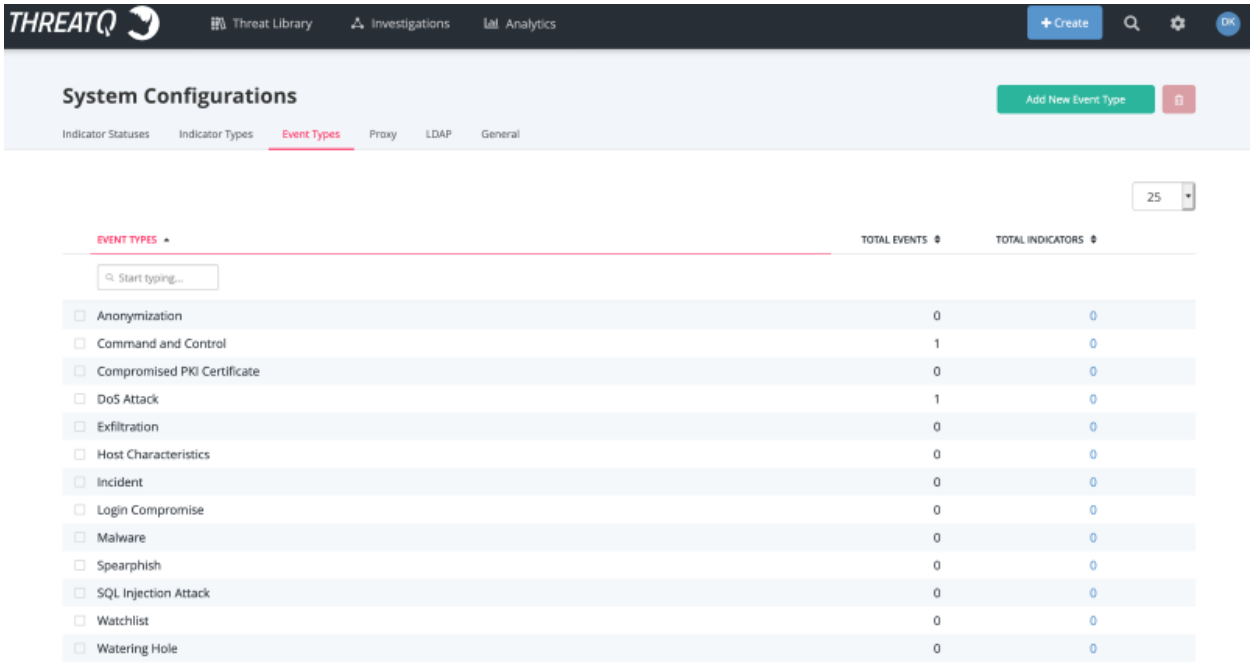
2. Click the **Indicator Types** tab.

   The Indicator Types tab opens.



Event Types

The Event Types page allows you to view, add, edit, and delete system events.



Event Types provided by ThreatQ cannot be edited or deleted, but you can add, edit, and delete your own custom event types.

System provided Event Types include:

- Anonymization
- Command and Control
- Compromised PKI Certificate
- DoS Attack
- Exfiltration
- Host Characteristics
- Incident
- Login Compromise
- Malware
- Sighting
- Spearphish
- SQL Injection
- Attack
- Watchlist
- Watering Hole

Related Topics:

- Viewing Event Types
- Editing an Event Type
- Editing an Event Type
- Deleting an Event Type

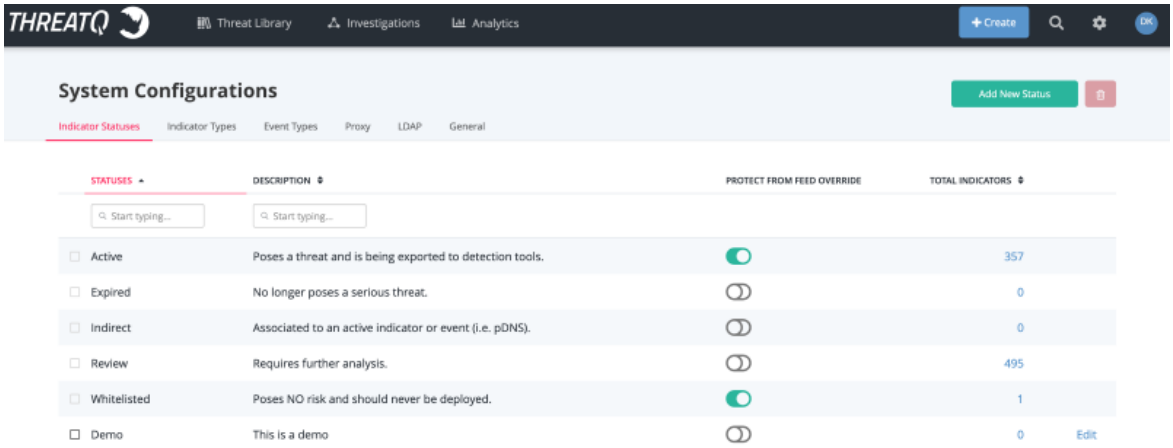
Viewing Event Types

To view existing event types, complete the following procedure.

To view Event Types found withing ThreatQ:

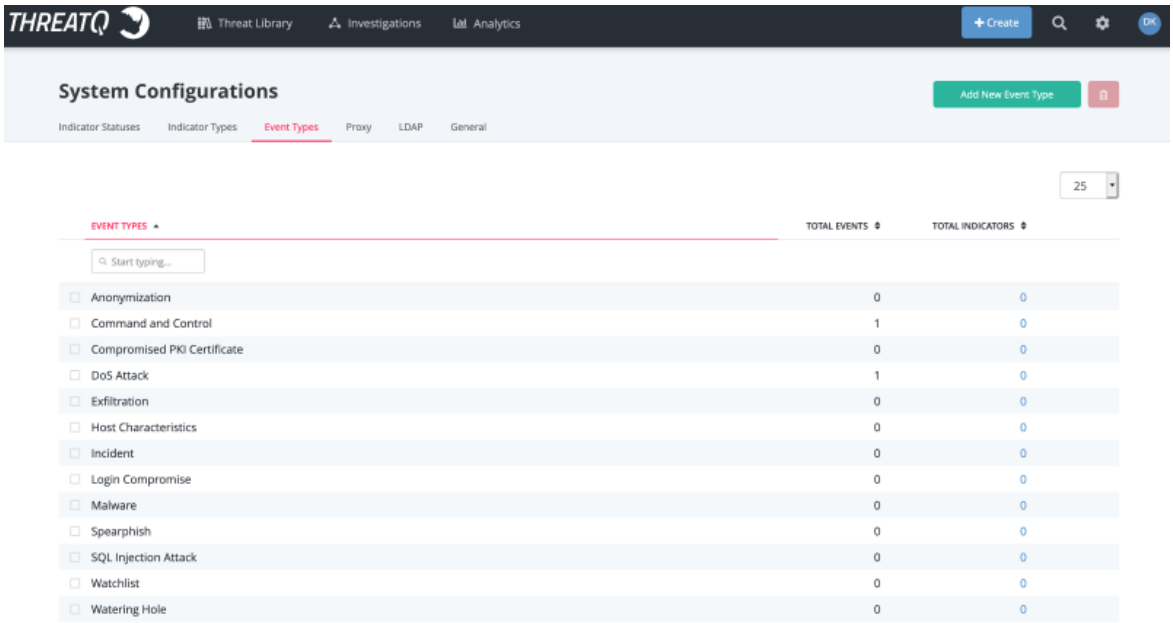
1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens.



2. Click the **Event Types** tab.

   The Event Types tab opens.



Event Types Table Functions:

Function	Description
Changing the number of entries displayed in the table	1. Click the dropdown menu at the top right of the table and select the desired option.
Sorting the table by a column	1. Click the column header. 2. To reverse the column sorting order, click the header a second time.

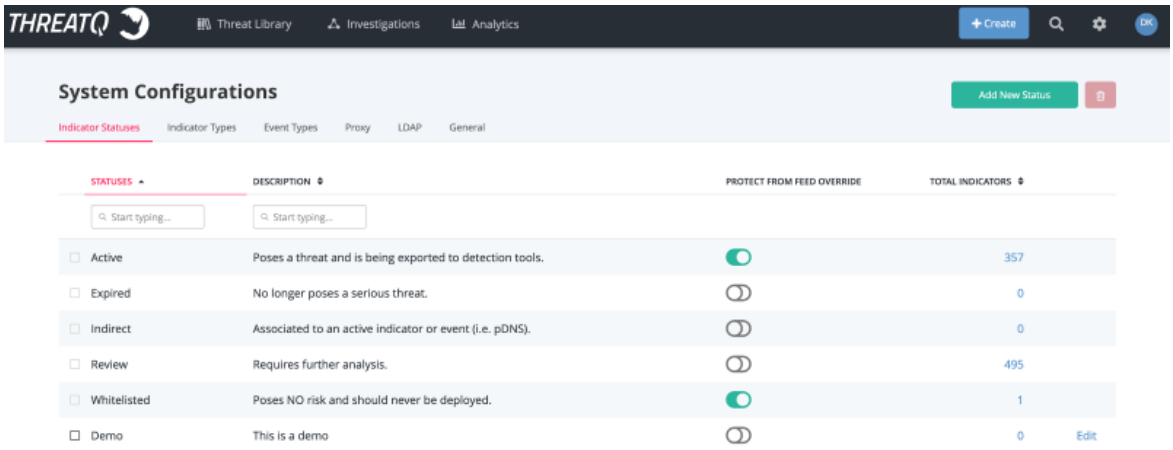
Adding an Event Type

To add an Event Type, complete the following procedure.

Procedure:

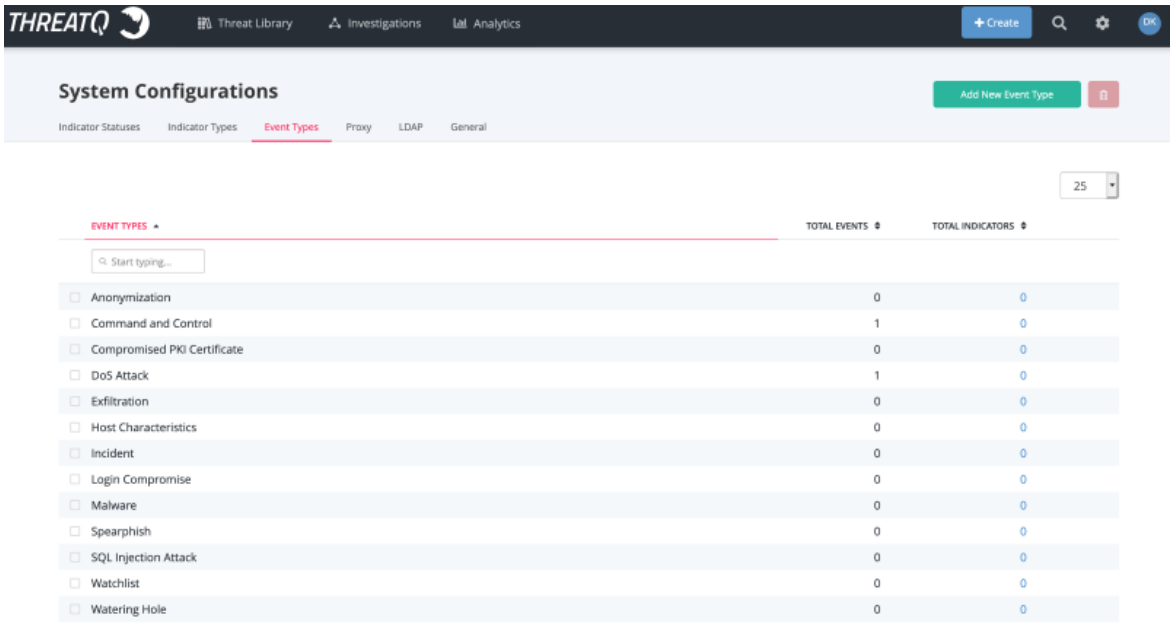
1. From the main menu, select **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



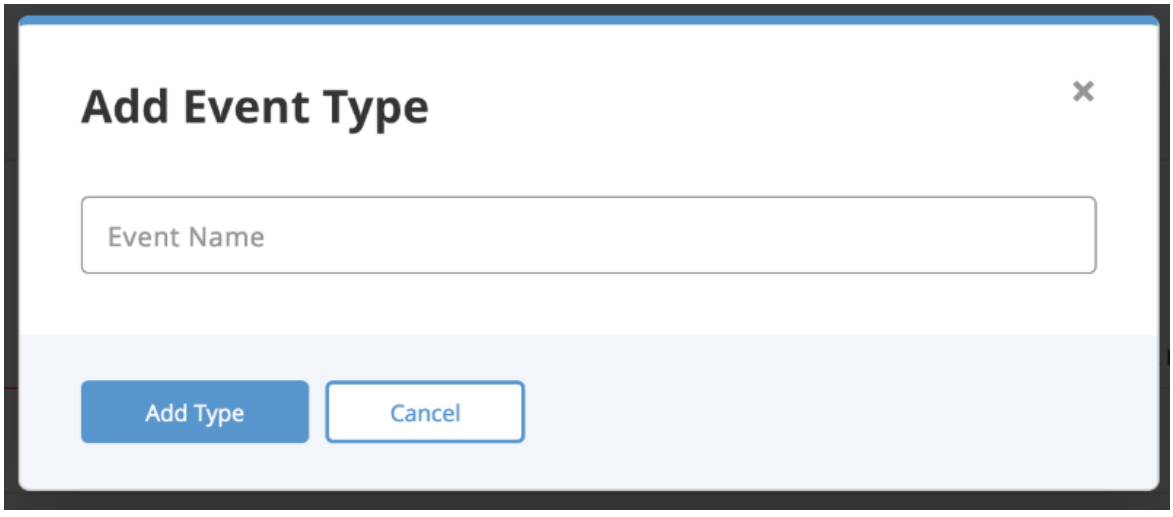
2. Click the **Event Types** tab.

   The Event Types tab opens.



3. Click **Add New Event Type**.

   The Add Event Type dialog box opens.



4. Enter a **Event Name**.
5. Click **Add Type**.

Editing an Event Type

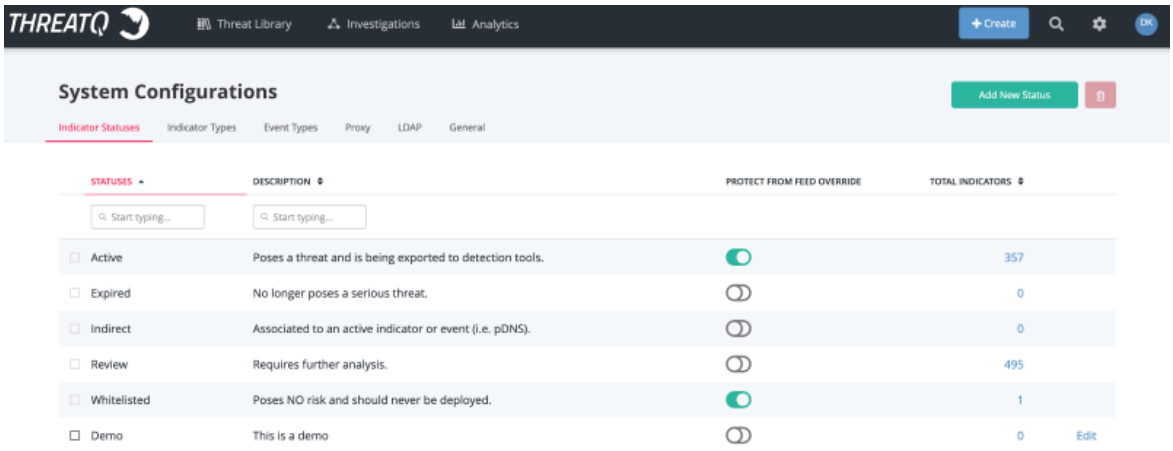
To edit a user-generated Event Type, complete the following procedure.

> You cannot edit an Event Type provided by ThreatQ.

Procedure:

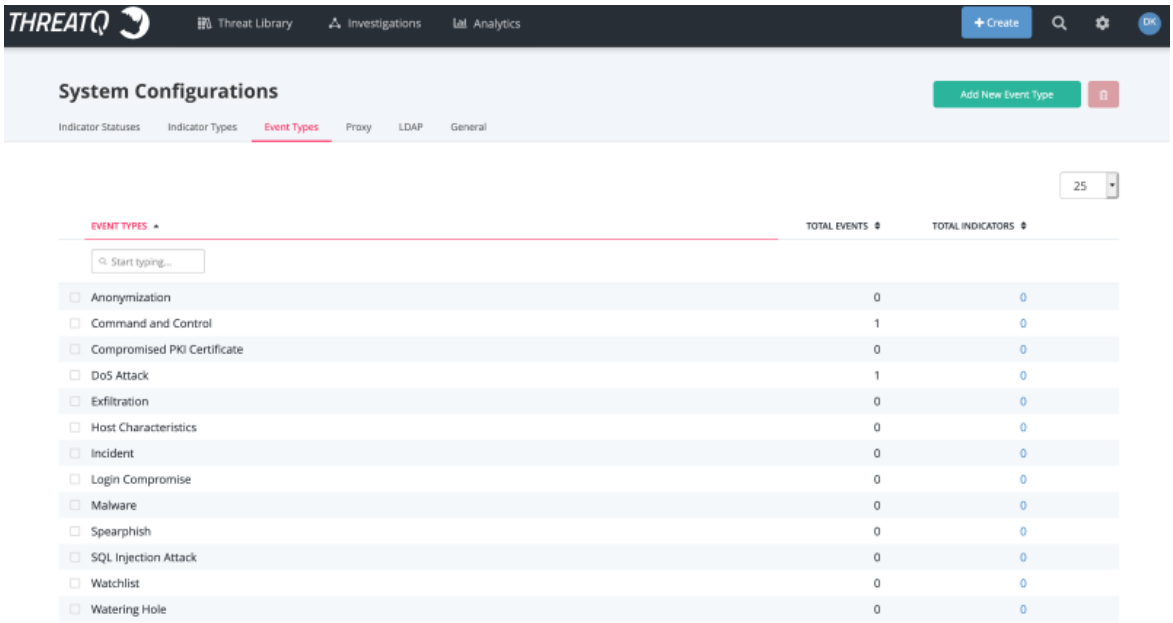
1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



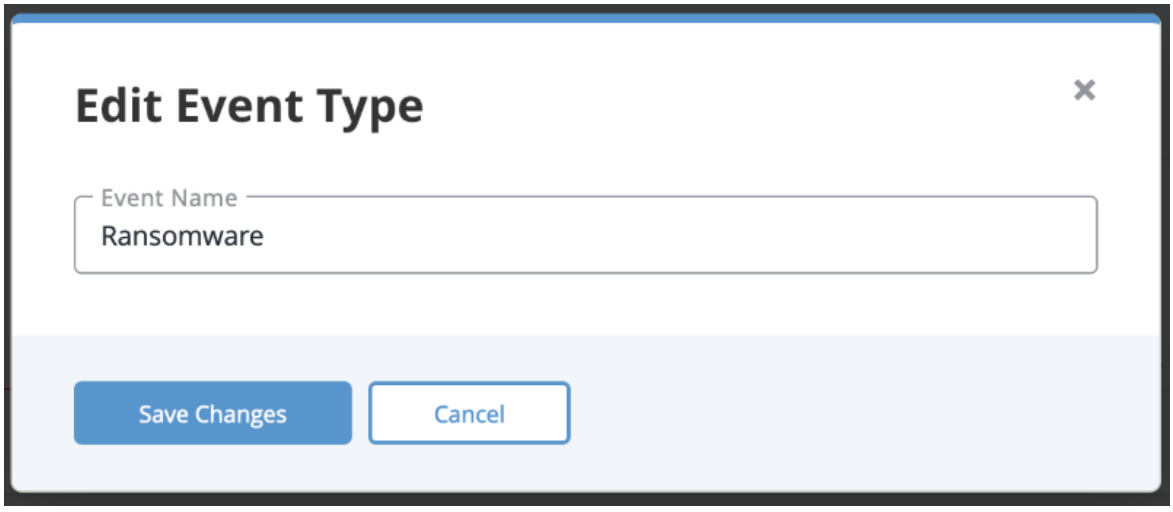
2. Click the **Event Types** tab.

   The Event Types tab opens.



3. Determine the Event Type you want to edit and click **Edit** in the far right column.

   The Edit Event Type dialog box opens.



4. Enter a new **Event Name**.
5. Click **Save Changes**.

Deleting an Event Type

To delete a user-generated Event Type, complete the following procedure.

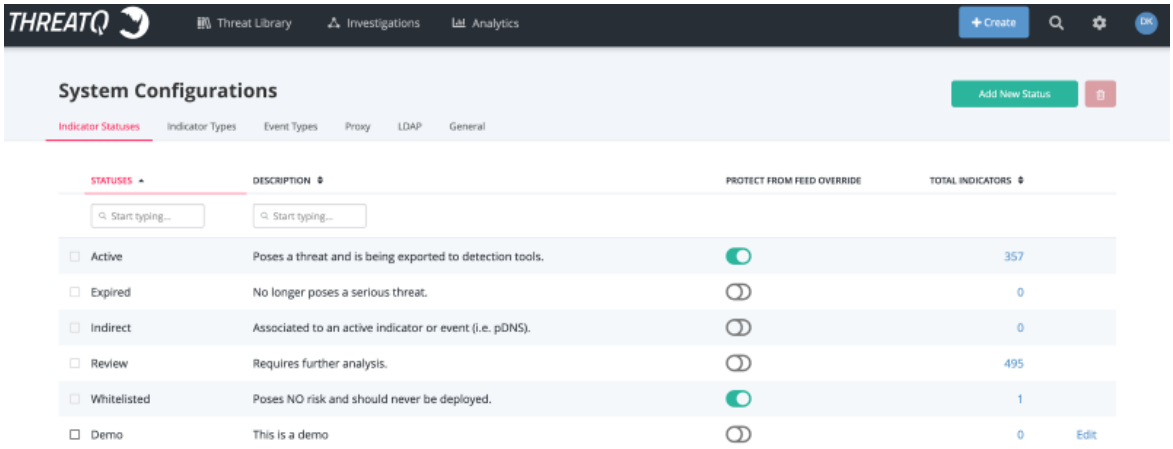
Custom Event Types can only be deleted if there are no events using that event type.

You cannot delete an Event Type provided by ThreatQ.

Procedure:

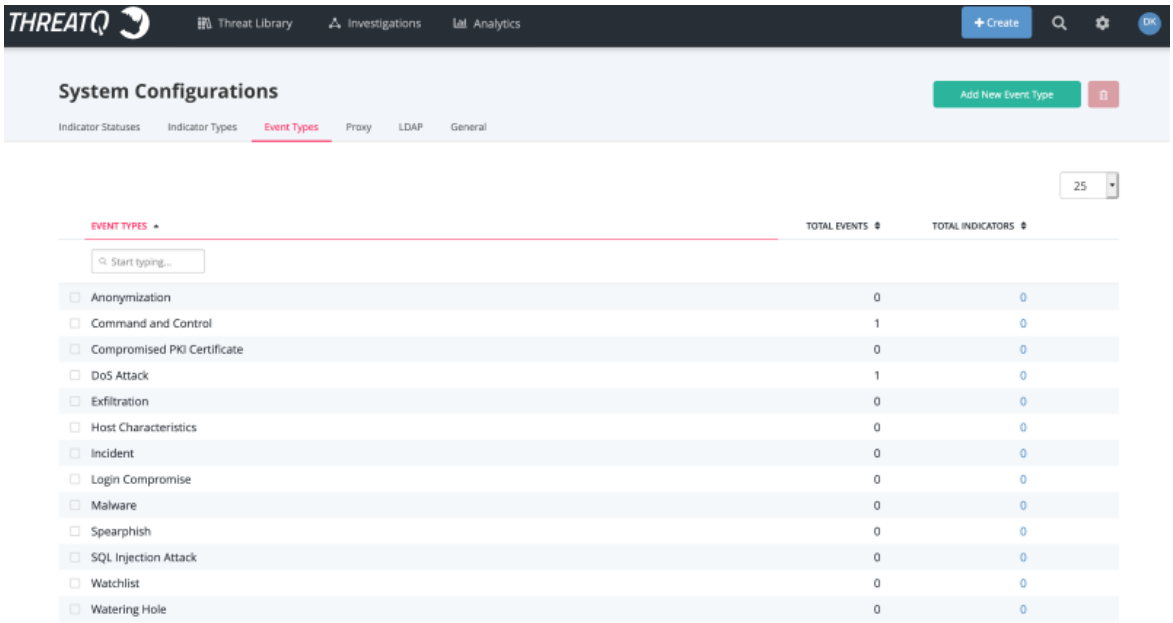
1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



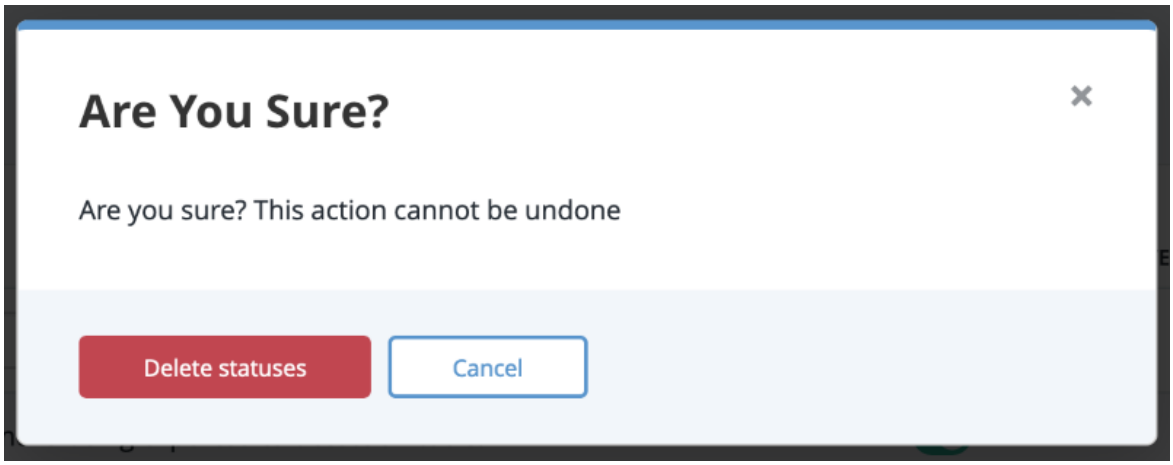
2. Click the **Event Types** tab.

   The Event Types tab opens.



3. Determine the event type you want to delete and select the corresponding check-box in the first column.
4. Click the **Delete icon** in the upper right hand corner.

   A confirmation dialog box appears.



5. Click **Delete Types**.

Proxy

The System Configuration: Proxy page allows you to enable or disable proxies.

> Users are required to set their proxy server settings to use http: for their https: traffic. The ThreatQ **Proxy Configuration** page can be found by navigating to **Settings > System Configuration > Proxy**.

Access Proxies

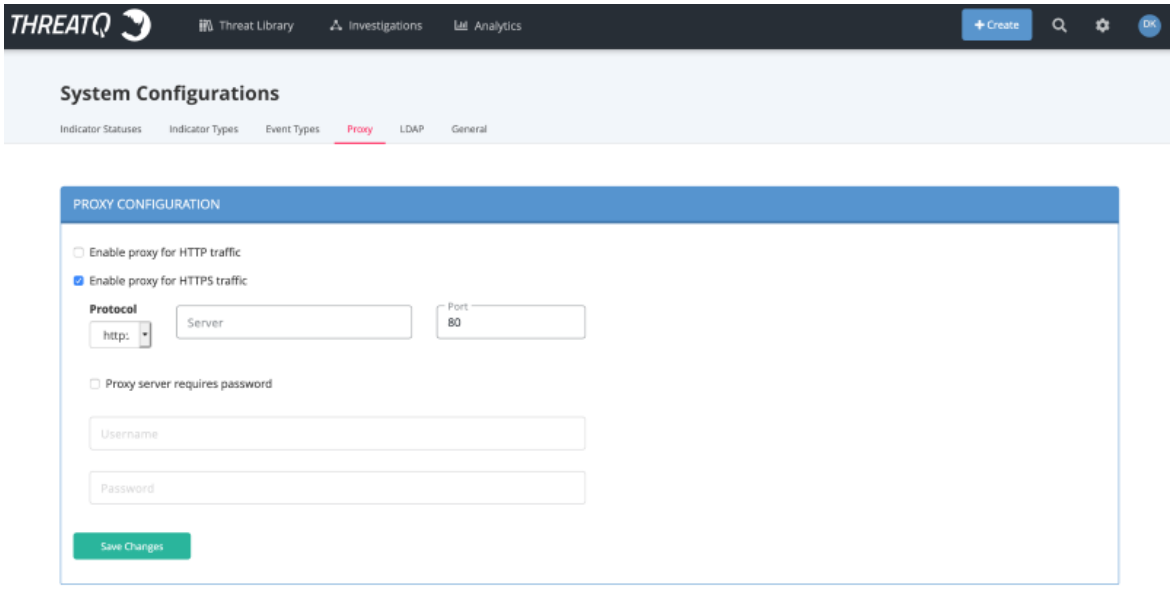
To access proxies:

1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.

2. Click the **Proxy** tab.

   The Proxy Configuration tab loads.



Proxy Table Functions:

Function	Description
Enabling a proxy for HTTP or HTTPS traffic	1. Check the correct proxy type and enter configuration details. Click **Save Changes**. ThreatQ will check that the proxy has been configured properly.
Disabling a proxy for HTTP or HTTPS traffic	1. Uncheck the proxy you wish to disable, and click **Save Changes**.

Account Security

The System Configuration: Account Security page allows you to configure the number of failed login attempts before a user is locked out and the number of minutes a user will be locked out before being able to reattempt login. By default, failed login attempts will be set to five and the timeout will be set to thirty minutes.

Configuring User Lockout

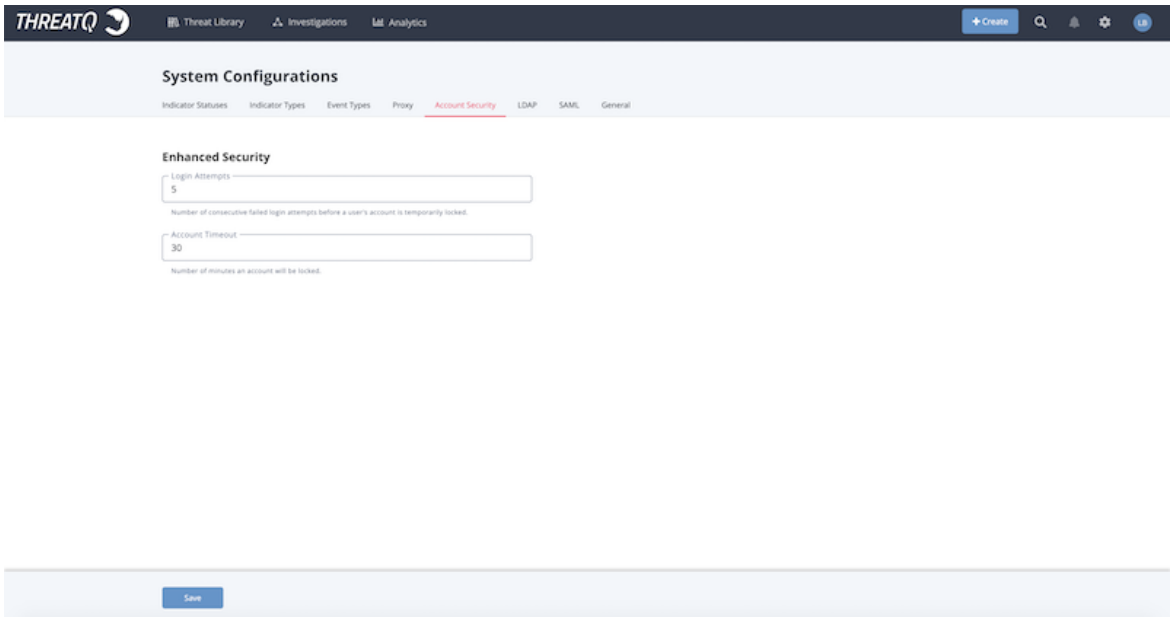
To configure user lockout:

1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.

2. Click the **Account Security** tab.

   The Account Security Configuration tab loads.



Account Security Functions:

Function	Description
Login Attempts	Number of consecutive failed login attempts before a user's account is temporarily locked.
Account Timeout	Number of minutes an account will be locked.

LDAP Authentication

AGDS Users -If you are using LDAP or SAML authentication on your **Source** ThreatQ instance, and require users transferred via import to have authentication capabilities on your **Target** ThreatQ instance, then you must enable the same authentication method on your **Target** ThreatQ

instance prior to performing import.

ThreatQ allows you to configure system access via LDAP, the Lightweight Directory Access Protocol. You have two configuration options:

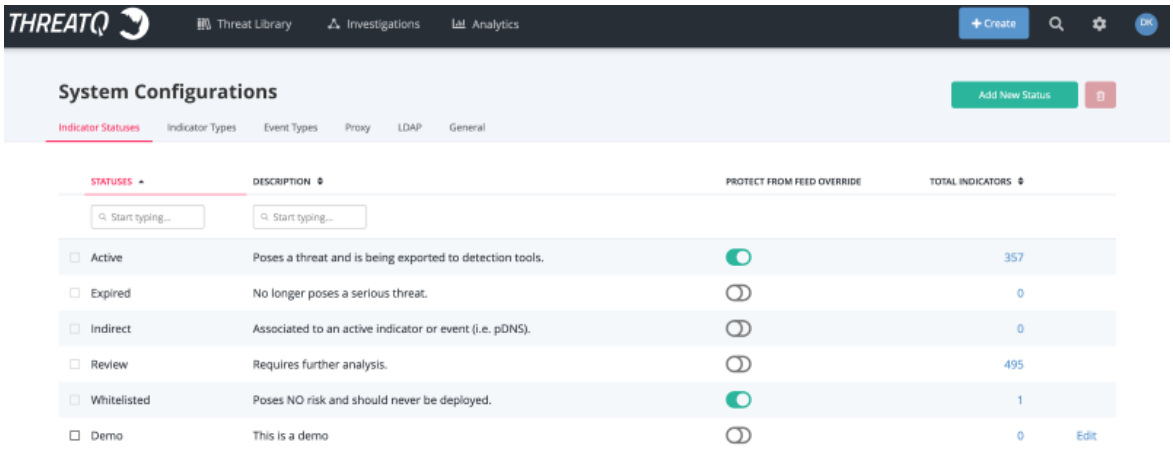
- Anonymous Bind (previously referred to as basic)
- Authenticated Bind

It is highly recommended that you review the Required Information for Creating LDAP Authentication topic before configuring your LDAP settings.

To Access the LDAP tab:

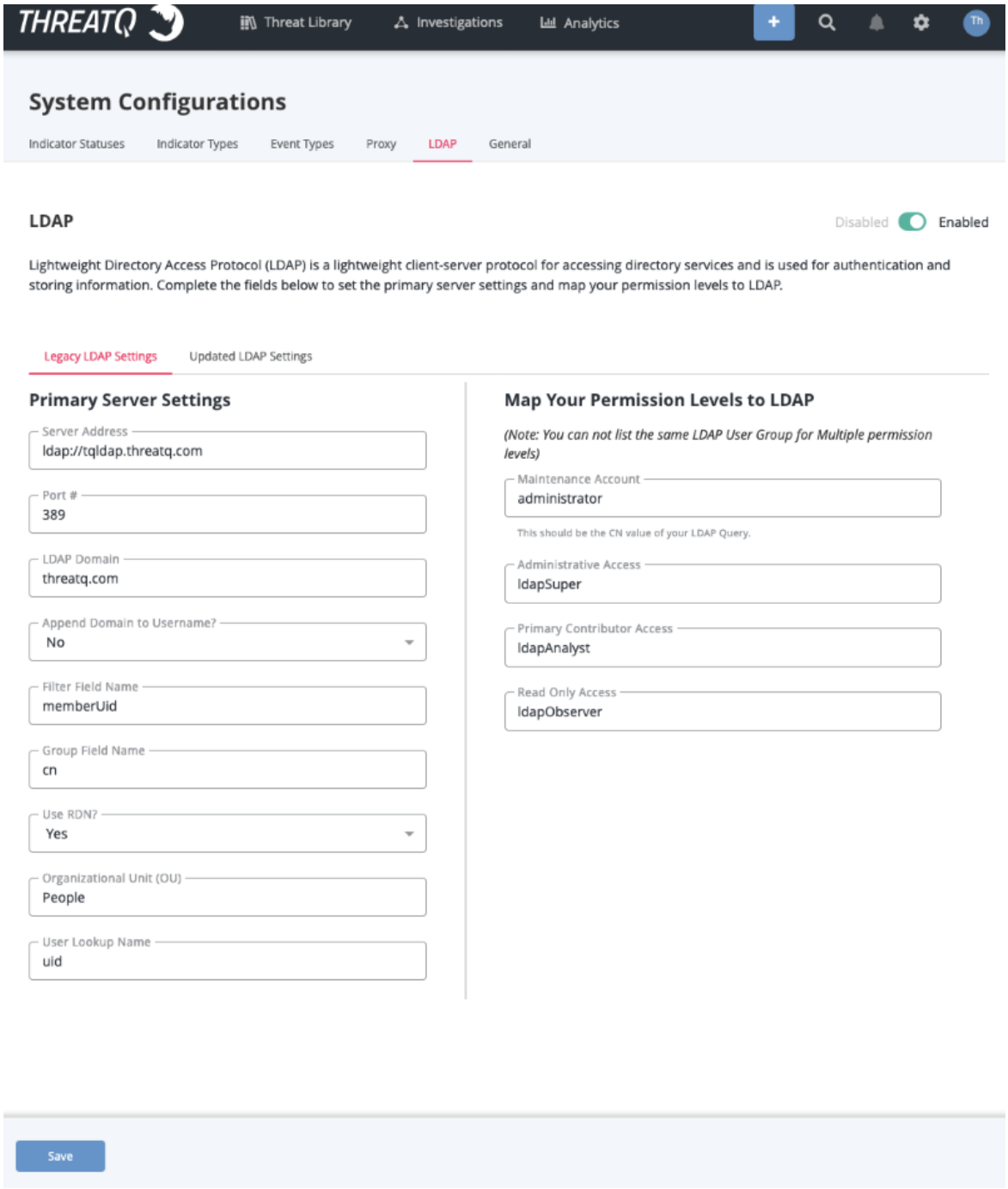
1. From the main menu, select **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



2. Click the **LDAP** tab.

The LDAP tab opens with the Legacy LDAP form loaded by default.



Switching LDAP Connections

To switch between using the Anonymous (Legacy) and Authenticated (Updated) Bind LDAP connections, open the desired connection type's form in the LDAP section and click on the Save button.

Example: A User is using the legacy LDAP Settings option. He switches to the Updated LDAP tab and clicks on Save. ThreatQ will now use the Updated LDAP Settings. If he switches back to the Legacy LDAP tab and clicks on Save again, ThreatQ will start using the Legacy LDAP settings again.

Related Topics:

- Required Information for Creating LDAP Authentication
- Configuring Anonymous Bind LDAP Settings
  - Configuring Secure LDAP
- Configuring Authenticated Bind LDAP Settings

Required Information for Creating LDAP Authentication

Before you configure a connection to your LDAP server, you should work with your LDAP administrator to collect, at minimum, the following information:

Anonymous Bind

- LDAP Server URL
- LDAP Port
- LDAP Group Field Name
- LDAP Filter Field Name
- LDAP group mappings for super, maintenance, analyst, and observer

Authenticated Bind

- LDAP Server name or IP Address
- LDAP port
- LDAP base DN
- LDAP Group Member Field Name
- LDAP Primary Group Name
- Whether to use LDAP over SSL (ldaps or ldap)
- LDAP User Id Key Field Name
- LDAP User Group Member Key Field Name
- LDAP group mappings for super, maintenance, analyst, and observer

Configuring Anonymous Bind LDAP Settings

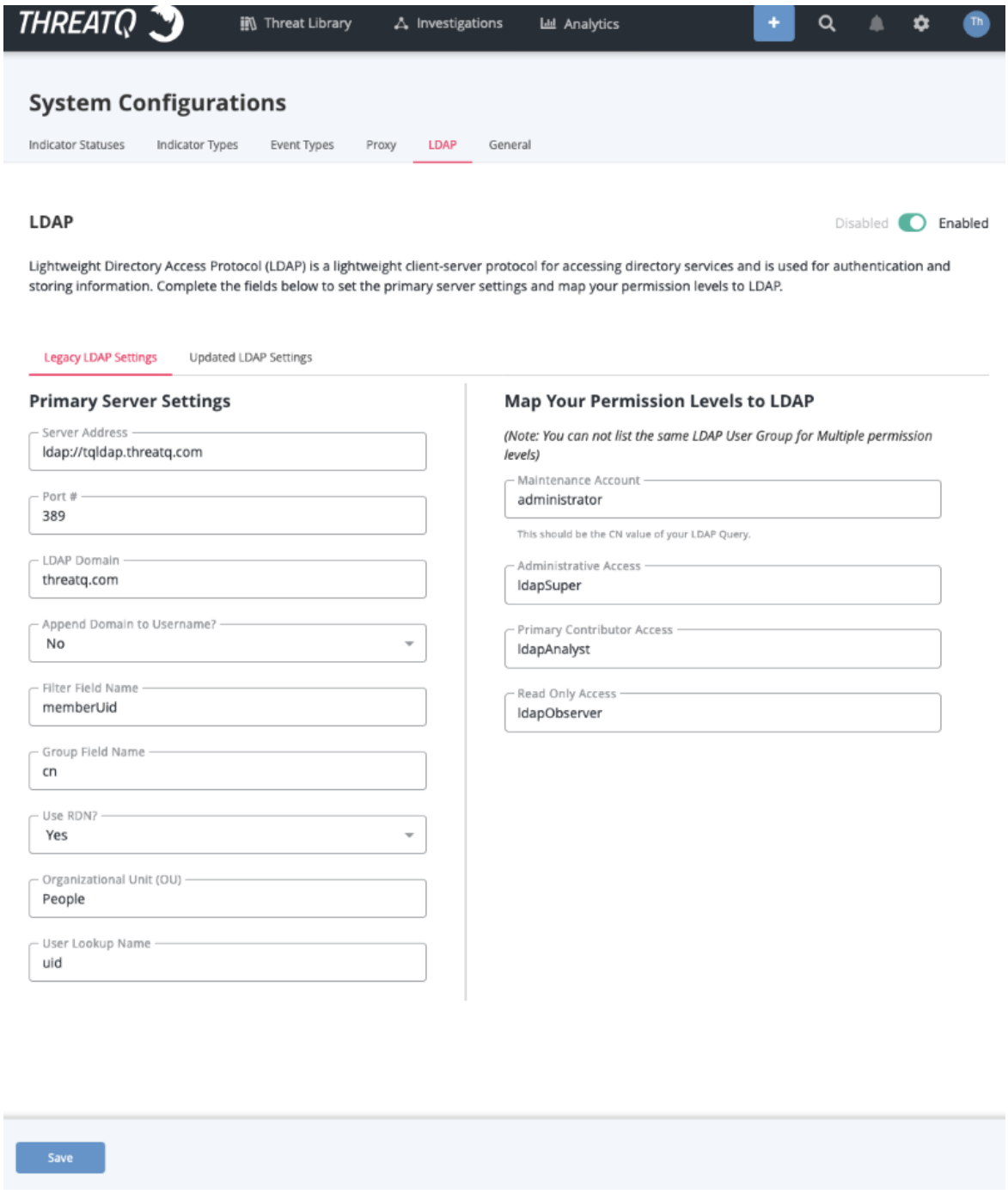
Only users with an Administrative or Maintenance account can access LDAP settings.

ThreatQuotient strongly recommends that you perform a full backup before changing your authentication method.

Procedure:

1. Navigate to **Settings** > **System Configurations**.
2. Click on the **LDAP** option.

   The Legacy LDAP Settings form will load by default.



3. Complete the following server settings:

Field	Description
Server Address	Enter the name of the server where LDAP is hosted. **Example:** ldap://[servername]
Port #	389 for LDAP 636 for LDAPS If LDAPS is used, the Port # will default to 636.
LDAP Domain	Enter the domain for which LDAP is configured to authenticate. **Example:** threatq.com
Append Domain to Username	Choose from the following options: • Yes for most Active Directory servers • No for most Open LDAP servers
Filter Field Name	This field is specific to your LDAP directory configuration. **AD Example:** memberuid **OpenLDAP Example:** uid
Group Field Name	This field is specific to your LDAP directory configuration. **AD Example:** memberof **OpenLDAP Example:** cn

Field	Description
Use RDN?	Choose from the following options: • Yes to use Relative Distinguished Names. • No to use full Distinguished Names
Organizational Unit (OU)	This field is specific to your LDAP directory configuration. Your LDAP administrator should provide the correct value for this field.
User Lookup Name	This field is specific to your LDAP directory configuration. **AD Example:** memberUid **OpenLDAP Example:** uid

4. Complete the **MAP your Permission Levels to LDAP** section:

You can not list the same LDAP User Group for multiple permission levels. For roles not mapped, you should enter a hyphen: "-." You cannot save the configuration without entering a value in each field.

Field	Example
Maintenance Account	**OpenLDAP Example:** ldapSuper **AD Example:** CN=tq-maintenance,CN=Builtin,DC=yourdomain,DC=com
Administrative Access	**OpenLDAP Example:** administrator **AD Example:** CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com

Field	Example
Read Only Access	**OpenLDAP Example:** ldapObserver **AD Example:** CN=read-onlyCN=Builtin,DC=yourdomain,DC=com
Primary Contributor Access	**OpenLDAP Example:** ldapAnalyst **AD Example:** CN=primary-contributor,CN=Builtin,DC=yourdomain,DC=com

5. Click **Save Changes**.
6. Click on the Enable/Disable toggle switch to enable LDAP.

If your LDAP fails to enable or fails to function properly, validate your inputs. If the configuration continues to fail, please contact ThreatQ Support.

Configuring Secure LDAP

This topic is for Anonymous Bind LDAP connections only. The steps needed to create a secured connection authenticated bind are included in the Configuring Authenticated Bind LDAP Settings topic.

ThreatQuotient strongly recommends that you perform a full backup before changing your authentication method.

To configure secure LDAP, you must complete the following steps:

1. Enter your LDAP settings in the ThreatQ user interface. See the Configuring Anonymous Bind LDAP Settings topic for more details.
2. Access the ThreatQ appliance command line as root and edit and navigate to the following directory: /etc/openldap/.

3. Use vi to edit ldap.conf and update/confirm that your settings are as follows:

```
#
# LDAP Defaults
#
```

```
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
```

```
BASE    dc=[your domain],dc=com
URI ldap://[your servername]:389 ldaps://[your servername]:636
```

```
#SIZELIMIT  12
#TIMELIMIT  15
#DEREF      never
```

```
TLS_CACERTDIR   /etc/openldap/certs
```

```
# Turning this off breaks GSSAPI used with krb5 when rdns =
false
SASL_NOCANON    on
TLS_REQCERT allow
```

> ThreatQ recommends that you edit ldap.conf on the appliance, rather than editing off box and uploading it. If you do edit the file off box, ensure that you use a linux editor. Windows and Mac editors may corrupt the file.

If your LDAP fails to enable or fails to function properly, validate your inputs. If the configuration continues to fail, please contact ThreatQ Support.

Configuring Authenticated Bind LDAP Settings

> It is recommended that you contact ThreatQ Support before configuring an authenticated bind connection.

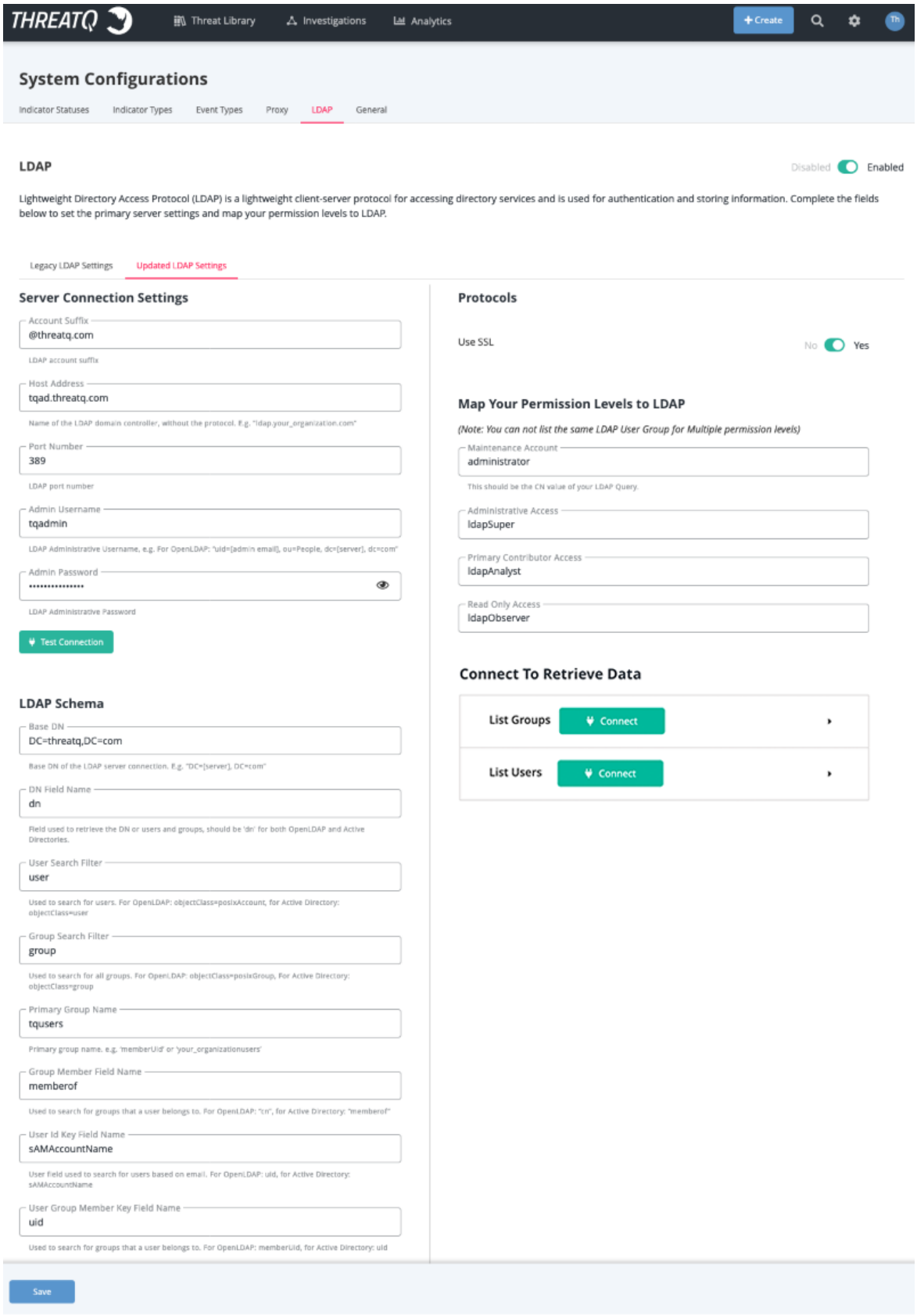
Only users with an Administrative or Maintenance account can access LDAP settings.

Procedure:

1. Navigate to **Settings** > **System Configurations**.

2. Click on the **LDAP** option and select the **Updated LDAP Settings** tab.

The Updated LDAP Settings form will load.


THREATQ
Threat Library
Investigations
Analytics
+ Create
System Configurations
Indicator Statuses
Indicator Types
Event Types
Proxy
LDAP
General
LDAP
Disabled
Enabled
Lightweight Directory Access Protocol (LDAP) is a lightweight client-server protocol for accessing directory services and is used for authentication and storing information. Complete the fields below to set the primary server settings and map your permission levels to LDAP.
Legacy LDAP Settings
Updated LDAP Settings
Server Connection Settings
Account Suffix
@threatq.com
LDAP account suffix
Host Address
tqad.threatq.com
Name of the LDAP domain controller, without the protocol. E.g. "ldap.your_organization.com"
Port Number
389
LDAP port number
Admin Username
tqadmin
LDAP Administrative Username, e.g. For OpenLDAP: "uid=[admin email], ou=People, dc=[server], dc=com"
Admin Password
LDAP Administrative Password
Test Connection
LDAP Schema
Base DN
DC=threatq,DC=com
Base DN of the LDAP server connection. E.g. "DC=[server], DC=com"
DN Field Name
dn
Field used to retrieve the DN or users and groups, should be 'dn' for both OpenLDAP and Active Directories.
User Search Filter
user
Used to search for users. For OpenLDAP: objectClass=posixAccount, for Active Directory: objectClass=user
Group Search Filter
group
Used to search for all groups. For OpenLDAP: objectClass=posixGroup, For Active Directory: objectClass=group
Primary Group Name
tqusers
Primary group name. e.g. 'memberUid' or 'your_organizationusers'
Group Member Field Name
memberof
Used to search for groups that a user belongs to. For OpenLDAP: "cn", for Active Directory: "memberof"
User Id Key Field Name
sAMAccountName
User field used to search for users based on email. For OpenLDAP: uid, for Active Directory: sAMAccountName
User Group Member Key Field Name
uid
Used to search for groups that a user belongs to. For OpenLDAP: memberUid, for Active Directory: uid
Protocols
Use SSL
No
Yes
Map Your Permission Levels to LDAP
(Note: You can not list the same LDAP User Group for Multiple permission levels)
Maintenance Account
administrator
This should be the CN value of your LDAP Query.
Administrative Access
ldapSuper
Primary Contributor Access
ldapAnalyst
Read Only Access
ldapObserver
Connect To Retrieve Data
List Groups
Connect
List Users
Connect
Save

3. Complete the **Server Connections Settings** section:

Field	Description
Account Suffix	The LDAP account suffix.
Host Address	Name of the LDAP domain controller without the protocol. **Example:** tqldap.threatq.com
Port Number	The LDAP port; either **636** or **389**. Only standard ports for secured and unsecured connections are supported. Use port 636 if using SSL to create a secured connection.
Admin Username	The LDAP administrative username.
Admin Password	The LDAP administrative password.

4. Click on **Test Connections** to verify the settings are correct.

5. Complete the **LDAP Schema** section:

Field	Description
Base DN	The Base DN of the LDAP server connection. **Example:** DC=[server], DC="com"
DN Field Name	The field used to retrieve the DN or users and groups.

Field	Description
	This field should be **DN** for both OpenLDAP and Active Directory.
User Search Filter	The field to search for users. For **OpenLDAP**: objectClass=posIxAccount For **Active Directory**: objectClass=user
Group Search Filter	The field to search for grpups. For **OpenLDAP**: objectClass=posIxGroup For **Active Directory**: objectClass=group
Primary Group Name	The primary group name.
Group Member Field Name	This field is used to search for groups that a user belongs to. For **OpenLDAP**: cn For **Active Directory**: memberof
User ID Key Field Name	Field used to search for users based on email. For **OpenLDAP**: uid For **Active Directory**: sAMAccountName
User Group Member Key Field Name	Field used to search for groups that user

Field	Description
	belongs to. For **OpenLDAP**: memberUid For **Active Directory**: uid

6. Under the Protocols section, use the **Yes/No** toggle switch to select whether the connection will use SSL.

If the connection will use SSL, confirm that the port number, set in step 3, is 636 to create a secured connection.

7. Complete the **MAP your Permission Levels to LDAP** section:

You cannot use the same LDAP User Group for multiple permission levels. For roles not mapped, you should enter a hyphen: "-." You cannot save the configuration without entering a value in each field.

Field	Description
Maintenance Account	The LDAP account the ThreatQ Maintenance group will map to for permissions. **Open LDAP Example:** ldapSuper **AD Example:** CN=tq-maintenance,CN=Builtin,DC=yourdomain,DC=com
Administrative Access	The LDAP account the ThreatQ Administrative group will map to for permissions. **Open LDAP Example:** administrator

Field	Description
	AD Example: CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Primary Contributor Access	The LDAP account the ThreatQ Primary Contributor group will map to for permissions. **Open LDAP Example:** ldapAnalyst **AD Example:** CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Read-Only Access	The LDAP account the ThreatQ Read-Only group will map to for permissions. **Open LDAP Example:** ldapObserver **AD Example:** CN=read-onlyCN=Builtin,DC=yourdomain,DC=com

8. Use the **Connect to Receive Data** section connect to your LDAP using the settings on this page to pull group information and user lists
9. Click on **Save**.
10. Click on the Enable/Disable toggle switch to enable LDAP.

Green indicates the feature is active.

SAML Authentication

Security Assertion Markup Language (SAML) is a single sign-on (SSO) standard that allows you to log into your ThreatQ instance using a credentials service outside of the platform.

Email addresses and passwords are authenticated outside of ThreatQ and user roles are determine using the permissions mappings located on the ThreatQ SAML configuration page.

Upon enabling SAML, users will see a SSO login option on the ThreatQ login page - see the Logging into ThreatQ topic.

Users cannot use SSO to log into a ThreatQ Local Maintenance account.

AGDS Users -If you are using LDAP or SAML authentication on your **Source** ThreatQ instance, and require users transferred via import to have authentication capabilities on your **Target** ThreatQ instance, then you must enable the same authentication method on your **Target** ThreatQ instance prior to performing import.

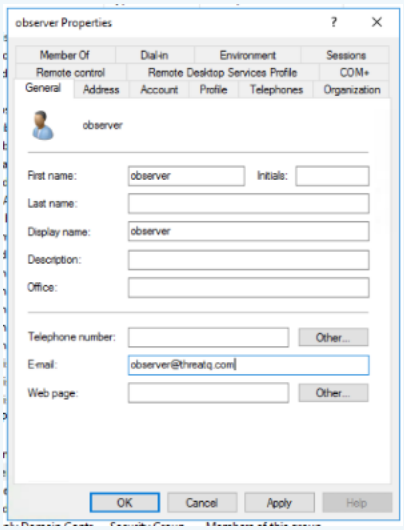
Related Topics:

- Configuring SAML
  - Adding ThreatQ as a Service Provider
  - Setting up LDAP Users/Groups for SAML
- Authentication Methods
- Transitioning Authentication Methods

Configuring SAML

ThreatQuotient strongly recommends that you perform a full backup before changing your authentication method.

SAML users are required to add their email address to their user profiles in order to use the SSO. As part of the integration process, the ThreatQ platform expects that the user's email address has already been added to their IdP. See the Setting up LDAP Users/Groups for SAML topic for more details.



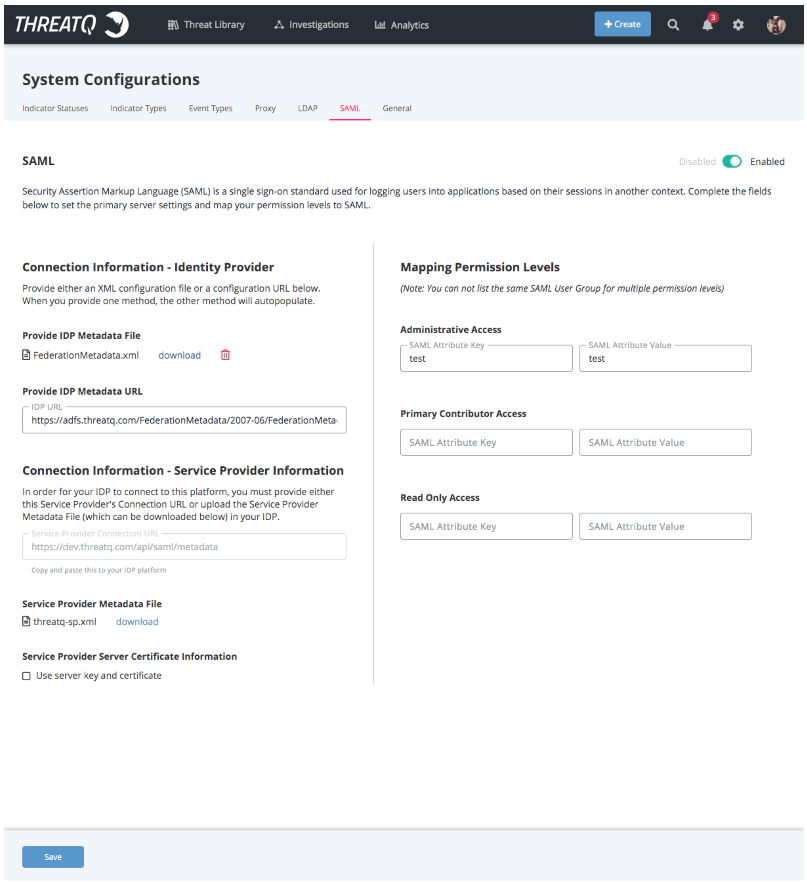
LDAP must be disabled before enabling SAML. The ThreatQ platform will alert you if LDAP is enabled when you try to enable SAML and will instruct you to disable LDAP.

1. From the main menu, select **Settings** > **System Configurations**.

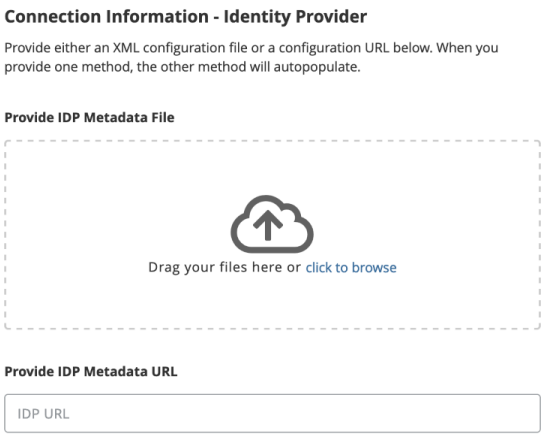
   The System Configurations page opens.

2. Click on the **SAML** tab.

   The SAML configuration page opens.

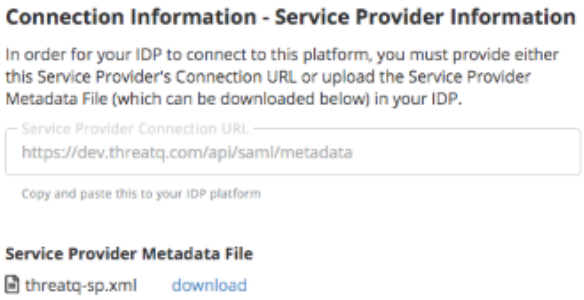


3. Complete the **Identity Provider (IdP)** section by either:
   - Uploading your IdP metadata file by dragging and dropping the file onto the field or using the browse button to locate the file saved on your local machine.
   - Entering your IdP metadata file's URL in the **Provide IdP Metadata URL** field.



Whichever method you choose to use will result in the auto-completion of the other field. **Example:** Uploading a metadata file will result in the IdP Metadata URL being populated with data parsed from the file.

4. Use either the **Service Provider Connection URL** or **Service Provider Metadata file** listed in the Connection Information - Service Provider Information section to provide your ThreatQ platform metadata to your Network Administrator to add ThreatQ as a service provider. The steps to add ThreatQ as a Service Provider may differ based on your environment - See the Adding ThreatQ as a Service Provider

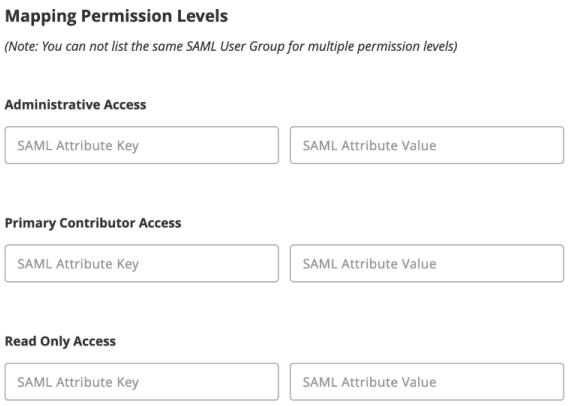


5. Check the **User Server Certificate and Key** option under the Platform Server Certificate Information section if your environment requires a certificate. You can upload the Certificate and .key file by either:

- Drag and drop the file into the field.
- Select browse to locate the file on your local machine.

> You Network Administrator will need the certificate and key later when applying the ThreatQ platforms connection information supplied in step 4.

6. Complete the Mapping Permissions Levels section by providing a SAML Attribute Key and SAML Attribute Value for each ThreatQ user role. See the Setting up LDAP Users/Groups for SAML topic for information on how to setup LDAP users and groups for SAML integration.



Mapping Notes:

- SAML cannot be used for Maintenance Accounts.
  - Local Maintenance Accounts cannot be mapped when enabling SAML.
  - If converting from LDAP authentication, LDAP groups that were mapped to the ThreatQ Maintenance role will have to be mapped to another user role.
- You cannot use the same SAML Key and Values for multiple roles.

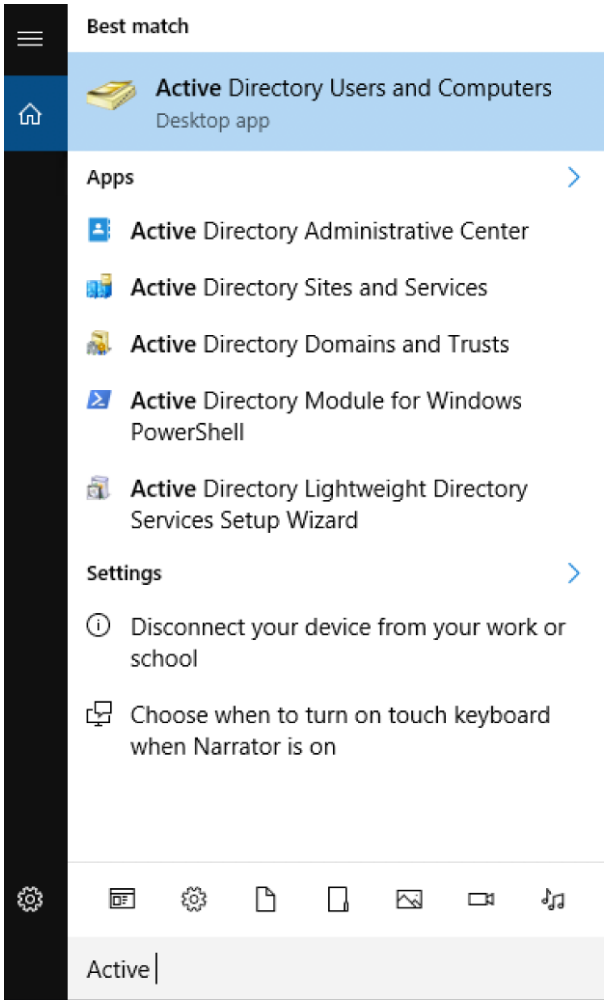
- You do not have to map all ThreatQ roles but at least one role has to be mapped to use SAML. **Example:** Administrator and Primary Contributor will be mapped but the Read Only Access role will be blank.

7. Click on **Save** located at the bottom of the page.
8. Confirm that your network administrator has completed Adding ThreatQ as a Service Provider before proceeding with the final steps listed below.
9. Click on **Test Authentication** to confirm that the ThreatQ platform and your IdP can connect.
10. Click on the **Enable** toggle switch located at the top-right of the page to enable SAML.

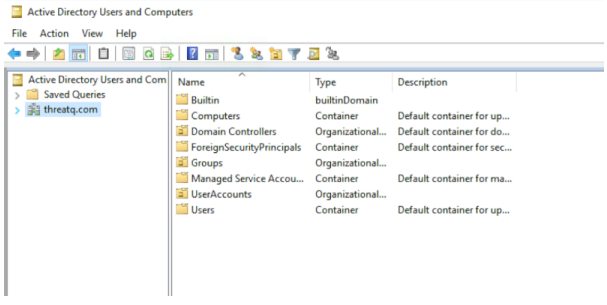
Setting up LDAP Users/Groups for SAML

The following steps detail how to set up LDAP users and groups for SAML integration.

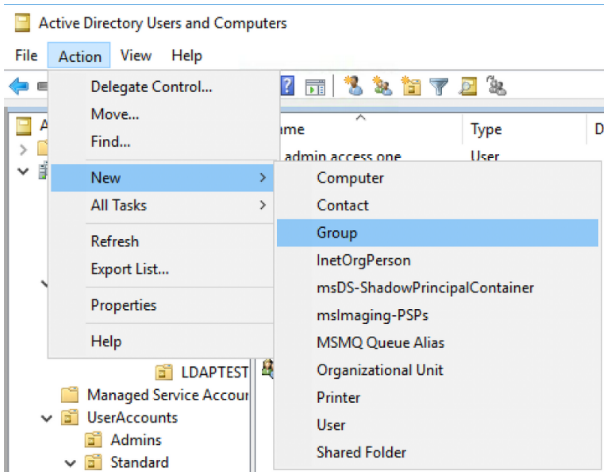
1. Log into the Windows Server.
2. Start the Active Directory Users and Computers application from the Start Menu.



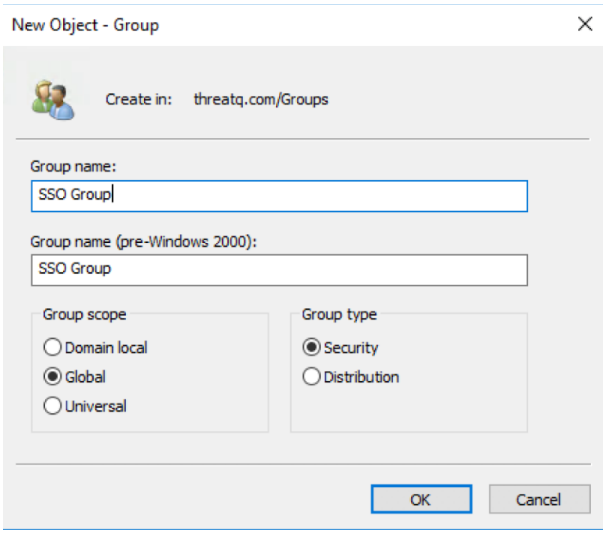
3. Navigate to and select the **Groups** folder under your LDAP domain.



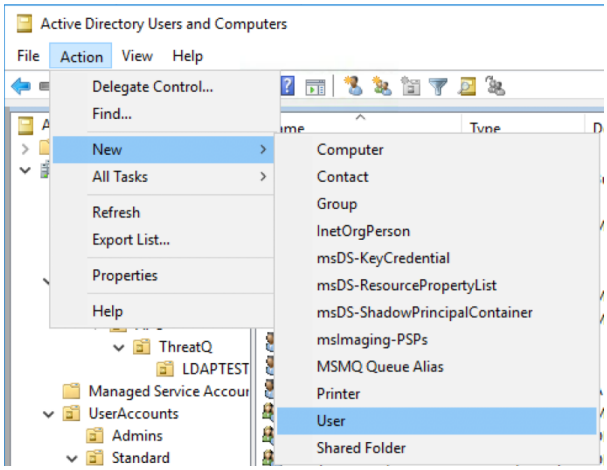
4. Click on **Actions > New > Group**.



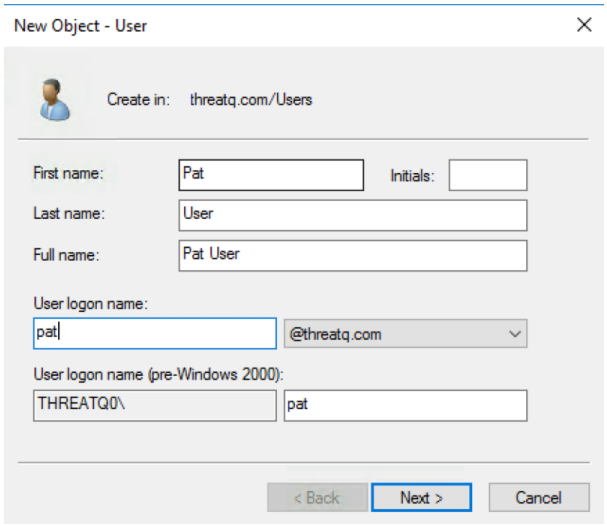
5. Enter in the **Group name** and click on **OK**.



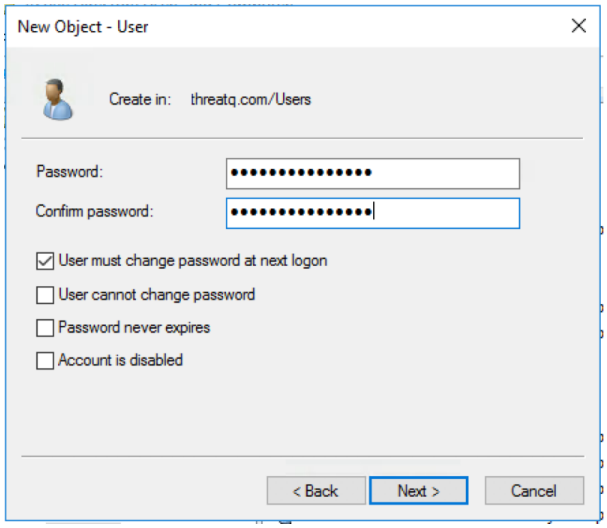
6. Select the **Users** folder and click on **Actions > New > User**.



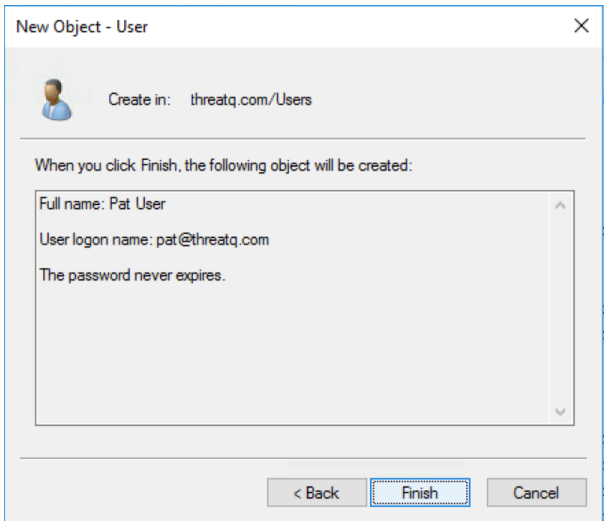
7. Enter in the **User Information** and click on **Next**.



8. Enter the **Password** and click on **Next**.

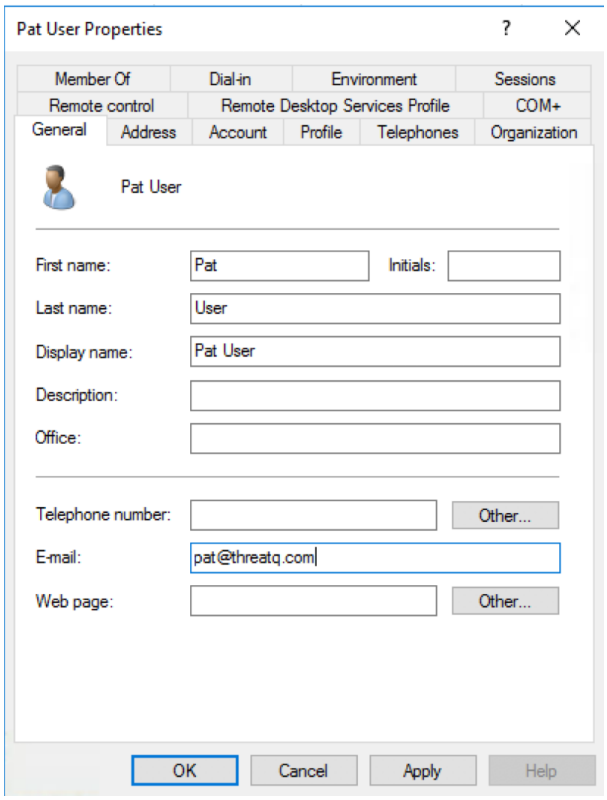


9. Confirm that the details are correct an then click on **Finish**.



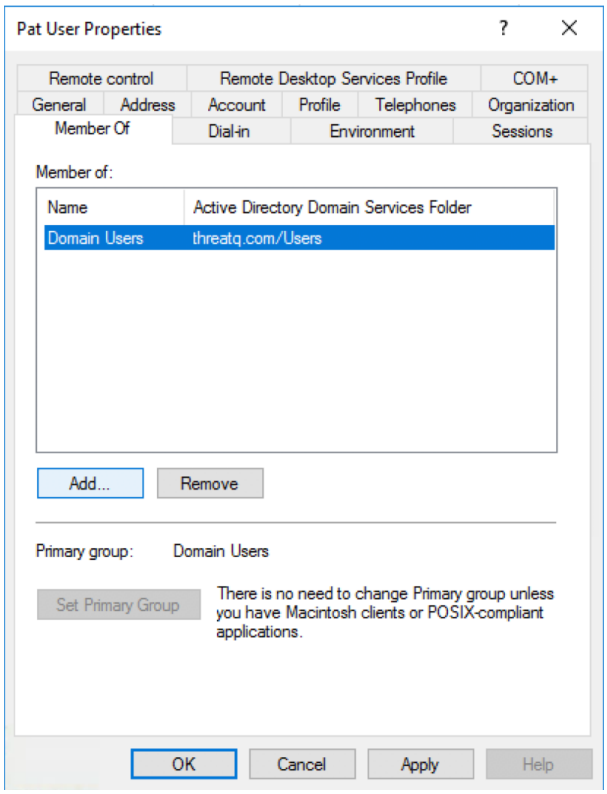
10. Find and double-click on the newly created user to edit the **User Properties**.

11. Confirm that the E-Mail has the user's correct email address.

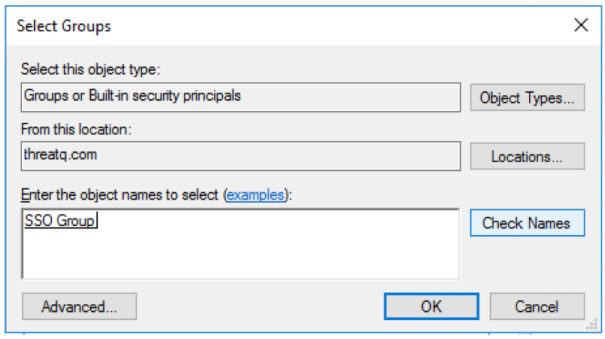


It is important that the E-mail field be filled in order for the SSO integration to work with this user.

12. Navigate to the **Member of** tab and click on **Add**.

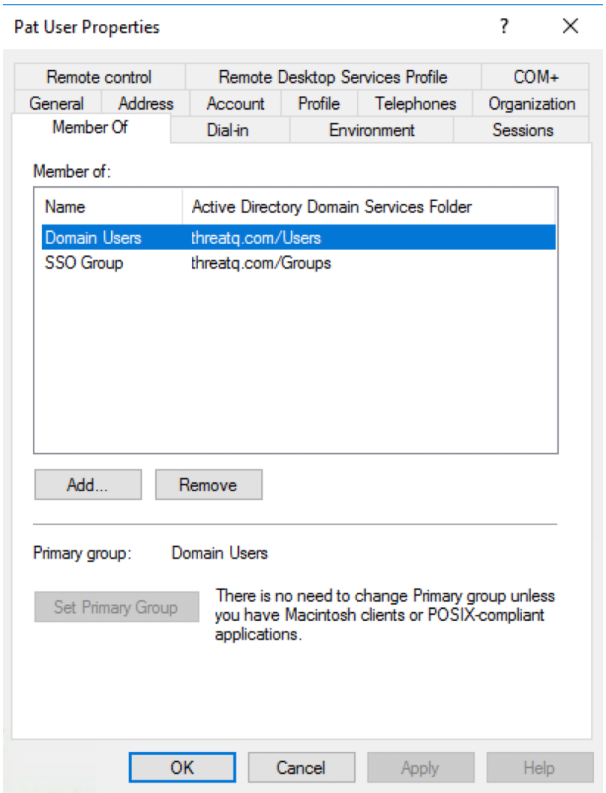


13. Enter the name of the group you created earlier in steps 4-5 in the field provided.



14. Click on **Check Names** to verify the group name and then click **OK**.

15. Verify that the User is now a member of the group.



16. Click **OK** to close the properties window.

Adding ThreatQ as a Service Provider

The topics in this section provide the required steps to add ThreatQ as a service provider for your IdP.

- ADFS 2016
- Azure AD Provider Setup
- Google G Suite Service Provider Setup
- Okta Service Provider Setup

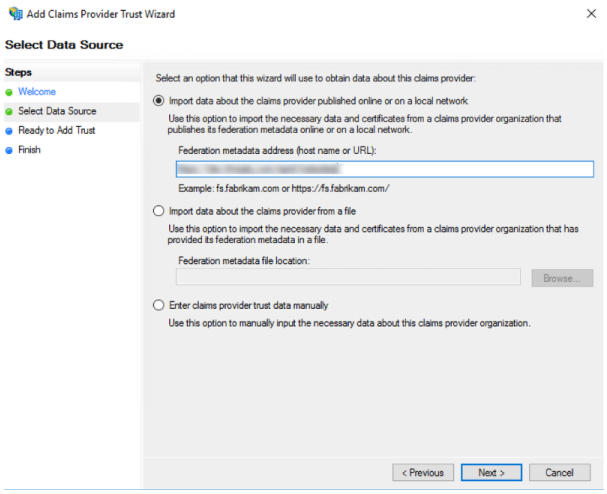
ADFS 2016

The steps below detail how to add ThreatQ as a service provider in ADFS 2016 .

From your server manager:

1. Select **AD FS** under the Dashboard heading.
2. Click on the **Tools** option and select **AD FS Management**.
3. Navigate to the Relying Party Trusts folder In the left-hand directory.
4. Click on the **Relying Party Trusts > Add Relying Party Trust** under the Actions heading.
5. Leave the **Claims Aware** option selected and click on **Start**.

   The Select Data Source section loads.



6. Confirm that the first radio option, **Import data about the claims provider published online...**, is selected.
7. Paste the **Platform Connection URL** located on the ThreatQ SAML page, step 4 on the Configuring SAML topic, into the Federation Metadata Address field in the following format:

```
https://<your hostname>/FederationMetadata/2007-06/Federa-
tionMetadata.xml
```

8. Click **Next**.

   A popup warning will appear stating that some metadata cotent was skipped.

9. Click **Ok** to proceed.
10. Continue through the next few sections by clicking **Next** until you reach the Ready to Add Trust page.
11. Review the information listed in the multiple tabs provided. Confirm that the proper certificates are listed under the **Certificate** and **Signature** tabs and upload any that are missing.
12. Click **Next**.

    The ThreatQ Relaying Party Trust has now been added. The next step to create 4 new Claims Rules for the new service provider.

    Contact your Network Administrator to receive the appropriate group mapping.

13. Click on **Add Rule**.
14. Select the **Send LDAP Attribute as Claims** claim rule template and click **Next**.
15. Enter a name for the rule. **Example:** email and UID.
16. Select the **Active Directory** as the Attribute Store.

    Active Directory must already be installed and enabled in order to complete this step

17. Add the following rows in the LDAP Mapping Attributes table:

LDAP Attribute	Outgoing Claim Type
E-Mail-Addresses	email
SAM-Account-Name	uid

18. Click on **OK** to create the rule.
19. Click on **Add Rule**.
20. Select the **Send LDAP Attribute as Claims** claim rule template and click **Next**.
21. Enter a name for the rule. **Example:** Email.
22. Select the **Active Directory** as the Attribute Store.
23. Add the following row in the LDAP Mapping Attributes table:

LDAP Attribute	Outgoing Claim Type
E-Mail-Addresses	E-Mail Address

24. Click on **OK** to create the rule.
25. Click on **Add Rule**.
26. Select the **Send LDAP Attribute as Claims** claim rule template and click **Next**.
27. Enter a name for the rule. **Example:** Groups.
28. Select the **Active Directory** as the Attribute Store.
29. Add the following row in the LDAP Mapping Attributes table:

LDAP Attribute	Outgoing Claim Type
Token-Groups - Unqualified Names	SSO

30. Click on **OK** to create the rule.
31. Click on **Add Rule**.
32. Select the **Transform an Incoming Claim** claim rule template and click **Next**.
33. Enter a name for the rule. **Example:** Named ID Transform.

34. Complete the following fields:

Field	Selection
Incoming Claim Type	E-Mail Address
Outgoing Claim Type	Name ID
Outgoing Name ID Format	Email

35. Select the **Pass through all claim value** radio option.
36. Click on **OK** to create the rule.
37. Click **OK** to close the Issuance Transform Rules dialog box.

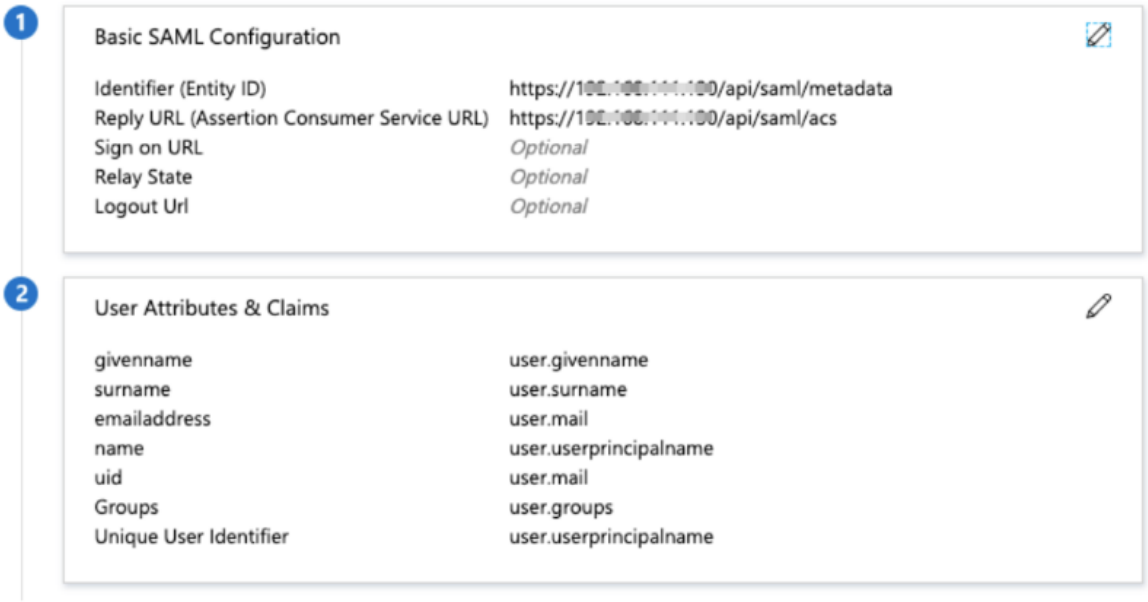
Azure AD Provider Setup

The steps below detail how to add ThreatQ as a service provider in Azure AD. This process is required in order to complete the SAML setup.

Setting Up the SAML App

1. Log in to the Azure portal with administrator permissions.
2. Go to **Azure Active Directory > Enterprise applications**
3. Click on **+New Application** then **Non-gallery application.**
4. Enter an application name such as **ThreatQ** then click **Add**.

5. Enter the **Single Sign On URL** and **SP Entity ID** as follows:



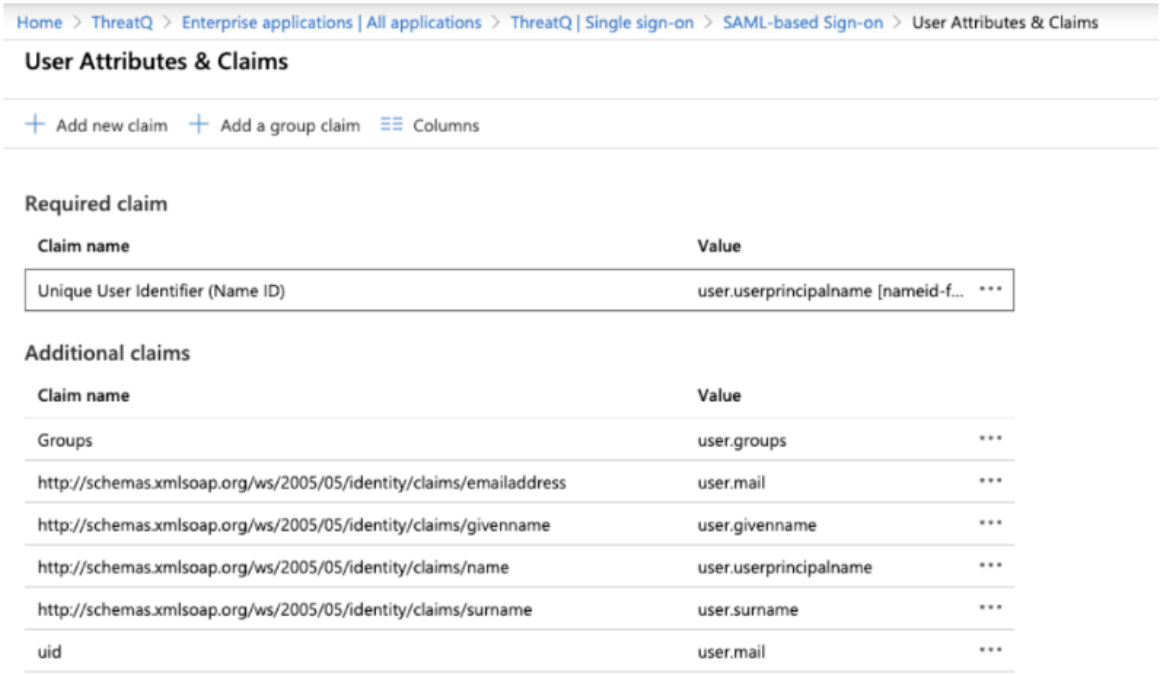
Field	Value	Description
ACS / Single Sign on URL	https://threatq.example.com/api/samle/acs	Assertion Consumer Service (ACS) is the ThreatQ URL + appended the "/ap-i/saml/acs" string.
SP Entity ID	https://threatq.example.com/api/samle/metadata	This is the ThreatQ entity ID which is the ThreatQ URL + appended with the "/api/saml/metadata" string.

6. Set the **Unique User identifier (Name ID) format** to **Email Address.**

7. In the **Additional claims** section **add uid** and set the value as `user.mail`.

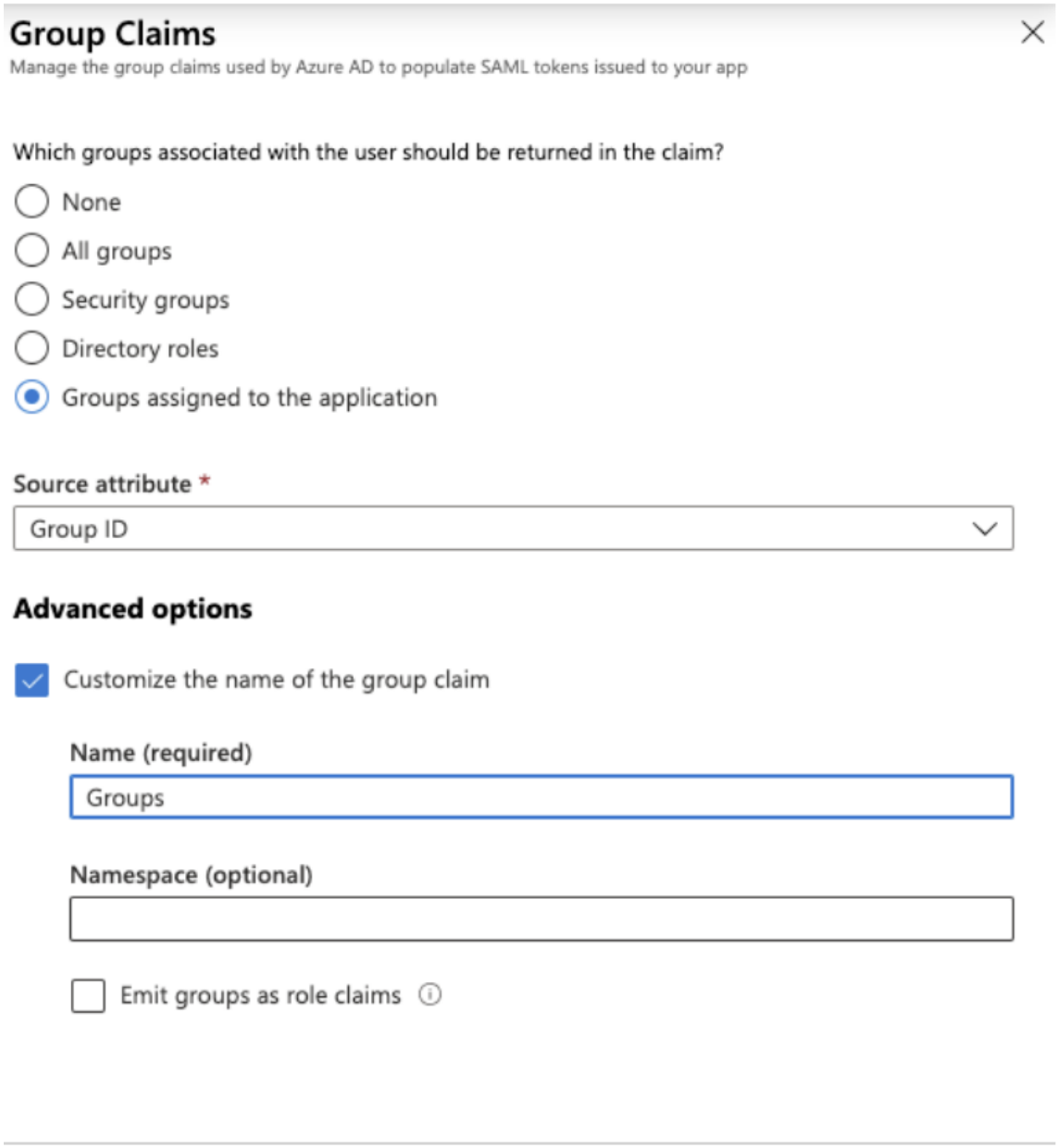
> Both the username and uid attributes are **required** and must be mapped to the user's Email address.

8. You also need to add an attribute you want to map to the roles in ThreatQ. In this example we added a Claim and created a **Groups** attribute and mapped it to all **user-.groups** assigned to the application. The group id the user belongs to is then included in the SAML assertion upon login.



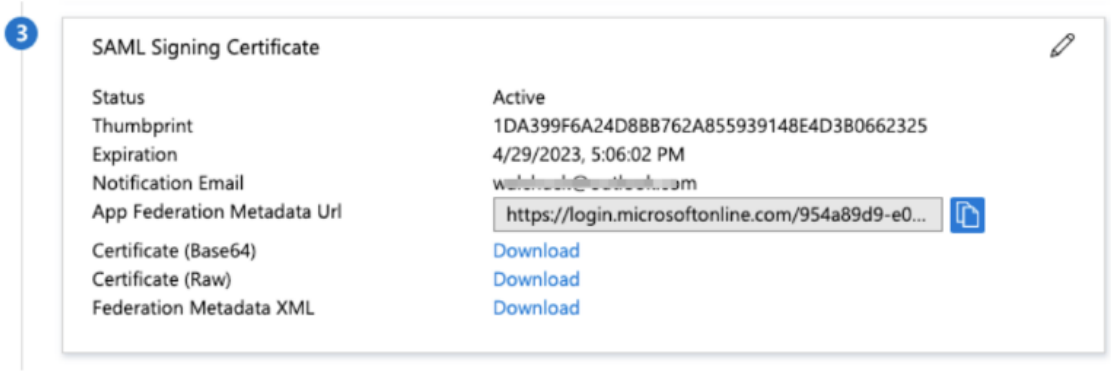
When adding a group claim it is recommended to customize name as this is what is required to be entered on the ThreatQ side as the SAML Attribute Key. This should not contain a namespace otherwise the full claim name will need to be entered - see http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname for more inform-

ation. See the example below:



9. On the Assignments tab, verify that each of the users or groups that should have access have been assigned to the application.
10. Under **SAML Signing Certificate**, click the **Download** link for the **Certificate (Base64)** and the **Metadata** file. These files are required in steps 4 and 5 in the

Configuring SAML topic.



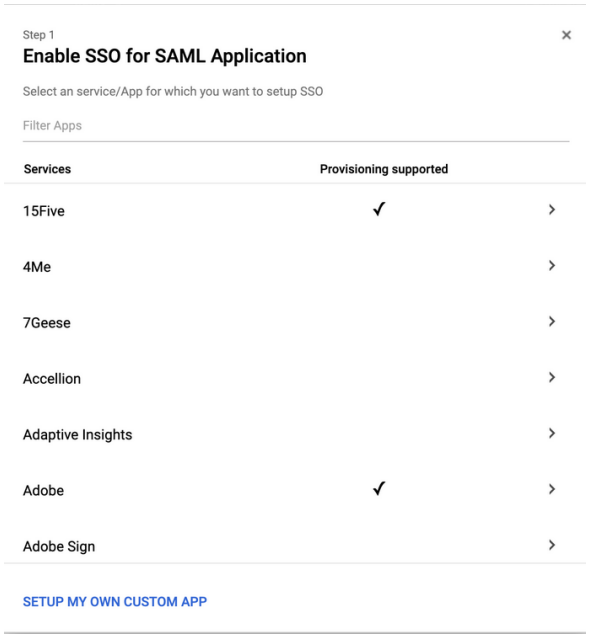
Google G Suite Service Provider Setup

The steps below detail how to add ThreatQ as a service provider in Google's G Suite. This process is required in order to complete the SAML setup.

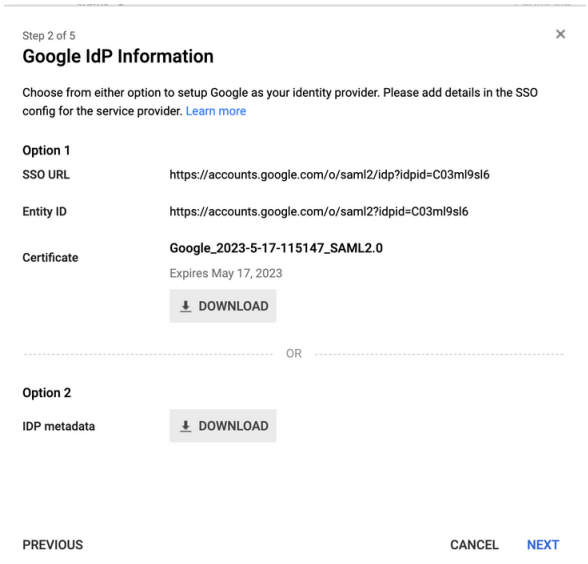
Setting Up the SAML App

1. Log into your **Google Administrative Console**.
2. Navigate to **Apps > SAML Apps**.
3. Click on the **+** icon located at the bottom-right on the page.

4. Select the **Setup my own custom app** option.



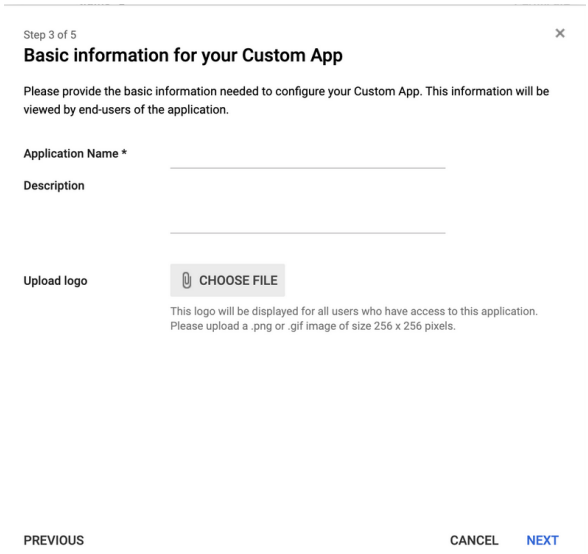
The Google IdP information page loads.



5. Click on **Next**.

6. Complete the *Basic Information for Your Custom App* fields:

Field	Description	Example
Application Name	The name of the application.	ThreatQ
Description	What function the app will serve.	SSO for ThreatQ Platform

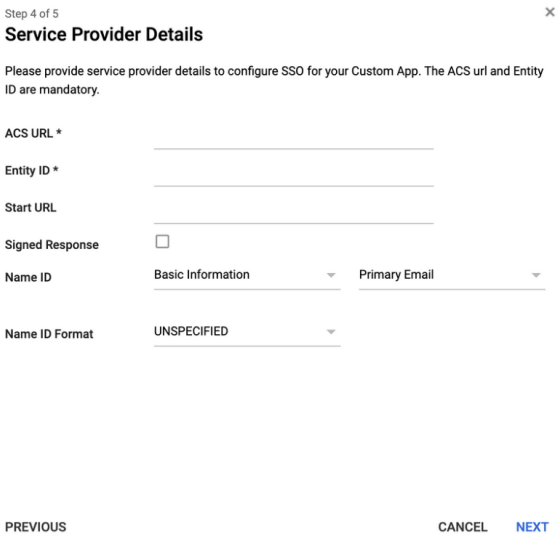


7. Click on **Next**.

8. Complete the *Service Provider Details* fields:

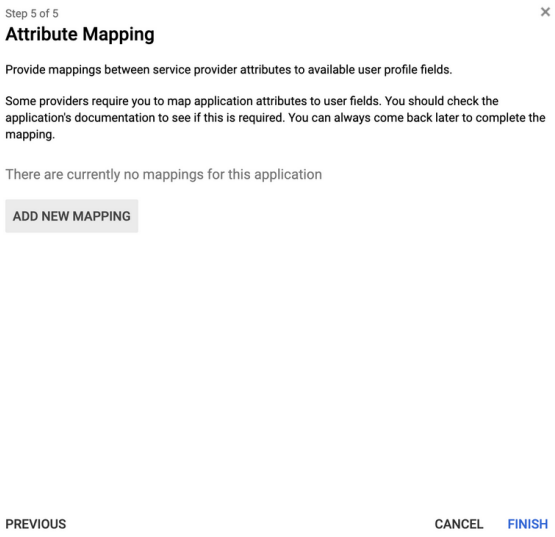
Field	Description	Example
ACS URL	Assertion Consumer Service is your ThreatQ URL + appended the “/api/saml/acs” string.	https://threatq.example.com/api/saml/acs
Entity ID	The Entity ID is your ThreatQ URL + appended with the “/ap-	https://threatq.example.com/api/saml/metadata

Field	Description	Example
	i/saml/metadata" string.	
Name ID Format	Set this field to **Email**.	N/A



9. Click on **Next**.

   The Attribute Mapping page loads.



10. Click on **Add New Mapping**.

> The **email** and **uid** attributes must be mapped to the **Primary Email** field.

11. Create the **email** mapping:

Attribute	Type	Google Data Field
email	Basic Information	Primary Email

12. Click on **Add New Mapping**.
13. Create the **uid** mapping:

Attribute	Type	Google Data Field
uid	Basic Information	Primary Email

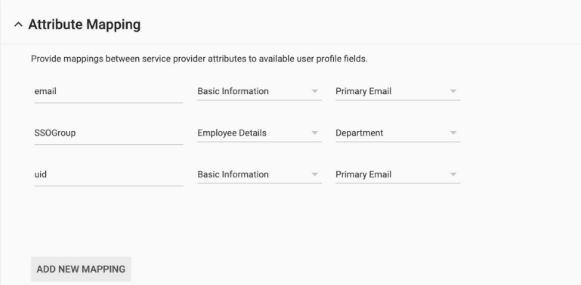
14. Click on **Add New Mapping**:

15. Create the **SSOGroup** mapping for ThreatQ roles:

Attribute	Type	Google Data Field
SSOGroup	Employee Details	< specific to your company >

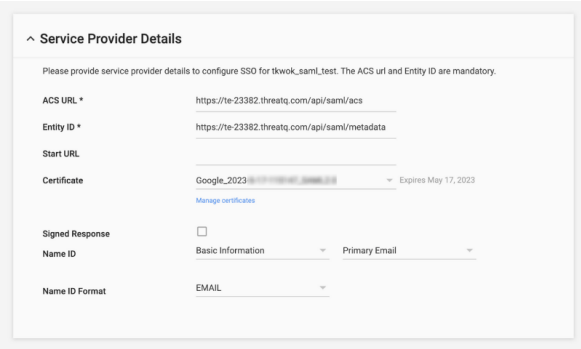
> Any attribute can be used for this mapping other than **Employee ID**. See the Creating custom attributes using the user schema Google support article for instructions on creating custom attributes to use for role mapping.

16. Your setup should now resemble the following screenshot:



17. Click on **Finish**.
18. Locate your new app under **Apps > SAML Apps**, click on the vertical ellipsis, and select **On for Everyone**.
19. Click on the app to open its settings details.
20. Click on **Service Provider Details**.

    The Service Provider Details page opens.



21. Click on **Manage Certificates**.
22. Download the **certificate** and the **IdP Metadata** files that are required in steps 4 and 5 in the Configuring SAML topic.

Okta Service Provider Setup

The steps below detail how to add ThreatQ as a service provider in Okta. This process is required in order to complete the SAML setup.

1. Log into the Okta web application.
2. Click on the **Admin** button located to the top-right of the screen.

   The Dashboard page loads.

3. Click on the **Applications** tab.

   The Application page loads.

4. Click on **Add Application**.

   The Add Applications page loads.

5. Click on **Create New App**.

   The Create New Application dialog box opens.

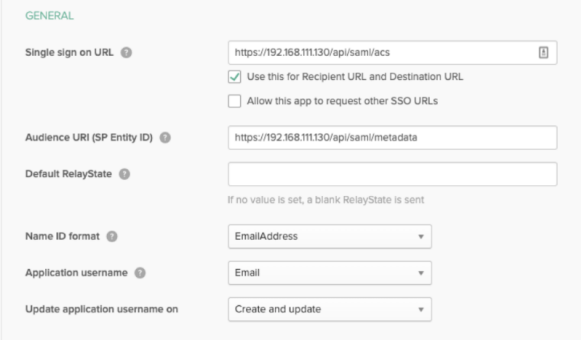
6. Select **Web** from the Platform dropdown.
7. Select **SAML 2.0** for the Sign on method.
8. Click on the **Create** button.

   The Create SAML Integration page opens with the General Settings tab selected.

9. Enter a name for the app in the **App Name** field.
10. Click on **Next**.

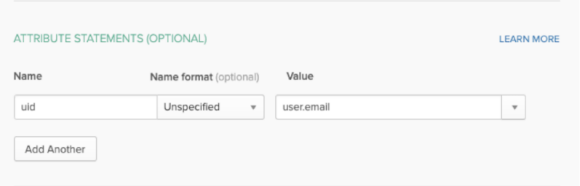
    The Configure SAML section loads.

11. Complete the following fields:



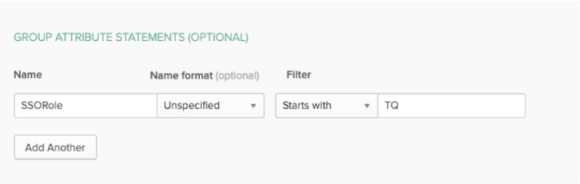
Field	Entry/Selection	Notes
Single sign on URL	https://< Host-name >.com/api/saml/acs	The Assertion Consumer Service (ACS) is your ThreatQ URL + appended the “/ap-i/saml/acs” string.
Audience URI (SP Entity ID)	https://< Host-name >/api/saml/metadata	The Audience URI is your ThreatQ URL + appended with the “/api/saml/metadata” string.
Default RelayState	https://< Host-name >/api/saml/acs	The Default RelayState is your ThreatQ URL + appended with the “/api/saml/metadata” string.
Name ID format	EmailAddress	
Application username	Email	ThreatQ requires that this field be set to Email.

12. Scroll down to the **Attribute Statements** section and add the following attribute:



Name	Name Format	Value
uid	Unspecified	user.email

13. Add the required attributes to the **Group Attribute Statements** that will be used to map Okta groups to ThreatQ user roles. In the example image below, an attribute called **SSORole** was created and is mapped to all Okta group names that starts with **TQ**.



> See Okta's Custom Expression help article for additional information on assigning an attribute.

14. Click on **Preview the SAML Assertion** to confirm that the settings are correct.
15. Click on **Next**.

    The Feedback section loads.

16. Select **I'm a software vendor. I'd like to integrate my app with Okta** and then click on **Finish**.

    The Application details page loads.

17. Click on the **Assignments** tab.

18. Click on the **Assign** dropdown and select **Assign to Groups**.
19. Assign the app to groups that will be used to map ThreatQ roles.
20. Click on **Save and Go Back**.
21. Click on **Done**.
22. Click on the **Sign On** tab.
23. In the **Sign On Methods** section, right-click and download the **Identity Provider metadata** file.
24. Click on the **View Setup Instructions** button.

    You will be able to review URL information such as the **Identity Provider Single Sign-On URL**, **Identity Provider Issuer**, and the **X.509 Certificate**.

25. Click on **Download Certificate**. The certificate and Identity Provider metadata file downloaded in step 23 are required in steps 4 and 5 in the Configuring SAML topic.

Date and Time Format

You can configure the date and time format of your choice system-wide within the ThreatQ platform.

If you make changes to the date and time format while another user is working concurrently in the same ThreatQ installation, that user must refresh their browser for the changes to take effect.

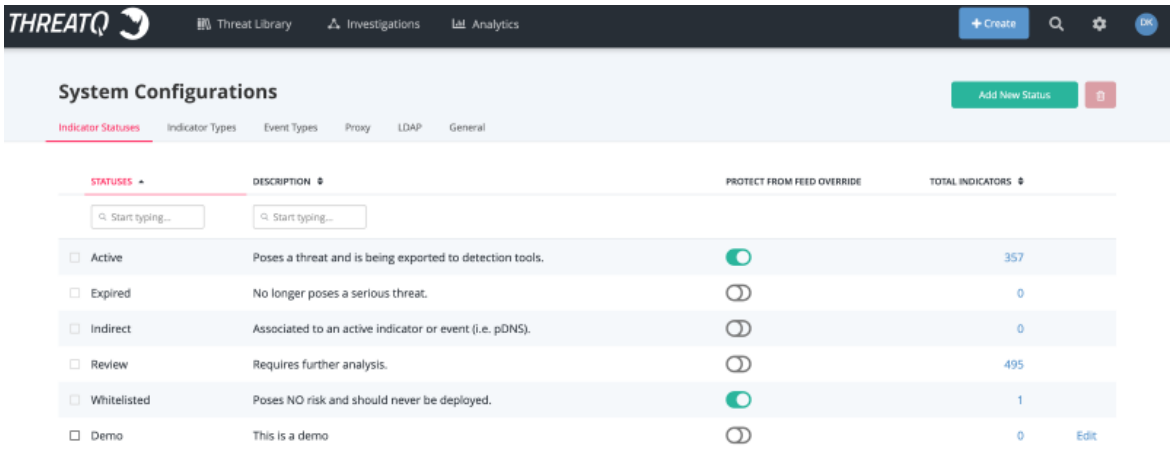
Related Topics:

- Configuring Date and Time Format

Configuring Date and Time Format

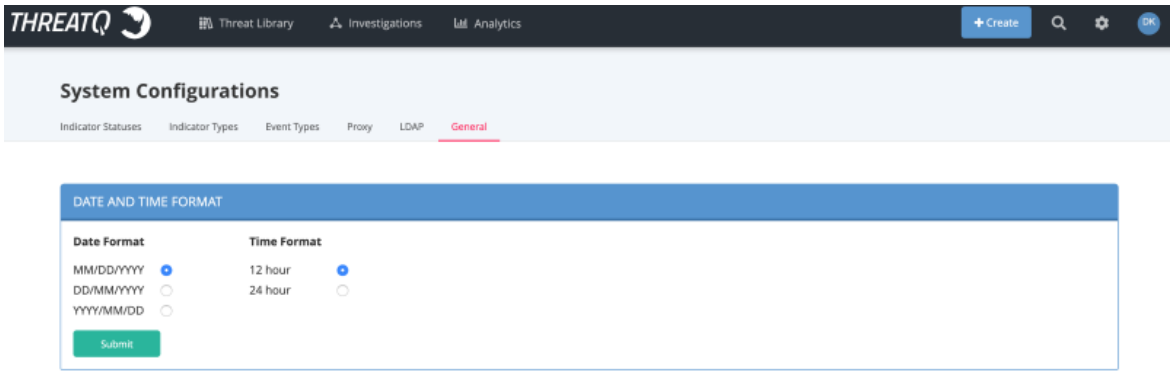
1. Navigate to **Settings** > **System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.



2. Click the **General** tab.

   The Date and Time Format tab opens.

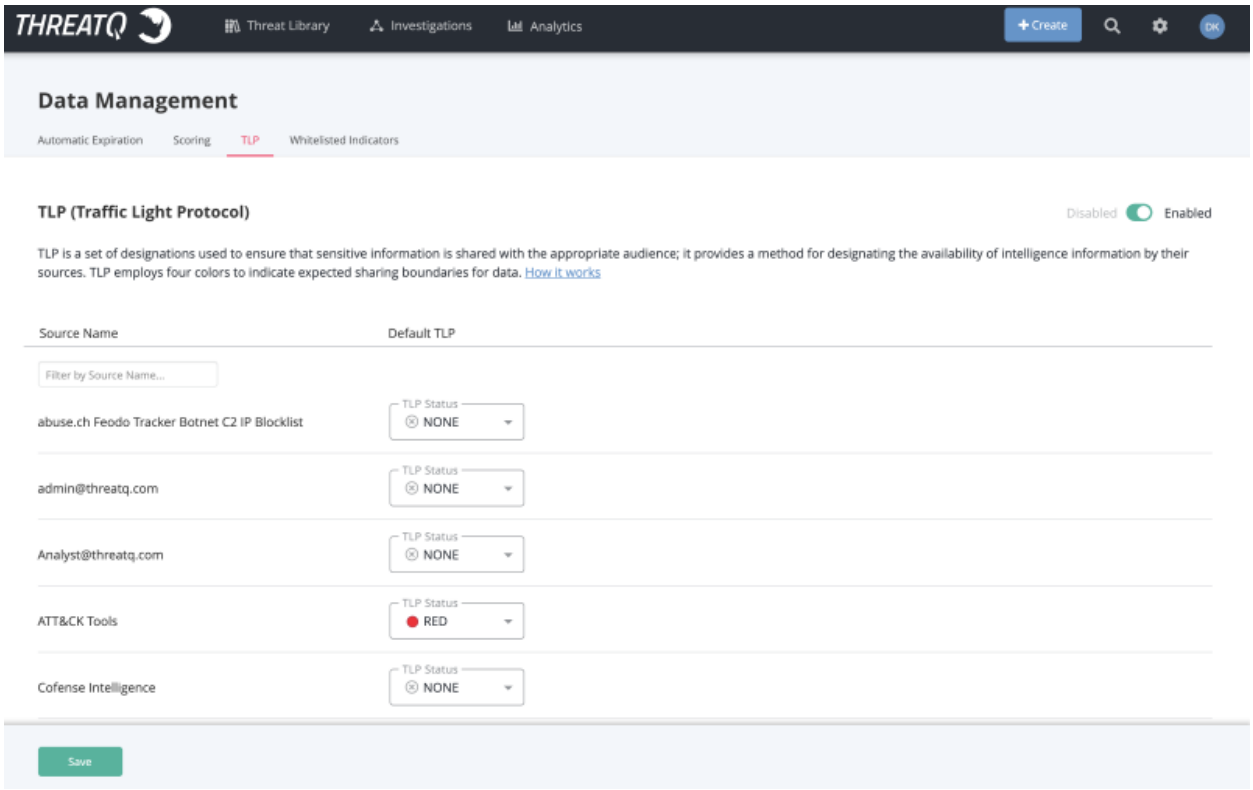


3. Select the desired **Date Format**. Options include: MM/DD/YYYY, DD/MM/YYYY, YYYY/MM/DD
4. Select the desired **Time Format**. Options include: 12 hour, 24 hours.
5. Click **Submit** to save your settings.

Traffic Light Protocol (TLP)

Traffic Light Protocol (TLP) schema provides a set of designations used to ensure that sensitive information is shared with the appropriate audience. ThreatQ provides a method for designating the availability of intelligence information by their sources. Users can also use TLP schema to filter objects when creating an export - see the Adding an Export topic for more details.

Administrators have the ability to configure TLP visibility settings for the ThreatQ application.



TLP employs four lights to indicate the expected sharing boundaries for data:

Light	Designation	Description
	Red	Not for disclosure, restricted to participants only.
	Amber	Limited disclosure, restricted to participant's organizations.

	Green	Limited disclosure, restricted to the community.
	White	Disclosure is not limited.

TLP Assignment Hierarchy

The ThreatQ TLP assignment hierarchy is as follows (highest to lowest precedence):

Method	Details
Manually Set	Using the Add New Source option when creating an object will allow you to select a TLP designation.
Source Provided Data	TLP information received from ingested data.
Source Default	Administrators can set a source's default TLP designation. See the Apply TLP Designation to Source topic for more details.
No TLP	A TLP designation has not been set for the source.

Access TLP Settings

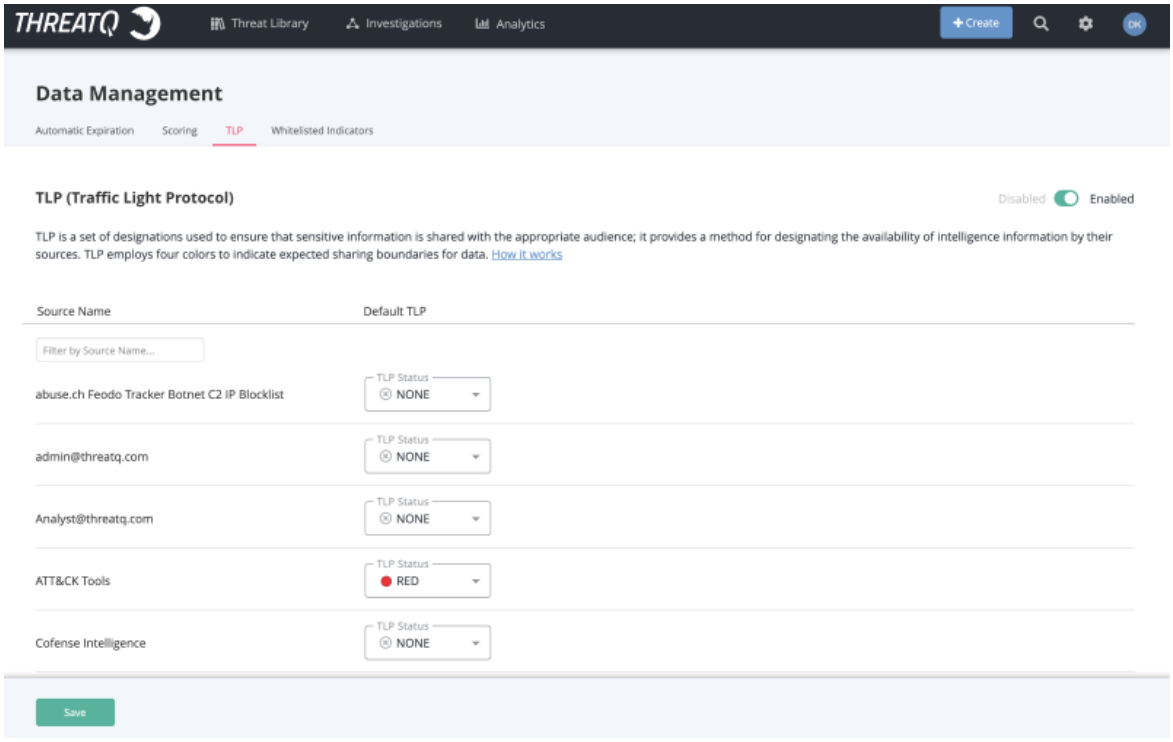
Users can manage TLP settings for system sources by accessing the **TLP** tab under the **Data Management** page.

1. From the main menu, select **Settings** > **Data Management**.

   The Data Management page will load with Automatic Expiration tab selected by default

2. Click on the **TLP** tab.

   The TLP Setting page will open.

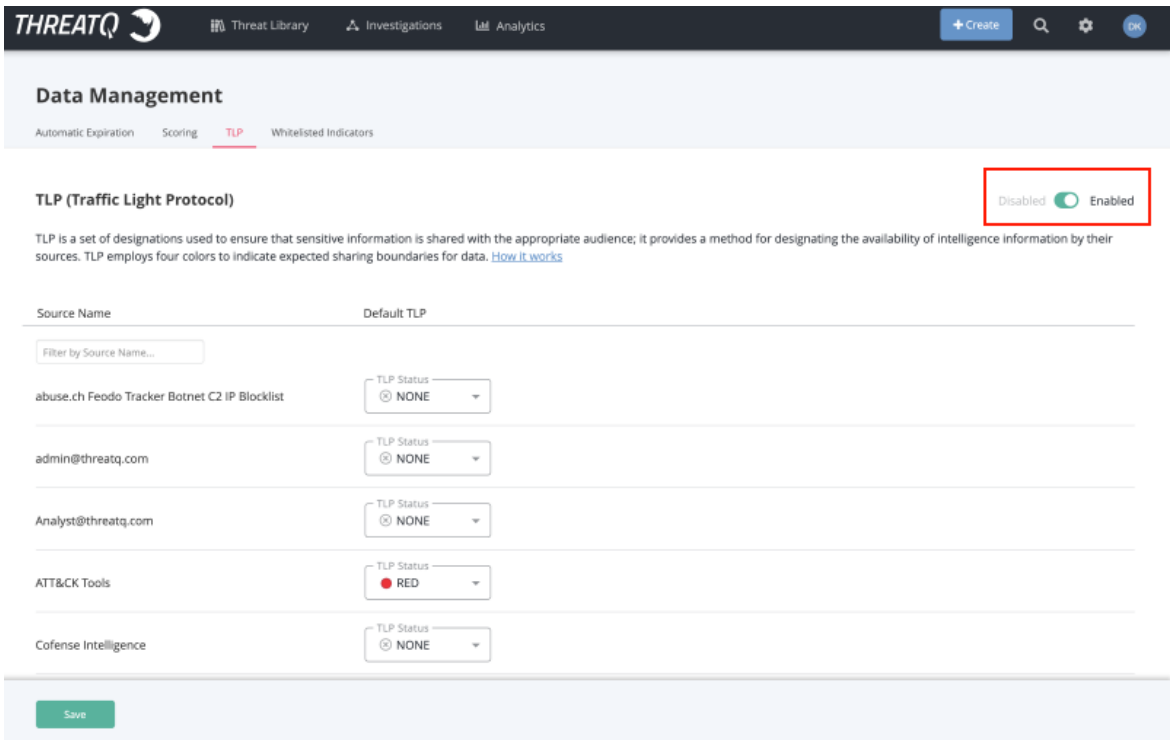


Configure TLP Visibility

System administrators can set visibility settings to either hide or show TLP designation lights to users.

From the TLP Settings Page (see the Access TLP Settings topic):

1. Click on the Enable/Disable toggle switch.



Enabled indicates that TLP designations are visible to users.

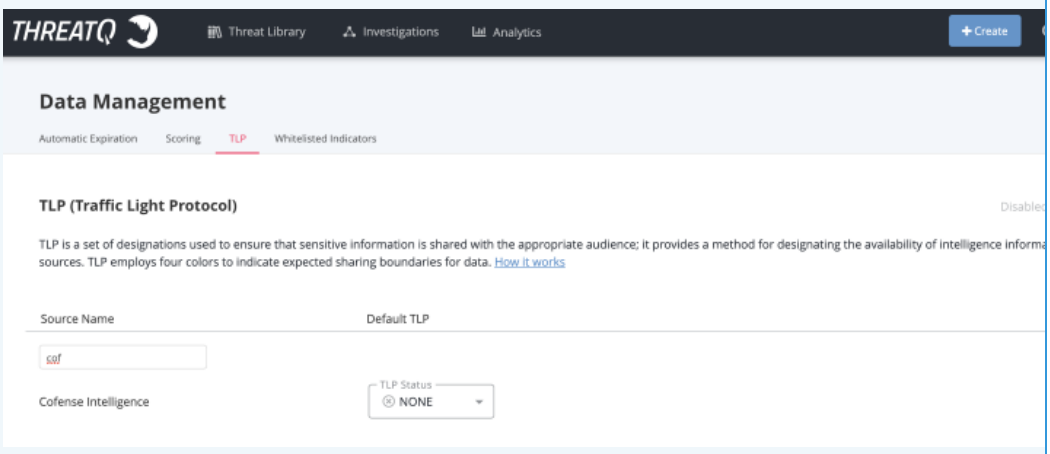
> Administrators will not need to click on the **Save** button, changes will be made upon clicking on the switch.

Apply TLP Designation to Source

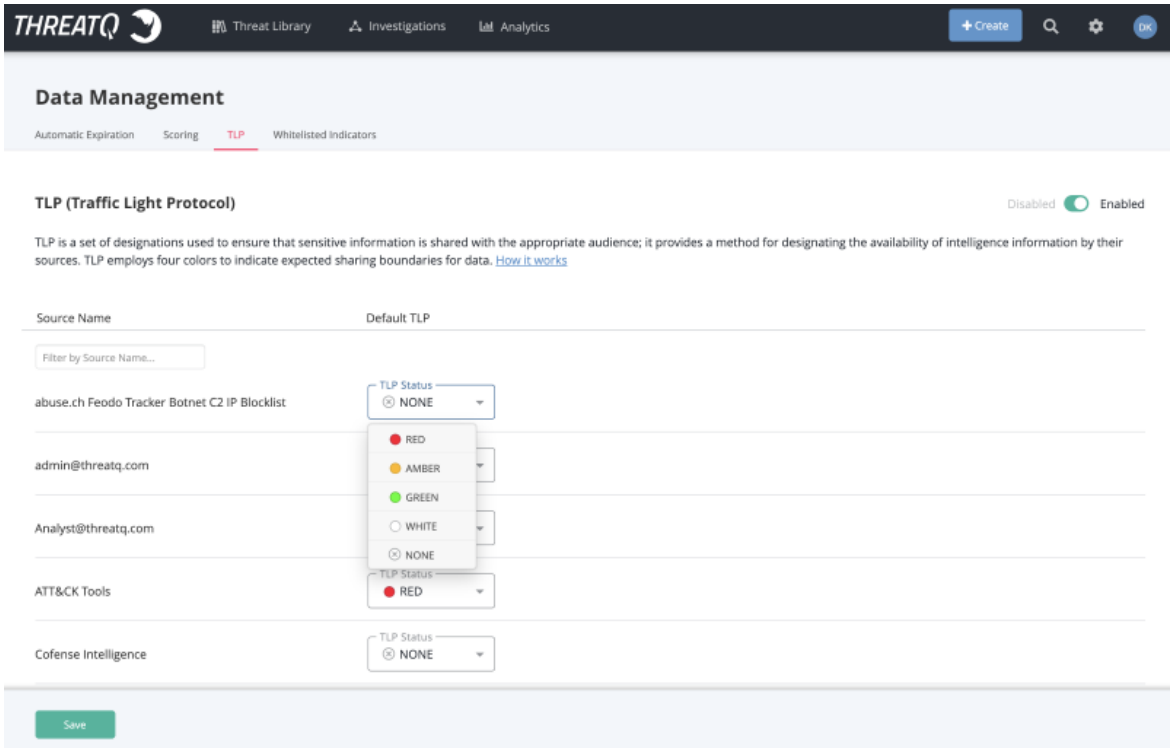
From the TLP Settings Page (see the Access TLP Settings topic):

1. Locate the source to update from the list provided.

You can use the Filter by Source Name field to locate the desired source.



2. Click on the TLP dropdown to the right of the source and select the appropriate TLP designation.



3. Click on **Save**.

You can override a source-default TLP designation when manually adding a source to an object. See the Adding a Source to an Object topic for more details.

Update TLP Schema using TLP Default - Command

Use the following command to update the TLP schema for an Object Source or Object Attribute Source with the source's default TLP designation.

See Apply TLP Designation to Source topic for more details on setting a default TLP designation for a source.

You should use this command to update your system to match default TLP configurations, specifically attributes and sources that were added to the Threat Library prior to the release of the TLP feature introduced with ThreatQ 4.11. This command will override previous TLP schema settings for a source including ones set by users. You will be prompted to confirm the action after entering the command. All updates will be recorded in the audit log.

The command will update using the default TLP designation. If a default designation is set to None, all references to the source will be updated to None.

Update All Sources

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Run the following command:

```
sudo php artisan threatq:apply-tlp-defaults
```

4. The application will warn you that this action is not reversible and will require user confirmation before proceeding.
5. Type **Yes** to confirm and proceed with the action.

The application will automatically be placed into maintenance mode. After the command has completed its operation, the application will be automatically be brought out of maintenance mode.

Update a Specific Source

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Run the following command:

```
sudo php artisan threatq:apply-tlp-defaults --
sources="<your source>"
```

You can apply the command to multiple sources by listing the sources in a comma-delimited format.
Example: --sources="CrowdStrike, AlienVault"

4. The application will warn you that this action is not reversible and will require user confirmation before proceeding.

5. Type **Yes** to confirm and proceed with the action.

The application will automatically be placed into maintenance mode. After the command has completed its operation, the application will be automatically be brought out of maintenance mode.

Convert TLP Command

Use the following command to update all object sources and object attribute sources that have TLP stored as an object attribute. This command will not affect TLP attributes that have already been converted. Users should use this command for new incoming data, such as migrating data into the system, which has TLP attributes but no TLP set.

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Place the application into maintenance mode - see the Maintenance Mode topic.
4. Run the following command:

```
sudo php artisan threatq:convert-tlp-attributes
```

5. Bring the application out of maintenance mode - see the Maintenance Mode topic.

Use Scenarios:

Object has one or more TLP Attributes with an invalid TLP (not currently in the TLP options)

- If the Object has just one TLP Attribute - none of its Sources or Attribute Sources will be updated.
- If the Object has more than one TLP Attribute - any Sources or Attribute Sources that match the Attribute Source of the TLP Attribute will not be updated.

Object has a single valid TLP Attribute

- All of the Object Sources and Object Attribute Sources will be updated to match the value of the TLP Attribute.

Object has multiple TLP Attributes

- Each TLP Attribute will be evaluated separately.
- Any Object Sources or Object Attribute Sources whose source matches that of the TLP Attribute will be updated with the value of the TLP Attribute.
- Any Object Sources or Object Attribute Sources whose sources do not match will not be updated.
- If there are no matches at all between the source of the TLP Attribute and any of the Object Sources or Object Attribute Sources, a new Object Source will be added using the Attribute's TLP value. Each of the Object Attributes will receive a new Object Attribute Source with the TLP value as well.

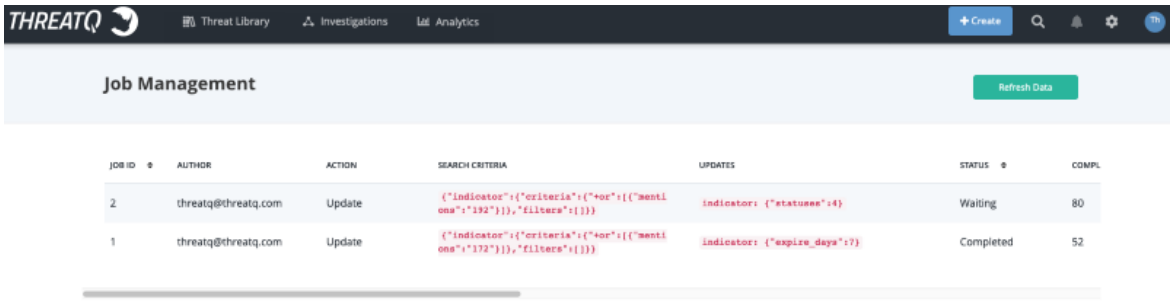
Job Management

> The Job Management page is only accessible to users with Administrator or Maintenance accounts.

The Job Management page allows you to view the status and outcome of Bulk Actions.

To access the Job Management page:

1. Navigate to **Settings** > **Job Management**.



Related Topics:

- Viewing Job Details

Viewing Job Details

The Job Management page allows you to view the following details about a Bulk Action job:

Field	Description
Job ID	The unique ID assigned to the job.
Author	The user that initiated the job.
Action	The Bulk Action selected.

Field	Description
Search Criteria	The search filters used to select the system objects for the job.
Updates	The Bulk Action being performed on the system objects selected. **Example:** If you were to run a Bulk Action on a set of indicators to expire on 2-29-2020, the Updates field will display: indicator: `{"expires_ats" : "2020-02-29"}`
Status	The current status of the job. Possible statuses include: • Created - The job has been queued. • In-Progress - The job is running. • Error - The job failed. • Waiting - The job is waiting for indexing to be complete. This only applies to the Bulk Change process. • Completed - The job has completed.
Completed	The timestamp of when the job completed.
Total	The total number of objects included in the job.
PID	The process ID of the worker executing the job.
Percent Completed	This represents the amount of system objects associated with the job that have been processed. **Example:** 100 indicators out of the 1000 associated with the job have been deleted = 10%.
Estimated Time	The estimated time remaining until the job is complete.

Field	Description
Remaining	
Date Created	The timestamp of when the job was created and queued.
Updated At	The timestamp of when the job or an system object associated with the job was last updated.
Start Time	The timestamp of when the job was started.
Completed At	The timestamp of when the job completed.
Failed At	If the job failed. the timestamp of when it failed.

Threat Library

The Threat Library is the central repository within ThreatQ that organizes and combines external and internal threat data.

The Threat Library can be broken down into three segments:

System Objects
Threat data, both ingested and manually added, is referred to as System Objects and is sorted and categorized by object type.

Advanced Search
The Advanced Search page is the primary interface for the Threat Library that allows you to search, filter, and sort through System Objects.

Object Details
The Object Details page allows you view detailed information about a specific object.

Advanced Search

The Advanced Search page is the primary interface for the Threat Library. You can search for any system object within the application, filter returned system objects, and apply bulk changes to search results. You can click on an individual object to navigate to its details page.

Depending on how you have navigate to the Threat Library will determine which object types appear on the page.

Threat Library Navigation Menu

You can click on **Threat Library > Object Type** to open the advanced search for a particular object type or select **Browse All**. You can also select which object types appear in your Threat Library view - see Selecting Object Type View for more details.

Search Link

You can click on **Search > Advanced Search** to open the advanced search for all object types within the Threat Library.

Refining Search Results

You can use Context Filters, Date Filters, Status Filters, Tasks Filters, and Types Filters to narrow down your search for a specific object or object type.

Related Topics:

- Performing an Advanced Search
- Managing Search Columns
- Exporting Search Results to CSV
- Managing Saved Searches
- Bulk Actions
- Filter Sets

Performing an Advanced Search

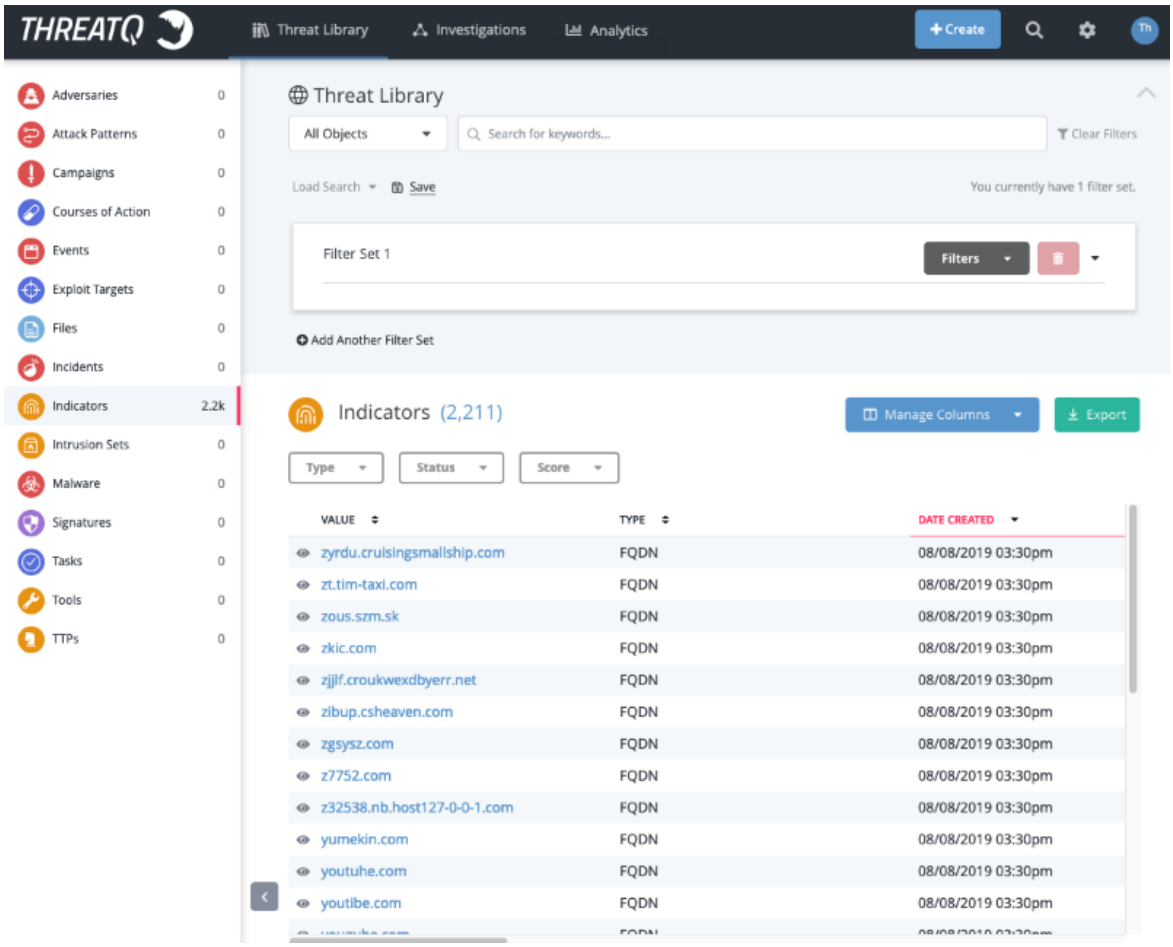
You can also click on **Threat Library** > **Browse All** to navigate to the advanced search page or click **Threat Library** >**Object Type** to navigate to the advanced search page for a specific object type.

To perform an advanced search:

1. Choose the Search icon.

2. In the Search dialog box, choose **Advanced Search**.

   The Advanced Search page opens.



3. Choose your object search category by selecting an object type from the Filters dropdown list or selecting an object type from the left-hand list.

   > See the Filter Sets topic for more information on narrowing down your search.

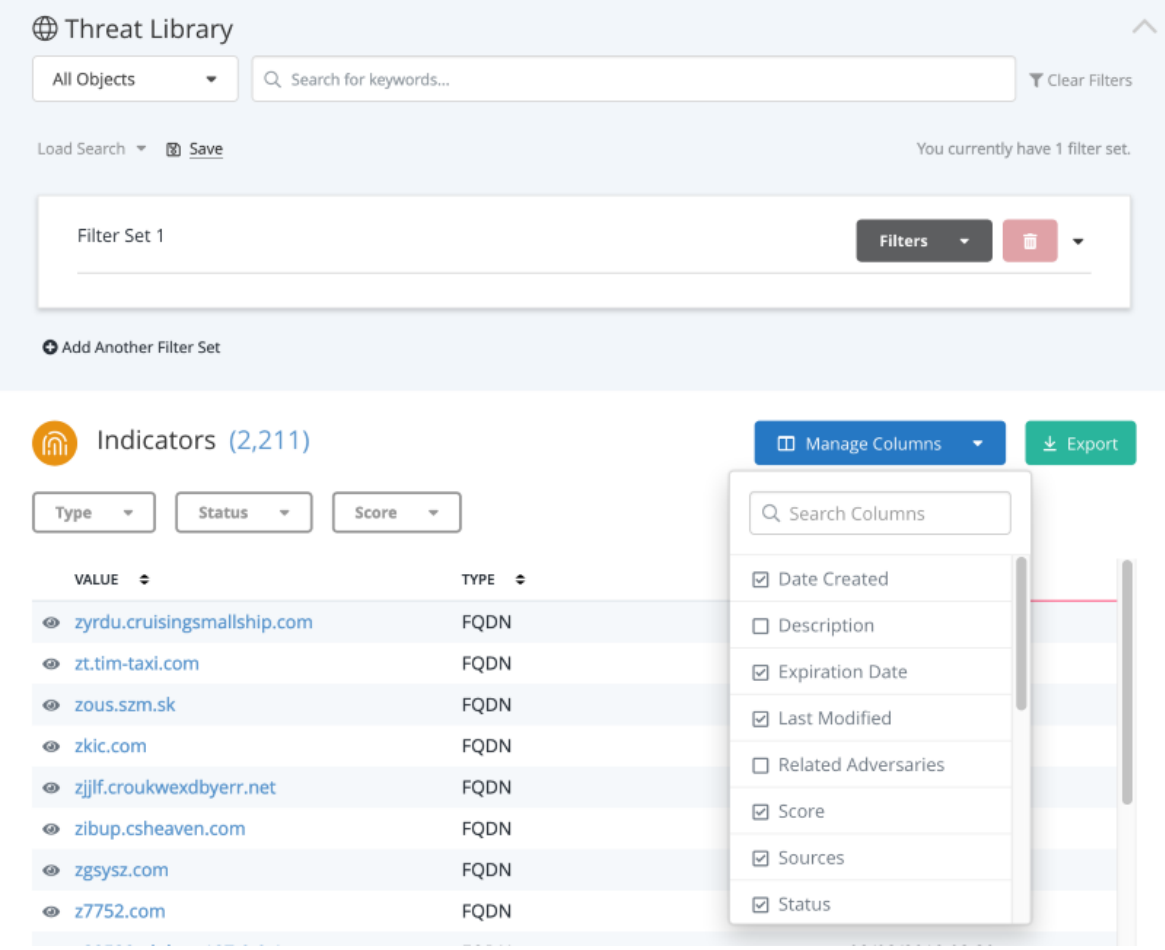
4. Use the **Not** checkbox to indicate whether search results will include or exclude the filter set.
5. Press Enter or Return.
6. Optionally, repeat steps 3 and 4 to further narrow your search.

Managing Search Columns

You can choose which columns to display in your search results.

To select columns:

1. Navigate to the Advanced Search page.
2. Choose **Manage Columns**.



3. Select the columns you wish to display. Clear the columns you wish to hide.

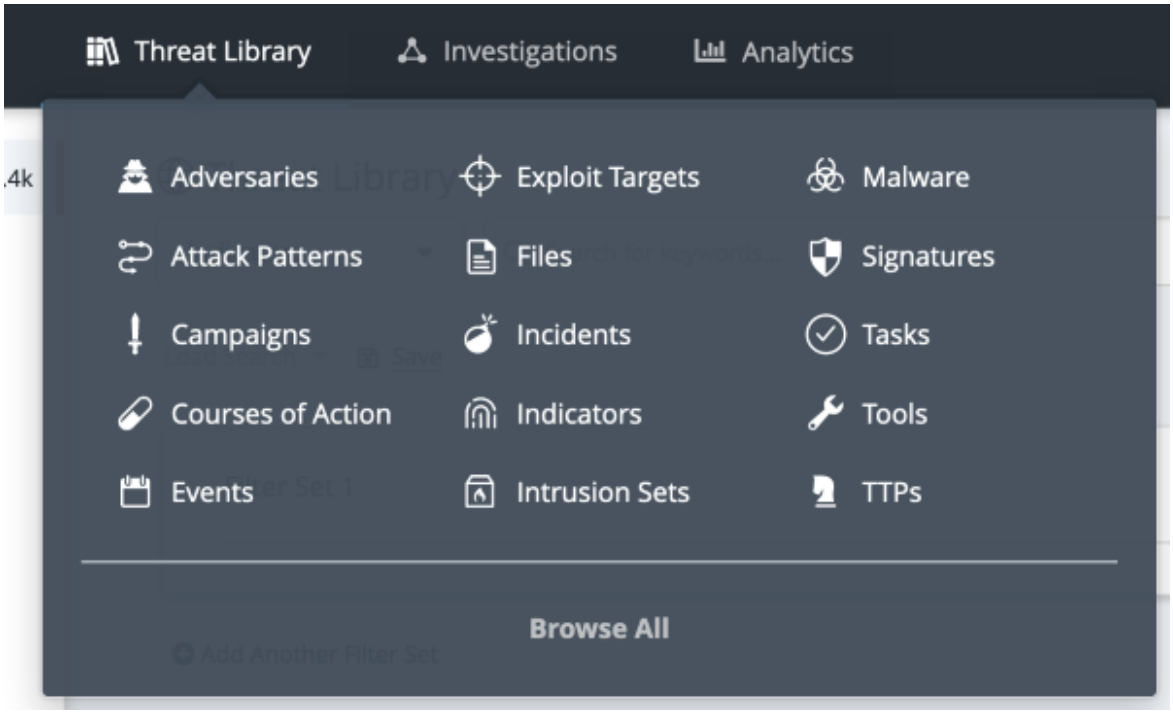
Selecting Object Type View

You can select which object types appear in your view of the Threat Library using the following methods:

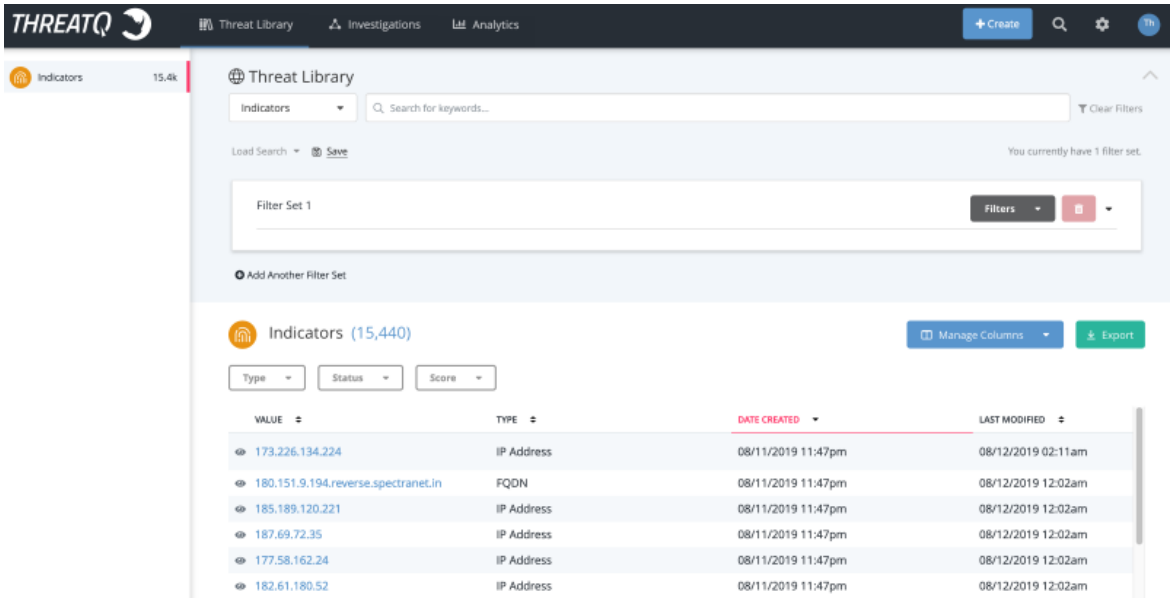
> The methods listed below will not be added to your filter set. See the Filtering by Object Type topic for details on how to add object type filtering to your filter sets.

Threat Library Navigation Menu:

1. Click on the **Threat Library** navigation dropdown and select an **Object Type**.



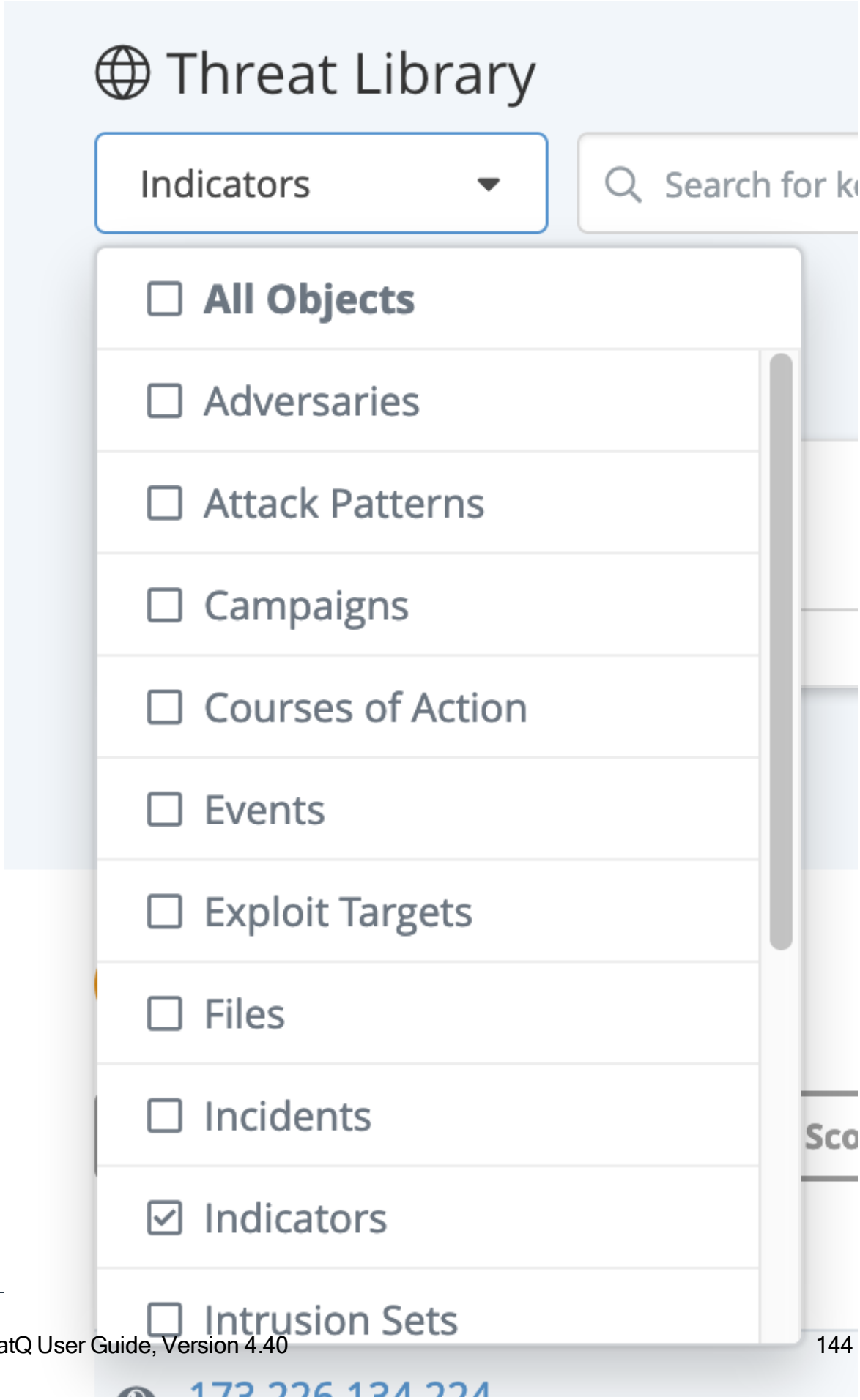
The Advanced Results page opens with the applied object type filter.



Object Type Dropdown List

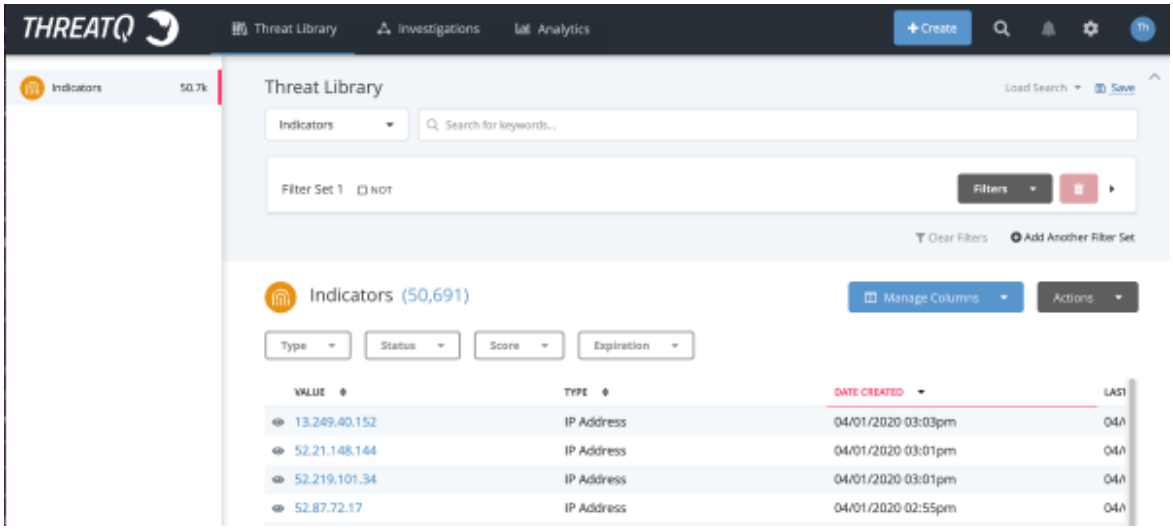
You can use the Global Filter dropdown list to select more than one object type.

1. Click on the **Object Type** dropdown list and select one or more object types.


Threat Library
Indicators
Search for k
All Objects
Adversaries
Attack Patterns
Campaigns
Courses of Action
Events
Exploit Targets
Files
Incidents
Indicators
Intrusion Sets

The Advanced Search Results page updates the list with the selected object type (s)

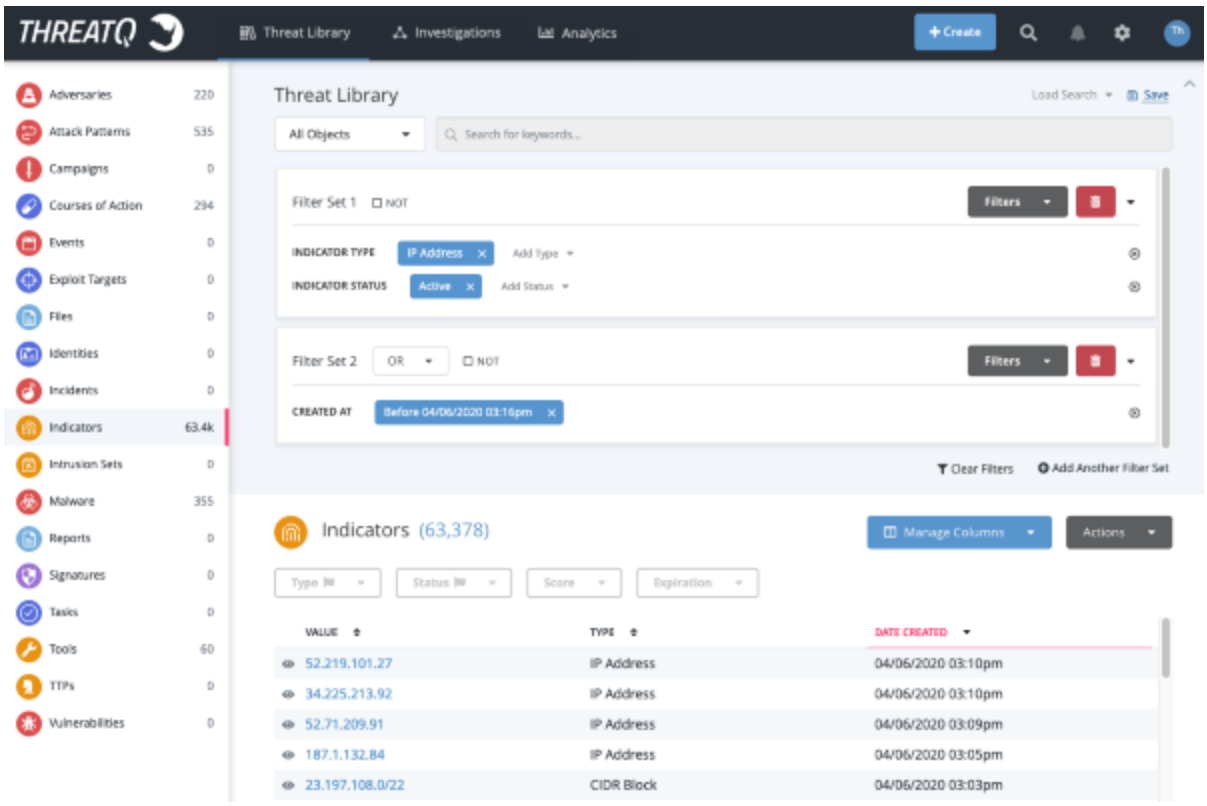
.



Filter Sets

Filter Sets allow you to create multiple sets of filters that can be applied to the threat library at the same time using AND/OR logic. You can also save your Filter Sets using the Save

Search option - see the Saving Searches topic for more details.



Related Topics:

- Adding Filter Sets
- Editing Filter Sets
- Deleting Filter Sets
- And/Or Order of Operations

Filter Options:

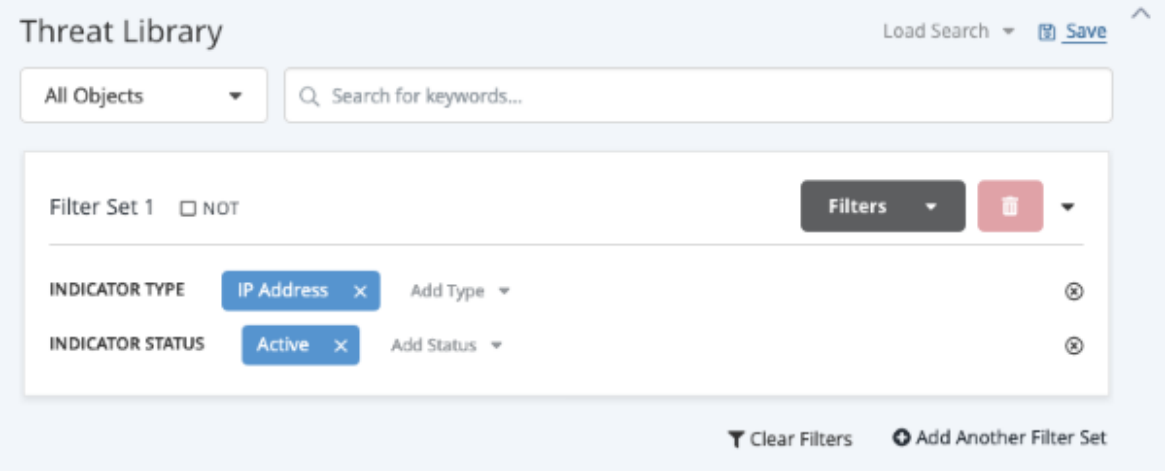
- Date Filters
- Context Filters
- Types Filters
- Status Filters

Adding Filter Sets

To Add a Filter Set to the search results:

From the Advanced Search page:

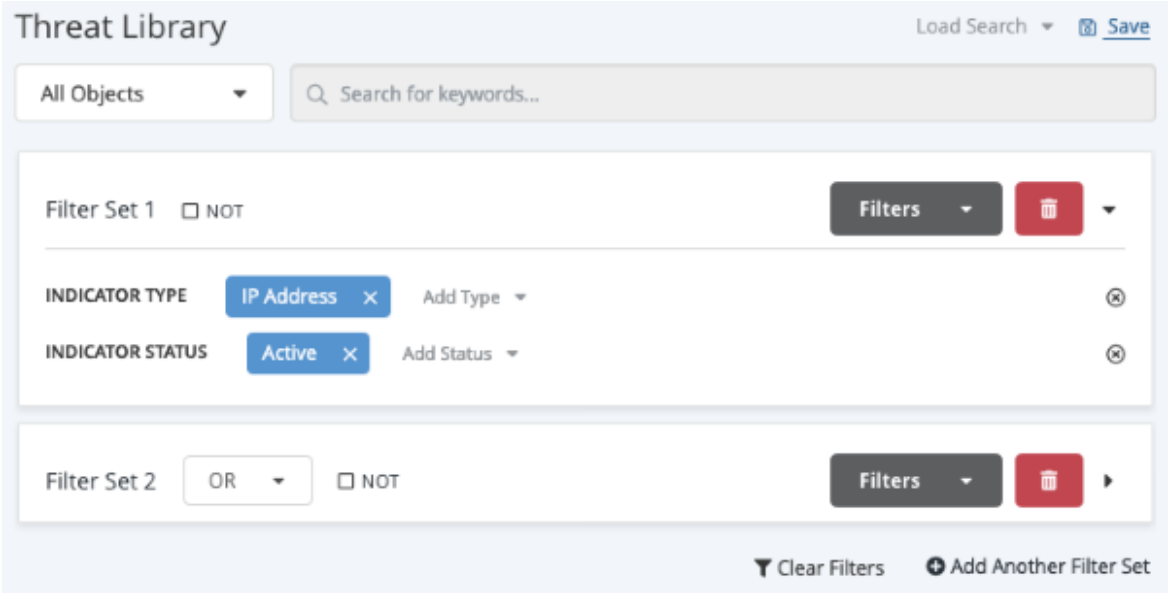
1. Use the **NOT** checkbox to determine if the filters in the initial filter set will be used to include or exclude Threat Library objects.
2. Select one or more filters for the search.



You can use the search box provided at the top of the filters drop-down to narrow down the list of available filters.

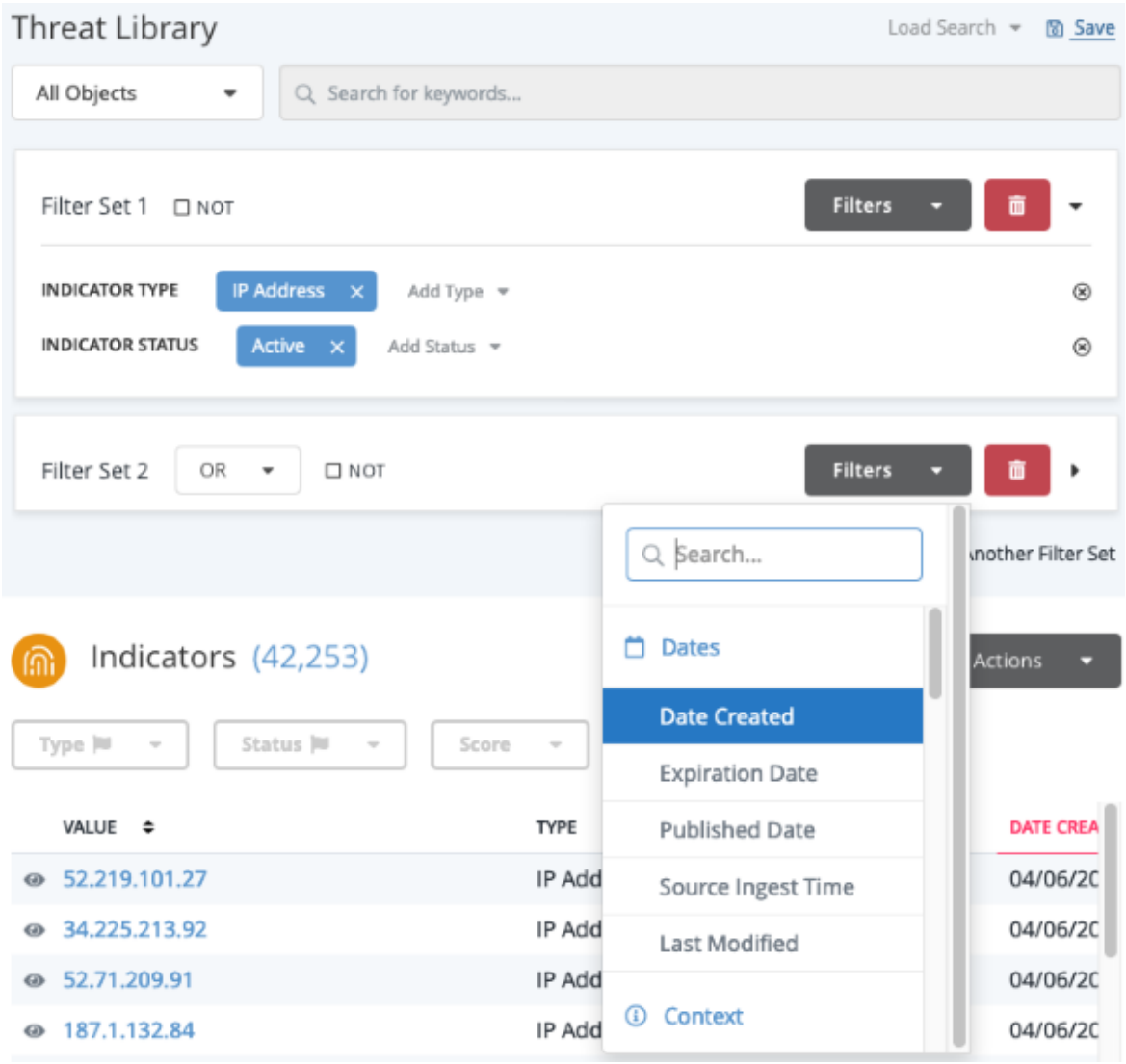
3. Click on **Add Another Filter Set**.

   A new Filter Set table will load below the first set.

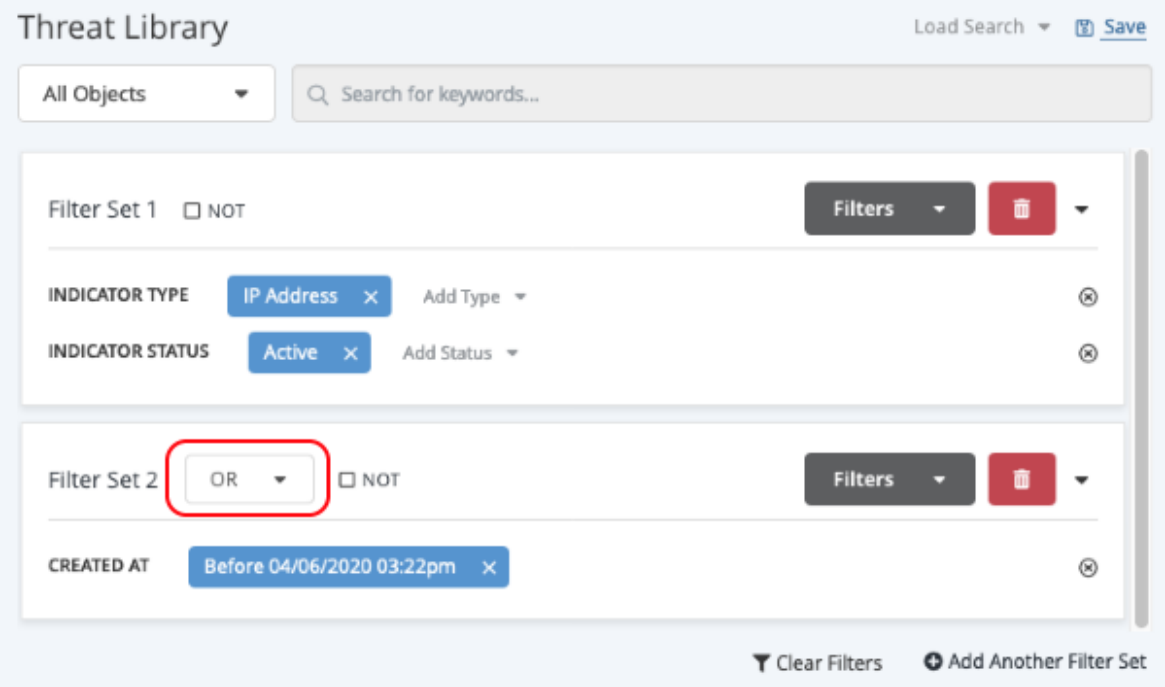


4. Use the **Not** checkbox to determine if the filters in the new filter set will be used to include or exclude Threat Library objects.

5. Use the Filters dropdown next to the new filter set to add filters.



6. Click on the **And/Or** dropdown to set the **And/Or** logic for the Filter Sets. See the And/Or Order of Operations topic for more details.



Repeat steps 3-6 to add additional filter sets.

Editing Filter Sets

The steps to editing a filter within a Filter Set may differ based on the type of filter.

Editing Filter Set Filter Values

Filter	Steps
Dates	
Date Created	1. Click on the pencil icon located to the right of the value. The Date Created dialog box opens. 2. Update the date values and click **Save**.
Last Modified	1. Click on the pencil icon located to the right of the value. The Last Modified dialog box opens.

Filter	Steps
	2. Update the date values and click **Save**.
Context	
Keyword	Keywords already applied to the filter cannot be edited and must be deleted. Perform the following: 1. Click on the **X** next to the existing keyword to delete it. 2. Click on the **Filters** dropdown and select **Keyword**. The Filter by Keyword dialog box opens. 3. Enter the new keyword and click **Add**.
Relationship	Related objects already applied to the filter cannot be edited and must be deleted. Perform the following: 1. Click on the **X** next to the existing related object to delete it. 2. Click on the **Filters** dropdown and select **Relationship**. The Filter by Relationship dialog box opens. 3. Use the search box to locate the object and click **Add**.
Indicator Score	1. Click on the **Update Score** option next to the existing score filter. The Define Your Score dialog box opens. 2. Adjust the score range and click **Submit**.
Source	Sources already applied to the filter cannot be edited and must be deleted. Perform the following: 1. Click on the **X** next to the existing source to delete it.

Filter	Steps
	2. If another source filter exists, click on **Add Source** option otherwise click on the **Filters** dropdown and select **Source**. The Source dialog box opens. 3. Use the search box to locate the source.
Tag	Tags already applied to the filter cannot be edited and must be deleted. Perform the following: 1. Click on the **X** next to the existing tag to delete it. 2. If another tag filter exists, click on **Add Tag** option otherwise click on the **Filters** dropdown and select **Tag**. The Tag dialog box opens. 3. Use the search box to locate the tag.
Value Contains	Values already applied to the filter cannot be edited and must be deleted. Perform the following: 1. Click on the **X** next to the existing value to delete it. 2. Click on the **Filters** dropdown and select **Value Contains**. The Value Contains dialog box opens. 3. Select an Object, enter a Value, and click **Add**.
With Attribute	With Attribute values already applied to the filter cannot be edited and must be deleted. Perform the following: 1. Click on the **X** next to the existing value to delete it. 2. Click on the **Filters** dropdown and select **With Attribute**. The With Attribute dialog box opens.

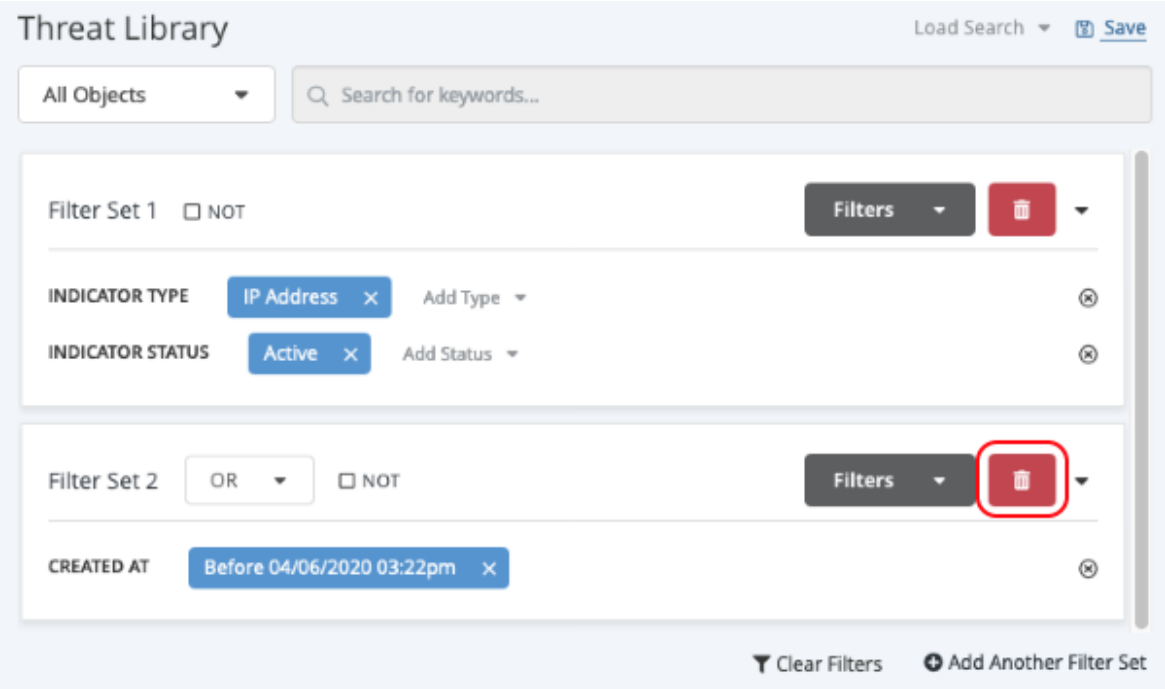
Filter	Steps
	3. Select an Attribute, enter a Value, and click **Add**.
Without Attribute	Without Attribute values already applied to the filter cannot be edited and must be deleted. Perform the following: 1. Click on the **X** next to the existing value to delete it. 2. Click on the **Filters** dropdown and select **Without Attribute**. The Without Attribute dialog box opens. 3. Select an Attribute, enter a Value, and click **Add**.
Types	
Object Type (Indicator, Event, Signature, File)	1. Click on the **Add Type** next to the existing types. The Type dialog box opens. 2. Use the checkboxes to select and unselect types.
Statuses	
Object Status (Indicator, Signature, Task)	1. Click on the **Add Status** next to the existing status. The Status dialog box opens. 2. Use the checkboxes to select and unselect statuses.

Deleting Filter Sets

Deleting a Filter Set removes it from the search results and cannot be undone.

To Delete a Criteria Set:

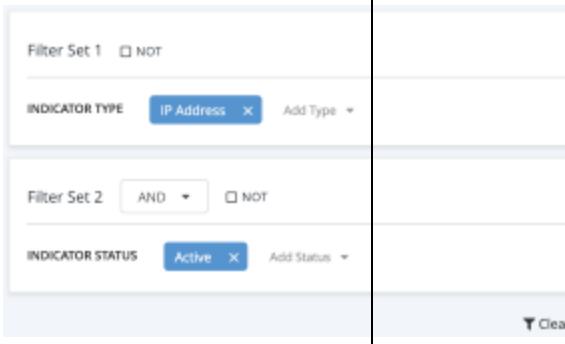
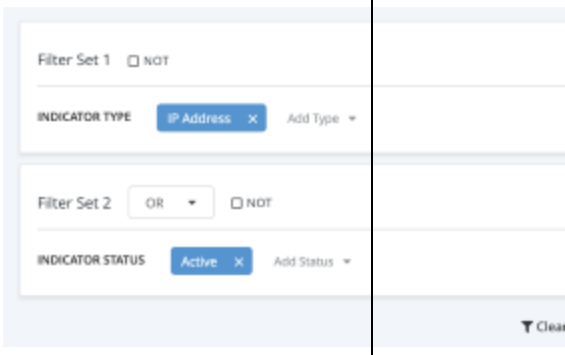
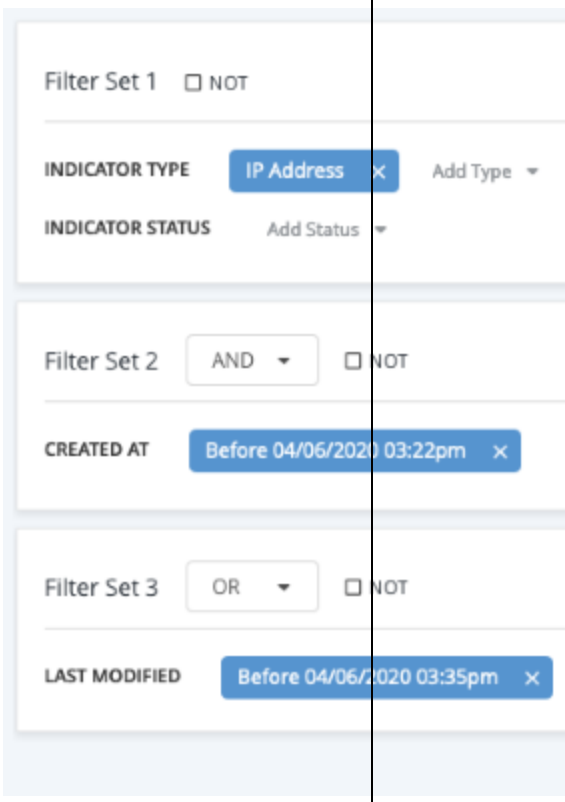
1. Click on the delete icon located next to the right of the Filter Set's name.

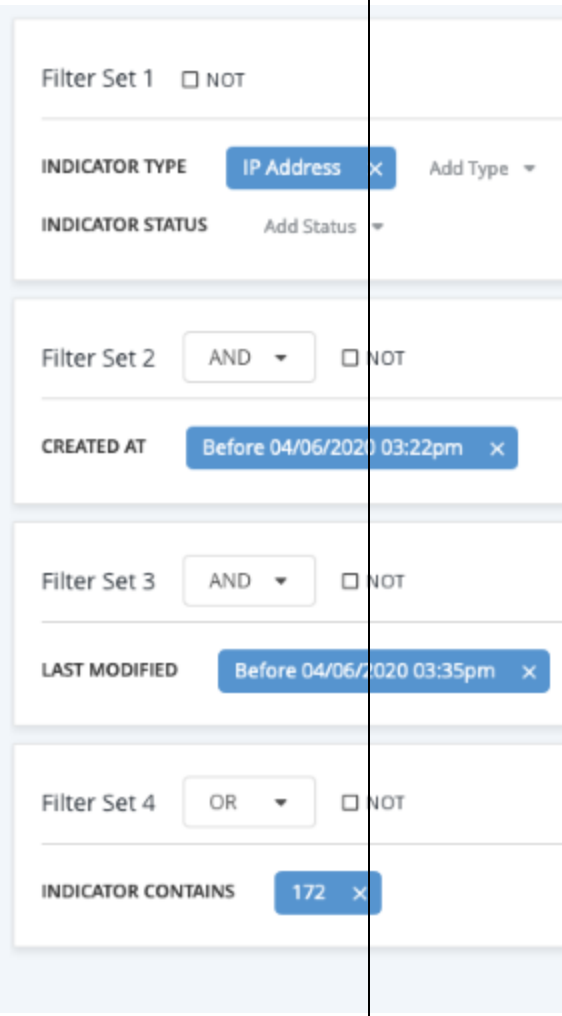


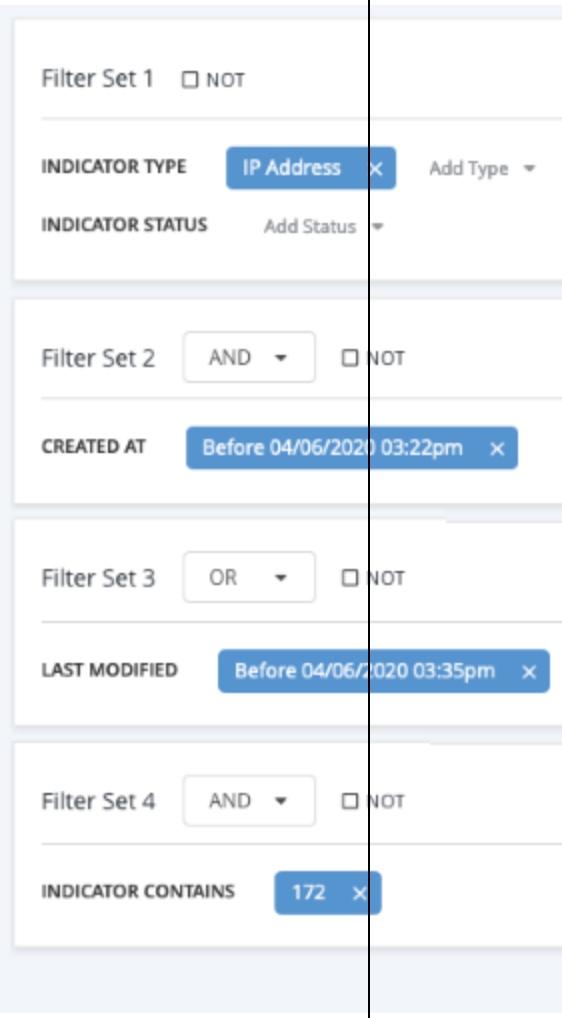
You can click on **Clear Filters**, located beneath the filter sets, to remove all filter sets from the current search.

And/Or Order of Operations

Filter Set AND/OR logic follows the standard mathematical order of operations with ANDs being executed before ORs. The table below provides different scenarios and examples for Filter Sets.

Scenario	Order	Example
Single AND	Filter 1 AND Filter 2	
Single OR	Filter 1 OR Filter 2	
Single AND, Single OR	(Filter 1 AND Filter 2) OR Filter 3	

Scenario	Order	Example
Multiple ANDs, Single OR	(Filter 1 AND Filter 2 AND Filter 3) OR Filter 4	

Scenario	Order	Example
Multiple ANDs, Multiple ORs	(Filter 1 AND Filter 2) OR (Filter 3 AND Filter 4)	

Date Filters

Date filters allow you to filter advanced search results by date-related values.

Additional Topics:

- Filtering by Date Created
- Filtering by Last Modified
- Filtering by Published Date

- Filtering by Source Ingest Time
- Filtering by Expiration Date

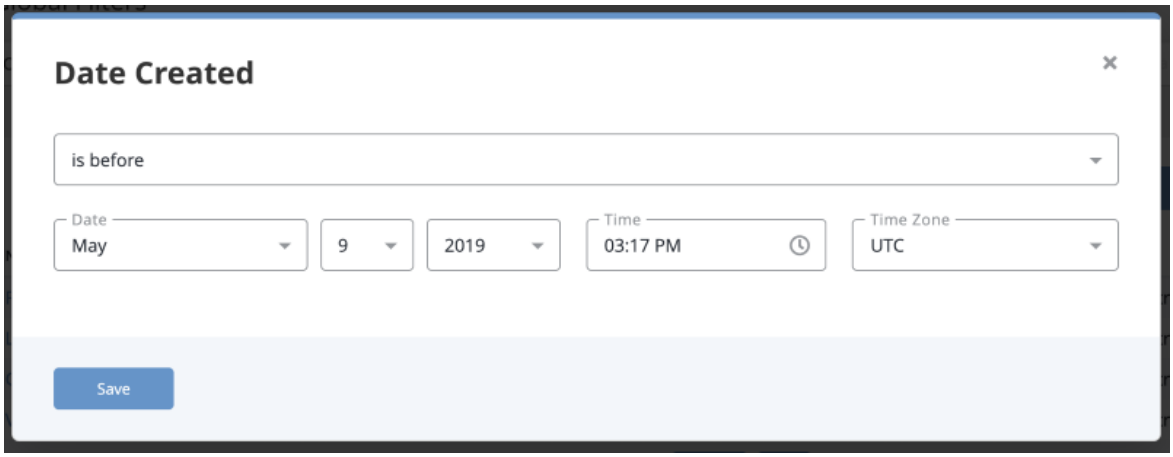
Filtering by Date Created

Complete the following procedure to filter Advanced Search results by the date the objects were created.

To filter by Date Created:

1. Click on the **Filters** option and select **Date Created**.

   The Date Created dialog box opens.



2. Select one of the following options to determine how the filter is applied:

Option	Result
is before	Search results include items before a selected date
is after	Search results include items after a selected date
is in the range of	Search results include items in a selected range of dates
is within the last	Search results include items within the selected number of days.

3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

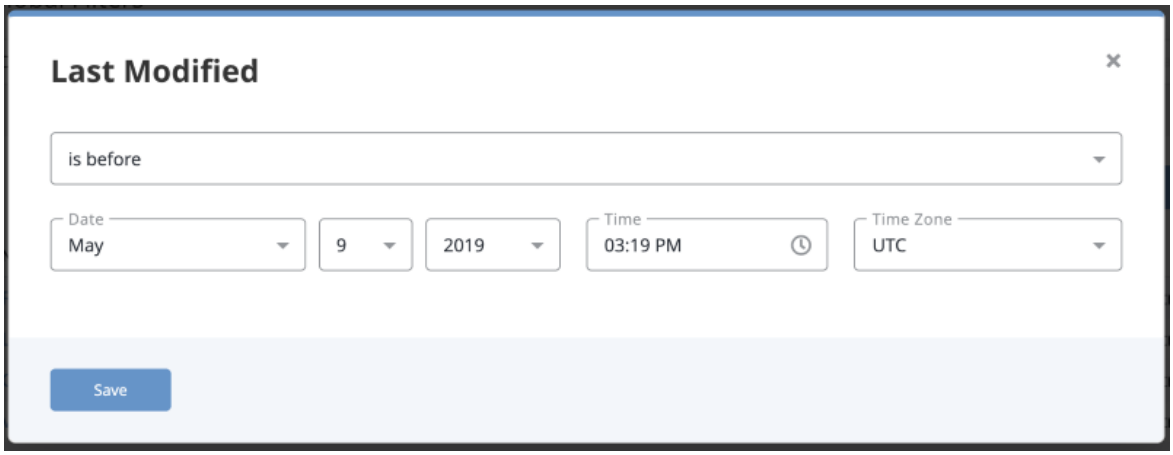
Filtering by Last Modified

Complete the following procedure to filter Advanced Search results by the date objects were last modified.

To filter by Last Modified:

1. Click on the **Filters** option and select either **Last Modified**.

   The Last Modified dialog box opens.



2. Select one of the following options to determine how the filter is applied:

Option	Result
is before	Search results include items before a selected date
is after	Search results include items after a selected date
is in the range of	Search results include items in a selected range of dates
is within the last	Search results include items within the selected number of days.

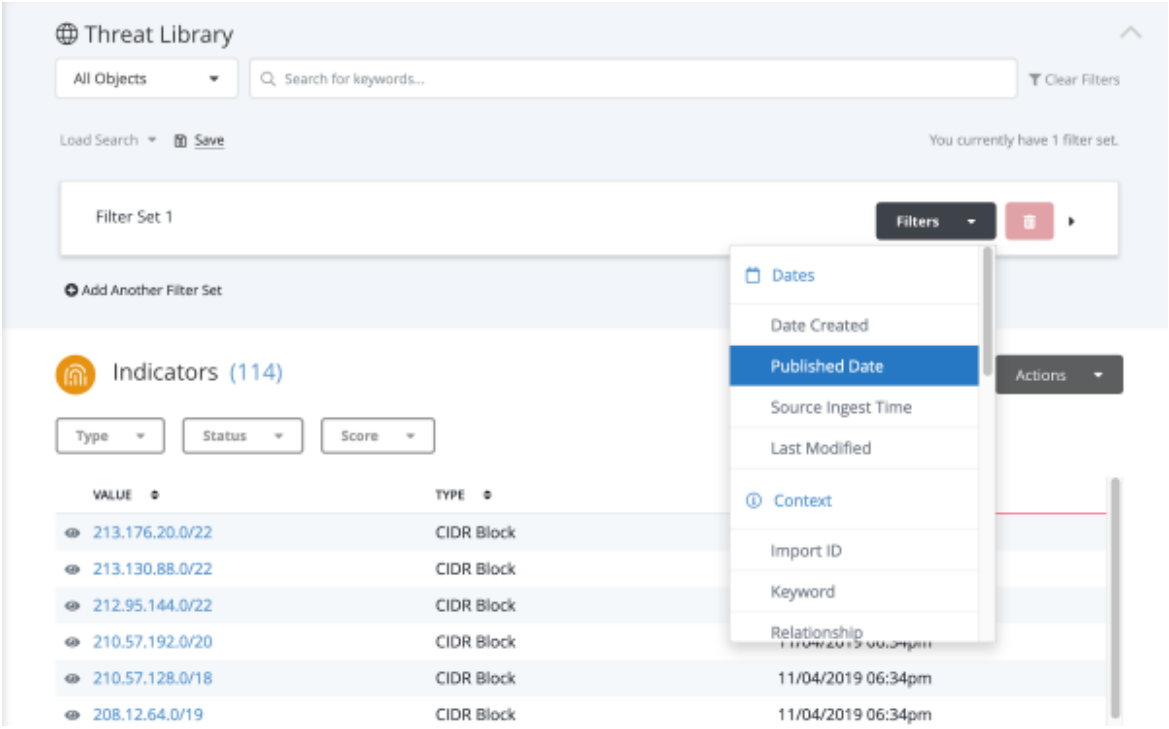
3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

Filtering by Published Date

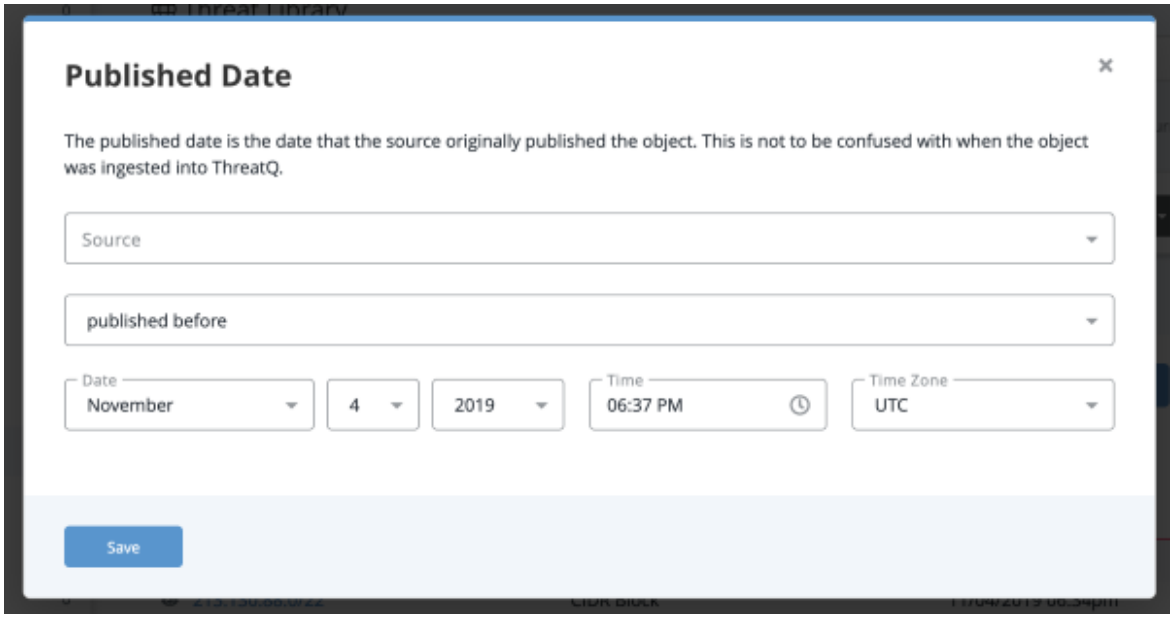
> The Published Date is the date that an object was originally published by the source. This is not to be confused with when the object was ingested into ThreatQ.

To filter by Published Date:

1. Click on the **Filters** dropdown option for a filter set and select **Published Date**.



The Published Date dialog box opens.



2. Select the **Source** that published the object.
3. Select one of the following options to determine how the filter is applied:

Option	Result
published before	Search results include items before a selected date
published after	Search results include items after a selected date
published between	Search results include items in a selected range of dates
published within the last	Search results

Option	Result
	include items within the selected number of days.

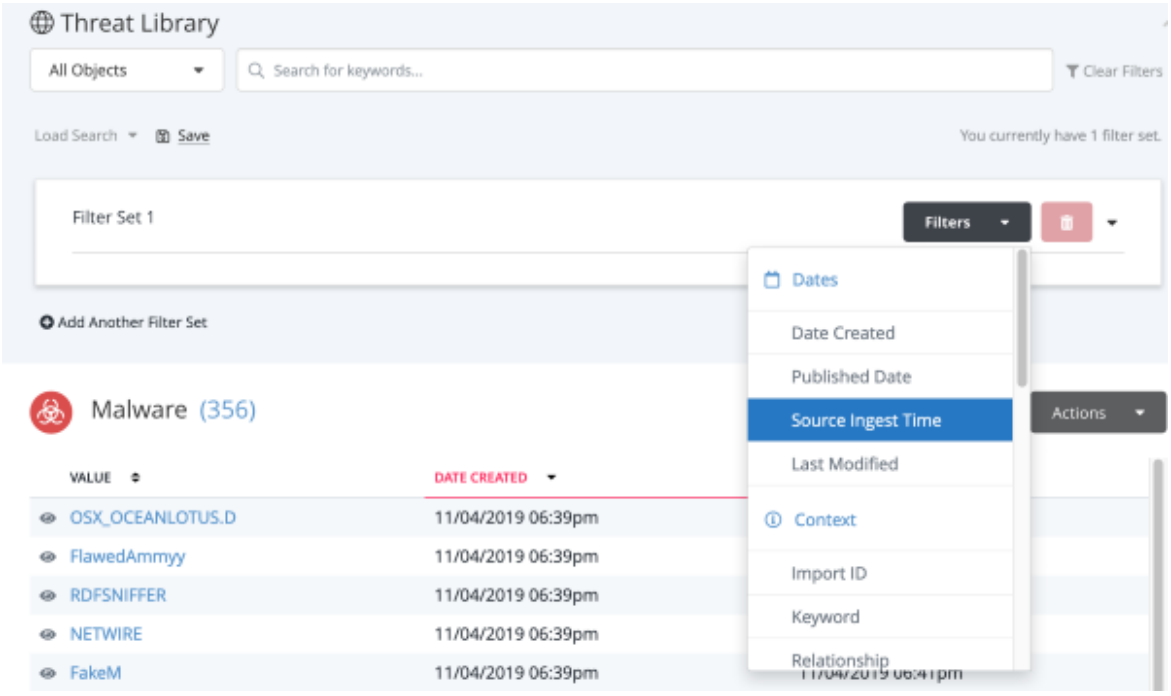
4. Select **Date**, **Time**, and **Time Zone** for the filter to use.
5. Click **Save**.

Filtering by Source Ingest Time

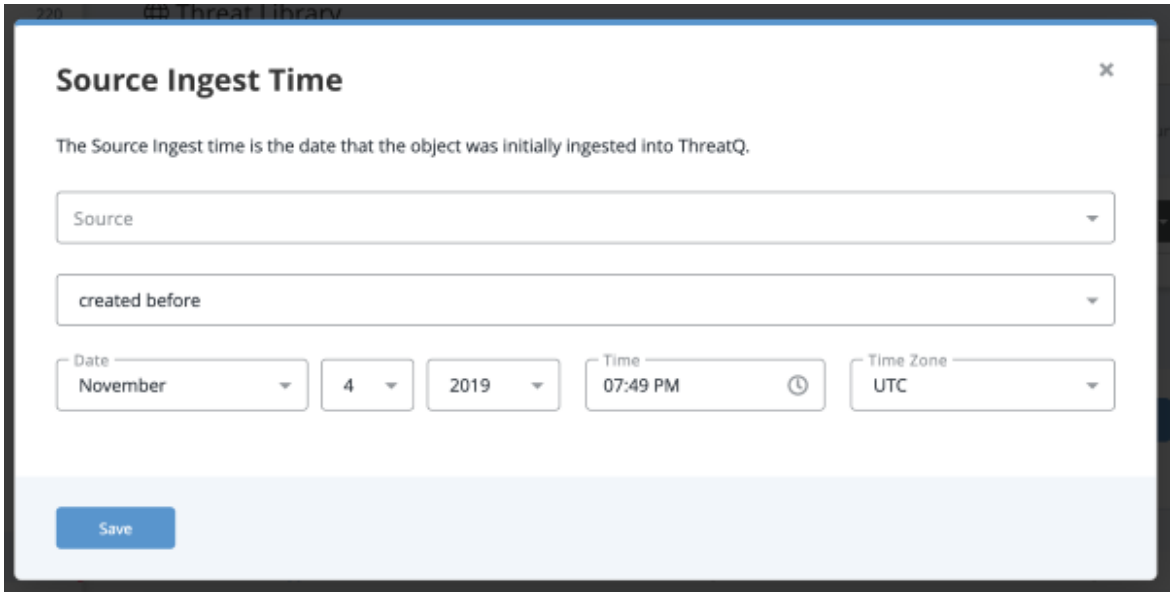
The Source Ingest Time is the date that an object was ingested into ThreatQ.

To filter by Source Ingest Time:

1. Click on the **Filters** dropdown option for a filter set and select **Source Ingest Time**.



The Source Ingest Time dialog box opens.



2. Select the **Source** that published the object.

   You have the option to select **Any Source**.

3. Select one of the following options to determine how the filter is applied:

Option	Result
created before	Search results include items before a selected date
created after	Search results include items after a selected date
created between	Search results include items in a selected range of

Option	Result
	dates
created within the last	Search results include items within the selected number of days.

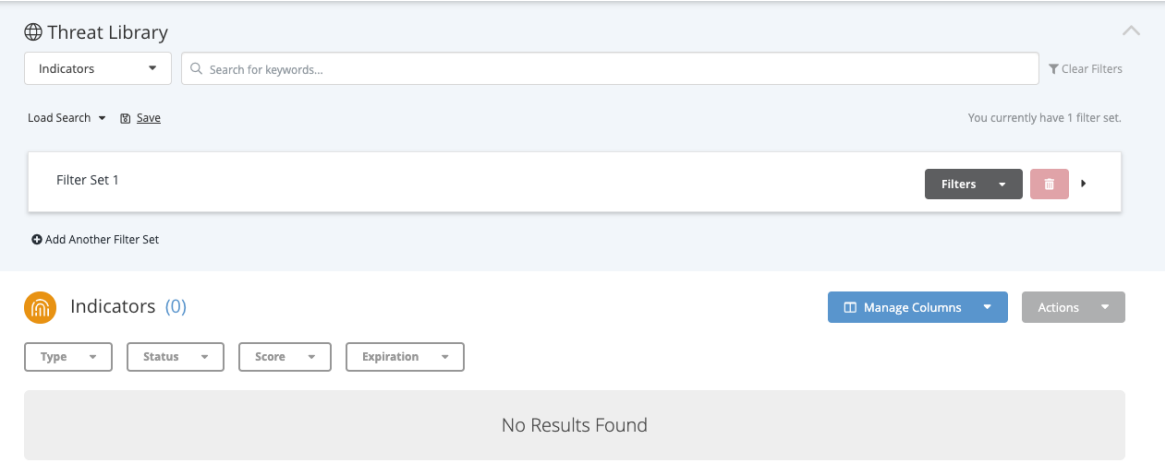
4. Select **Date**, **Time**, and **Time Zone** for the filter to use.
5. Click **Save**.

Filtering by Expiration Date

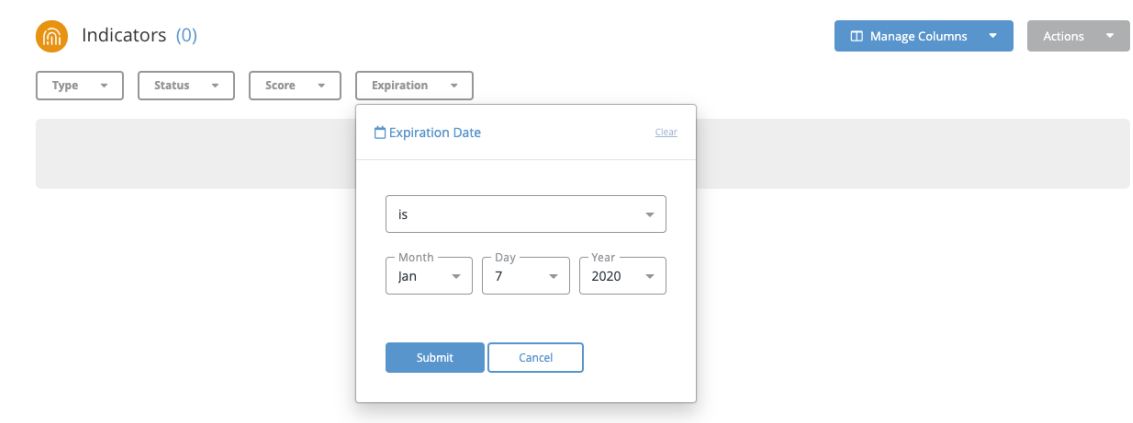
You can narrow down the Indicators in your search results by the expiration date.

To filter by Expiration Date:

1. Click on the **Filters** dropdown option for a filter set and select **Expiration Date**.



If you are currently viewing system indicators in the Threat Library, you can click on the **Expiration** button located above the search results.



The Expiration Date dialog box opens.

2. Select one of the following options to determine how the filter is applied:

Option	Result
is	Search results include the specified date.
is not	Search results exclude items from a range of dates.
is after	Search results include items after a selected date.
is before	Search results include items before a selected date.
is between	Search results include items in a selected range of dates.
is within the last	Search results include items within the selected number of days.
is within the next	Search results include items within a range of future dates.
is protected from auto-expiration	Search results include items that are protected from auto-expiration.

3. Select **Day**, **Month**, and **Year** for the filter to use.

4. Click **Submit**.

Context Filters

Context filters allow you to filter advanced search results by specific details associated with an object.

Additional Topics:

- Filtering by Attribute
- Filtering by Value Contains
- Filtering by List of Indicators
- Filtering by Keyword
- Filtering by Relationship
- Filtering by Related Object Types
- Filtering by Score
- Filtering using Tags

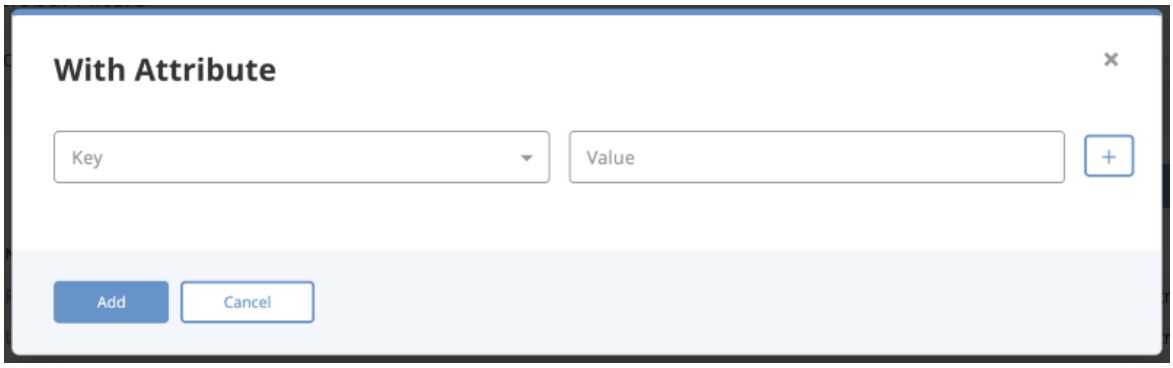
Filtering by Attribute

You can filter the Threat Library list to include or exclude objects with a specific attribute.

From the search results:

1. Click on the **Filters** option and select either **With Attribute** or **Without Attribute**.

   The Attribute Filter dialog box opens.



2. Select an **Attribute Type**.
3. Enter an **Attribute Value** associated with the **Attribute Type**.

   Users can leave the **Attribute Value** field blank to filter for *any value* associated with the selected **Attribute Type**.

4. Click on the **Plus** icon to the right of the dialog box to add another attribute and repeat steps 2-3. This step is optional.
5. Click on the **Add** button.

The filters will be applied to the search results.

The following section applies to using multiple attribute filters.

The **Match Any/All** toggle option will allow users to configure the filter to include objects that either fit one attribute filter or all. The **Any** option will be selected by default. This means the filter will display results that fit any of the attribute filters. The **All** option means the filter will display results that fit all attribute filters.

Example:

ANY - Match Toggle Selection		
Setting	**Field**	**Value**
Filter A	Attribute Type	Attack Phase
	Attribute Value	C2
Filter B	Attribute Type	Severity
	Attribute Value	High
Filter Options	Any/All Toggle	Any
Result	Search Results are filtered to include/exclude objects with Attack Phase: C2 **OR** Severity: High attributes.	

ALL - Match Toggle Selection		
Setting	**Field**	**Value**
Filter A	Attribute Type	Attack Phase
	Attribute Value	C2
Filter B	Attribute Type	Severity
	Attribute Value	High
Filter Options	Any/All Toggle	All
Result	Search Results are filtered to include/exclude objects with Attack Phase: C2 **AND** Severity: High attributes.	

Common Scenarios

The following scenarios demonstrate the Attribute Filter option in use with search results.

Applying a "With Attribute" filter (All items with an Attribute Type and Value)

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Filters** button and select **With Attribute**.

The Attribute Filter dialog box opens.

3. User selects **Attack Pattern** as the **Attribute Type** and **C2** as the **Attribute Value**.
4. User clicks on **Add**.

*The User will now see a search parameter **With Attribute** with **Attack Pattern: C2** listed. The search results update to show all Indicators with an attribute of **Attack Pattern: C2**.*

Applying a "Without Attribute" filter (All items without an Attribute Type and Value)

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Filter** button and select **Without Attribute**.

The Attribute Filter dialog box opens.

3. User selects **Attack Pattern** as the **Attribute Type** and **C2** as the **Attribute Value**.
4. User clicks on **Add**.

*The User will now see a search parameter **With Attribute** with **Attack Pattern: C2 listed**. The search results update to show all Indicators without an attribute of **Attack Pattern: C2**.*

Applying a "Without Attribute" filter (All items Without a specific Attribute Type with any Value)

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Filters** button and select **Without Attribute**.

The Attribute Filter dialog box opens.

3. User selects **Attack Pattern** as the **Attribute Type** and leave the **Attribute Value** blank.
4. User clicks on **Add**.

*The User will now see a search parameter **Without Attribute** with **Attack Pattern** listed. The search results update to show all Indicators that do not have an **Attribute Type** of **Attack Pattern** assigned to them.*

Applying keyword filters then applying a "With Attribute" filter

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User searches for keyword: **demo**.

The User will see a search parameter listed Keyword: "demo" and the results update to show only indicators that mention demo.

3. User clicks on the **Filters** button and select **With Attribute**.

The Attribute Filter dialog box opens.

4. User selects **Attack Pattern** as the **Attribute Type** and **C2** as the **Attribute Value**.
5. User clicks on **Add**.

The User will now see a search parameter **With Attribute** with **Attack Pattern: C2** listed. The search results will update to show all Indicators that mention the keyword **demo AND** have an attribute of **Attack Pattern: C2**.

Editing multiple attributes that were applied as part of the search parameters

1. User clicks on the **Threat Library** tab and navigates to the **Indicators** tab.
2. User clicks on the **Filter** button and select **With Attribute**.

   The Attribute Filter dialog box opens.

3. The User specifies two attributes:
   - Attack Pattern:C2
   - Severity: High
4. User clicks on **Add**.

   *The User will now see two search parameters under the **With Attribute** section - **Attack Pattern: C2** and **Severity: High**. The search results updates to show all Indicators with an attribute of **Attack Pattern: C2** and **Severity: High**. The search parameter for attributes is defaulted to Any. This indicates that objects with an attribute of **Attack Pattern: C2** or **Severity: High** are displayed.*

5. User clicks on the **Filters** option and selects **With Attribute**.

   A form will load with all applied filter attributes.

6. The User clears the **Attack Pattern's Attribute Value** field and clicks **Add**.

   The User will now see two search parameters under the **With Attribute** section: **Attack Pattern: Any** and **Severity: High**. The search results updates to show all Indicators with an attribute type of **Attack Pattern OR Severity: High**.

Add multiple attributes and toggle Match from Any to All

1. User applies two attribute filters to the indicators results: **Attack Phase: C2** and

Severity:High.

The filtered results will display any indicators that has either of those attributes.

2. User clicks on the **Any/All** Match toggle button and select **All**.

The filtered results will display any indicator that has both of those attributes

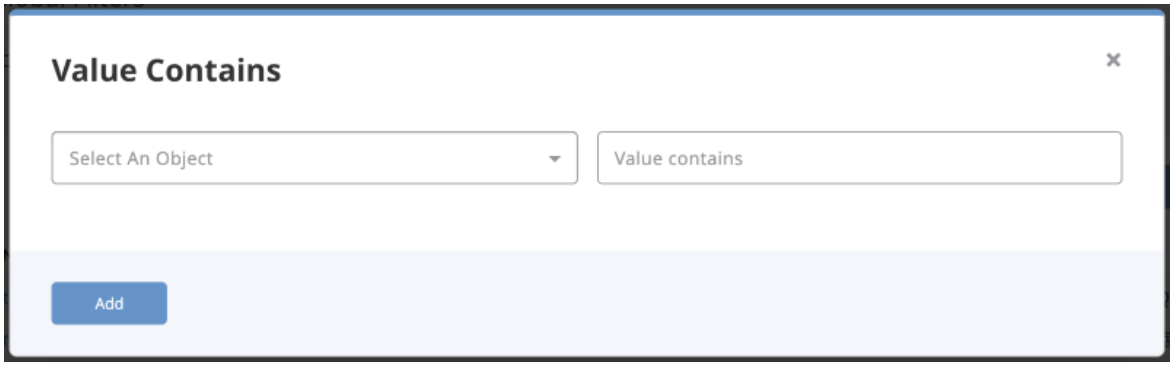
Filtering by Value Contains

You can now filter Threat Library objects by a specific value or string within the value using the Value Contains filter.

To filter by contains:

1. Click on the **Filters** option and select **Value Contains**.

   The Contains dialog box opens.



2. Select an **Object**, enter a **Value**, and click **Add** to apply the filter.

Filtering by Keyword

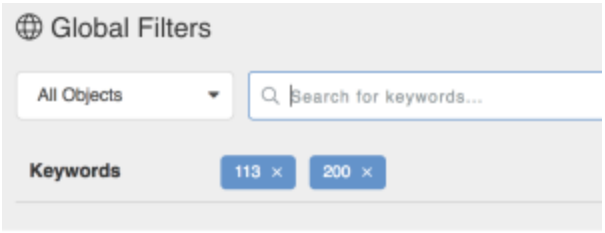
You can filter the Threat Library items on the Advanced Search by keyword.

To filter by keyword:

1. Navigate to the Advanced Search page.
2. Enter a keyword in the Keyword text field and press **<Enter>** or **<Return>**.

   Repeat Step 2 to apply multiple keyword filters

   Each keyword filter appears in a box below the keyword text field. "



3. Click on the **X** for each filter to remove it or select **Clear All Filters** to remove all filters

The following list of fields are all searched against for any matches of keywords:

- Source Names
- Attribute Names
- Attribute Values
- Comments
- Tags
- Adversary Name
- Adversary Description
- File/Attachment Name
- File/Attachment Title
- File/Attachment Type Name
- File/Attachment Content-Type Name
- File/Attachment Hash

- File/Attachment Description
- File/Attachment Contents
- Event Title
- Event Type Name
- Event Description
- Spearphish Subject (for Events of Type 'Spearphish')
- Spearphish Value (for Events of Type 'Spearphish')
- Indicator Type Name
- Indicator Status Name
- Indicator Value
- Indicator Class
- Indicator Description
- Signature Name
- Signature Description
- Signature Value
- Signature Has
- Signature Type Name
- Signature Status Name
- Task Name
- Task Description
- Task Status Name
- Task Assignee Source Name
- Task Creator Source Name

Filtering by List of Indicators

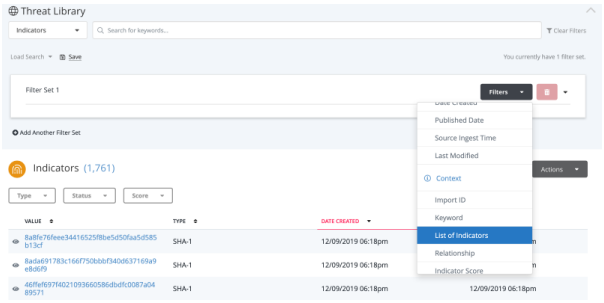
The List of Indicators Filter option allows you to filter the Threat Library by pasting a list of indicators, in raw text.

> The filter will return indicators that are an exact match. It does not return partial matches.

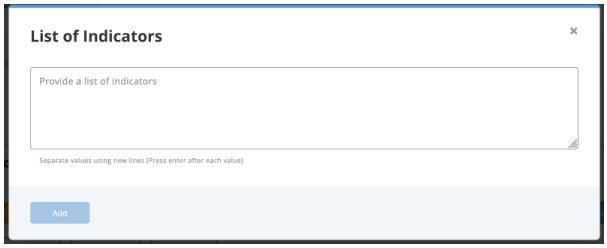
To Filter by a List of Indicators:

From the search results:

1. Click on the **Filters** option and select **List of Indicators**.



The List of Indicators dialog box opens.



2. Enter or paste your list of indicators into the textbox provided.

The accepted list format is one indicator per line.

3. Click on **Add** to apply the filter.

Filtering by Related Object Types

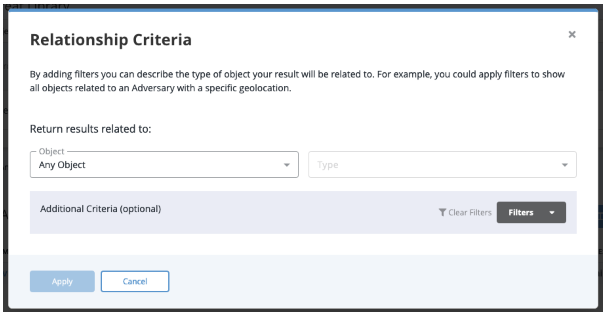
The **Related Object** filter allows you to filter search results by related object type. Using this filter, you can do the following:

- Filter search results that return related items linked to certain objects.
- Filter search results that return related items linked to certain object types.
- Apply a Value Contains filter to the results.

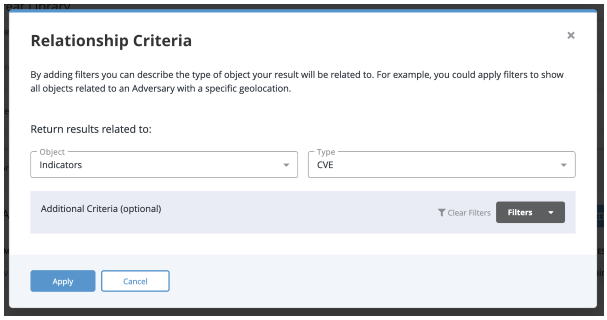
To Filter by Related Object Types:

1. Click on the **Filters** option and select **Relationship Criteria**.

   The **Relationship Criteria** dialog box opens.

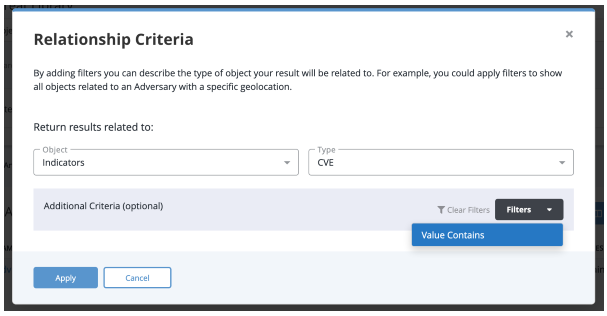


2. Use the text box to select your **Object** and **Type**.

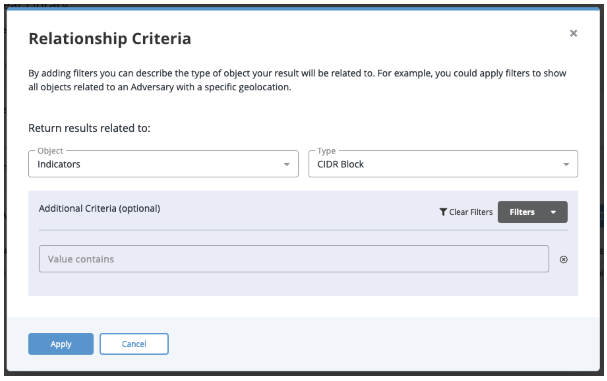


Steps 3-4 are optional.

3. Click on the **Filters** dropdown and select **Value Contains**.



4. Enter your desired value in the field provided.



5. Click on **Apply** to filter.

Filtering by Relationship

The Relationship Filter option allows you to filter the Threat Library by related objects. Using the Relationship filter, you can:

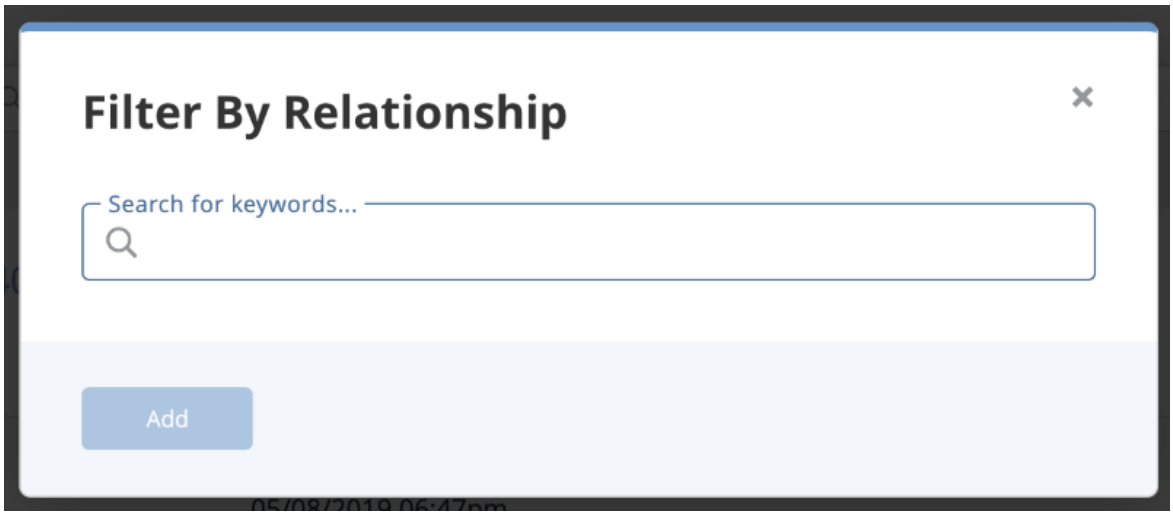
- Filter search results to include objects related to a specific object.
- Filter search results to include objects using multiple related object filters. You will also have the option to set the filter to include objects that fit one of the multiple filters or all.

To Filter by Related Object:

From the search results:

1. Click on the **Filters** option and select **Relationship**.

   The Filter by Relationship dialog box opens.



2. Use the textbox provided to select an object.

   Repeat step 2 to add multiple object filters.

3. Click on **Add** to apply the filter.

   The **Match Any/All** toggle option will allows you to configure the filter to include objects that either fit one related object filter or all. The **Any** option will be selected by default. This means the filter will display results that fit any of the related object filters. The **All** option means the filter will display results that fit all related object filters.

Examples:

ANY - Match Toggle Selection	
Setting	**Related Object**
Filter A	ABC Indicator

Filter B	DEF Event
Filter Option	Any
Result	Search Results are filtered to include objects related to the ABC Indicator **OR** the DEF Event.

ALL - Match Toggle Selection	
Setting	**Related Object**
Filter A	ABC Indicator
Filter B	DEF Event
Filter Option	All
Result	Search Results are filtered to include objects related to the ABC Indicator **AND** the DEF Event.

Filtering by Score

You can filter indicators in the advanced search results by score.

This option is only available for indicators.

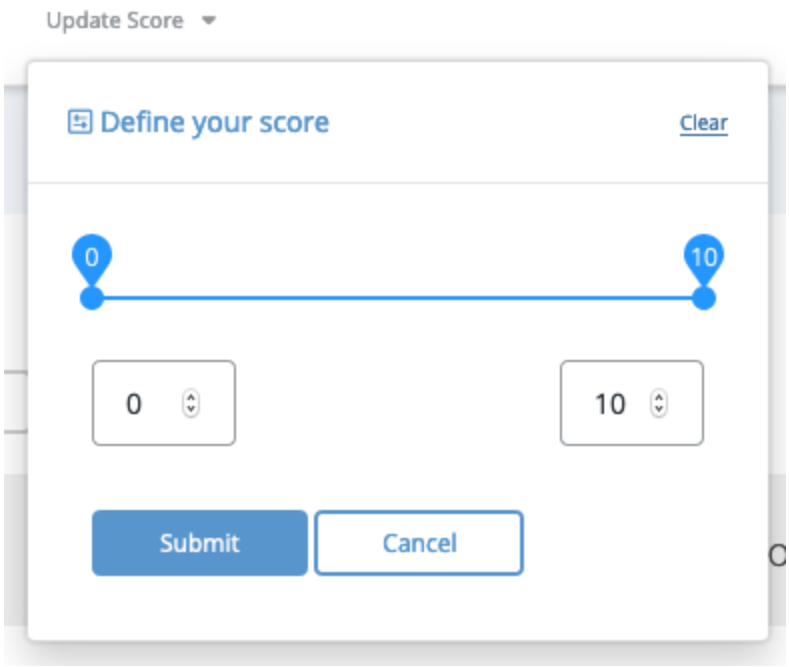
To filter by score:

1. Navigate to the Advanced Search results page by selecting **Search > Advanced Search** then selecting **Indicators** from the left-hand object type menu.

   You can also select **Threat Library > Indicators** from the main menu.

2. Click on the **Filters** dropdown and select the **Indicator Score** filter option.
   The Indicator Score dialog row will load in the filter set.



> The scale offers a range of 1-10.

3. Adjust the score scale to filter the results.

   Filtering by Scoring Range

   You can move the two scale markers to select a scoring range.

   Example: Move the left marker to 6 and the right marker to 8 to filter the search results to include indicators with a score between 6 and 8.

   Filtering by Specific Score

   You can move the scale makers to the same scoring number to filter by a specific score.

Example: Move the left and right markers to 8 to filter the search results to only include indicators with a score of 8.

Select the **Update Score** filter again and select **Clear** to remove the filter.

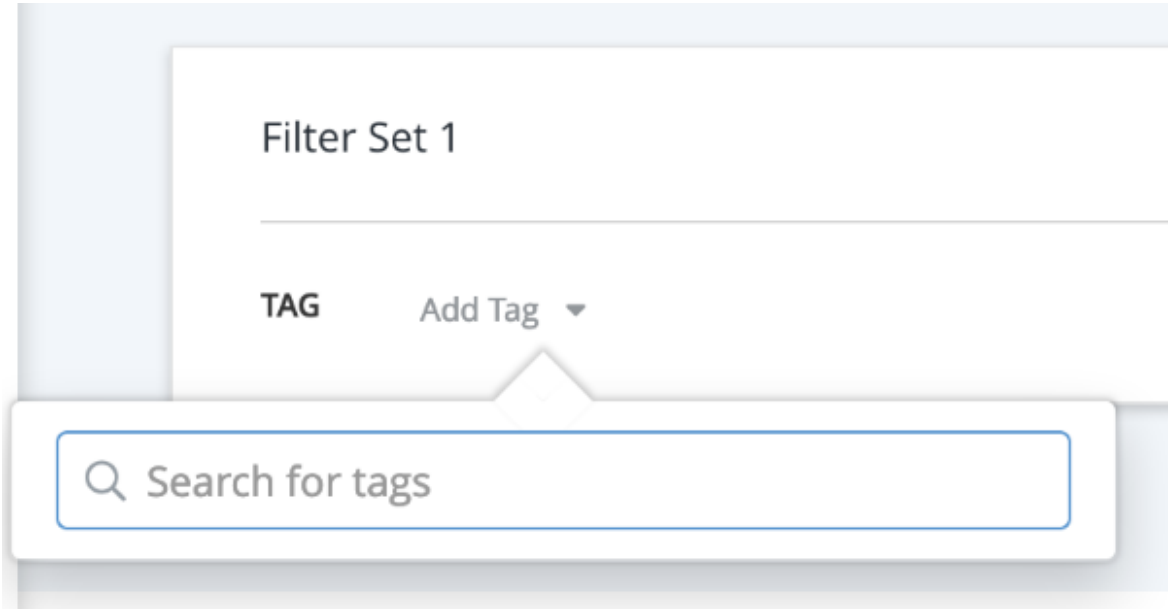
Filtering using Tags

Using the **Tags** filter allows you to filter search results based on tags applied to an object.

From the search results:

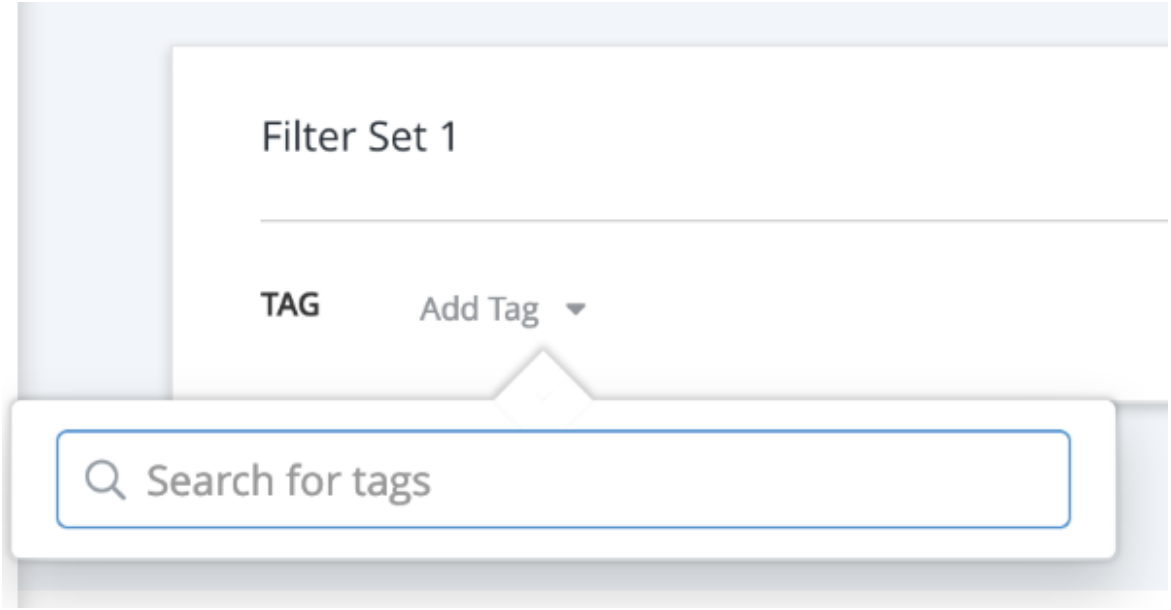
1. Click on the **Filters** option and select **Tags**.

   The Filter by Tag row opens.



2. Select **Add Tag**.

   The Add Tag dialog box opens.



3. Use the supplied text field to select a tag.
4. Repeats steps 2-3 to apply multiple tag filters.

The **Match Any/All** toggle option will allows you to configure the filter to include objects that either fit one tag filter or all. The **Any** option will be selected by default. This means the filter will display results that fit any of the tag filters. The **All** option means the filter will display results that fit all-tag filters.

Examples:

ANY - Match Toggle Selection	
Setting	**Tag**
Filter A	Phishing
Filter B	DDoS
Filter Option	Any
Result	Search Results are filtered to

	include items with either Phishing **OR** the DDoS tags.

ALL - Match Toggle Selection	
Setting	**Tags**
Filter A	Phishing
Filter B	DDoS
Filter Option	All
Result	Search Results are filtered to include items with both Phishing **AND** DDoS tags.

Tasks Filters

Tasks filters allow you to filter tasks based on their priority and to whom they are assigned.

Related Topics:

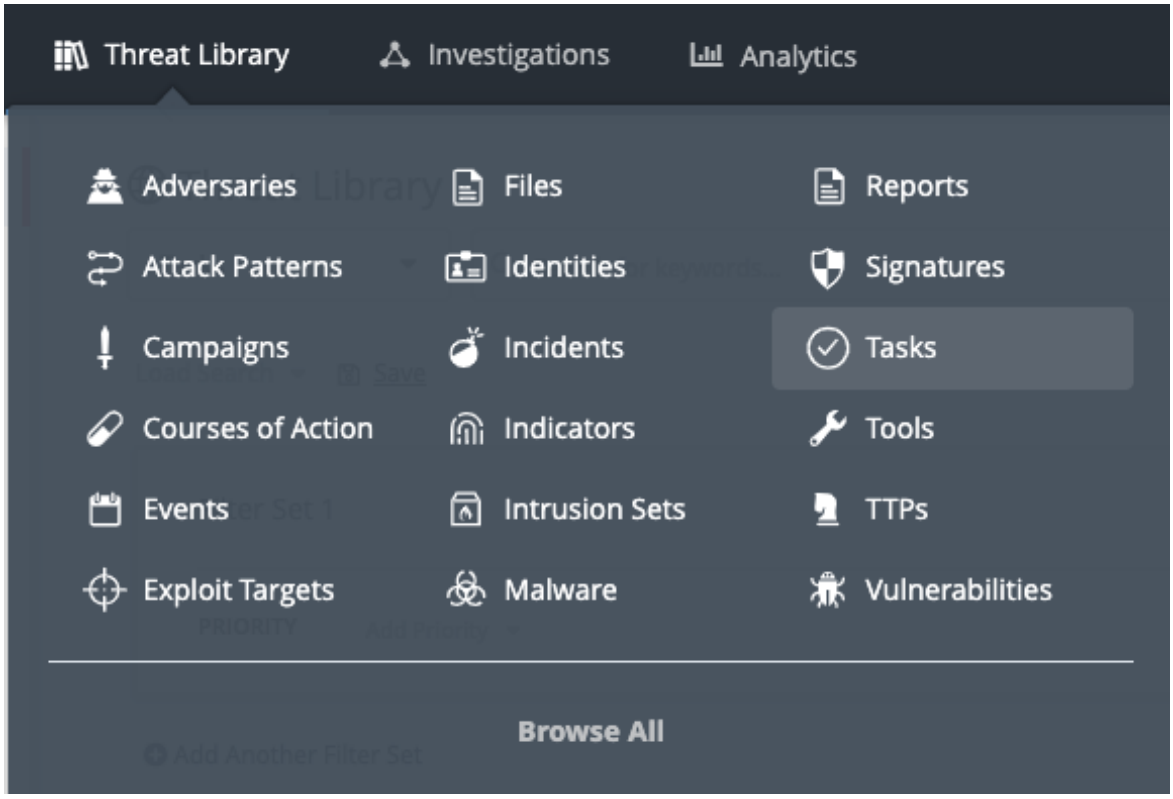
- Filtering Tasks by Assignment
- Filtering Tasks by Due Date
- Filtering Tasks by Priority
- Filtering Tasks by Reported By

Filtering Tasks by Assignment

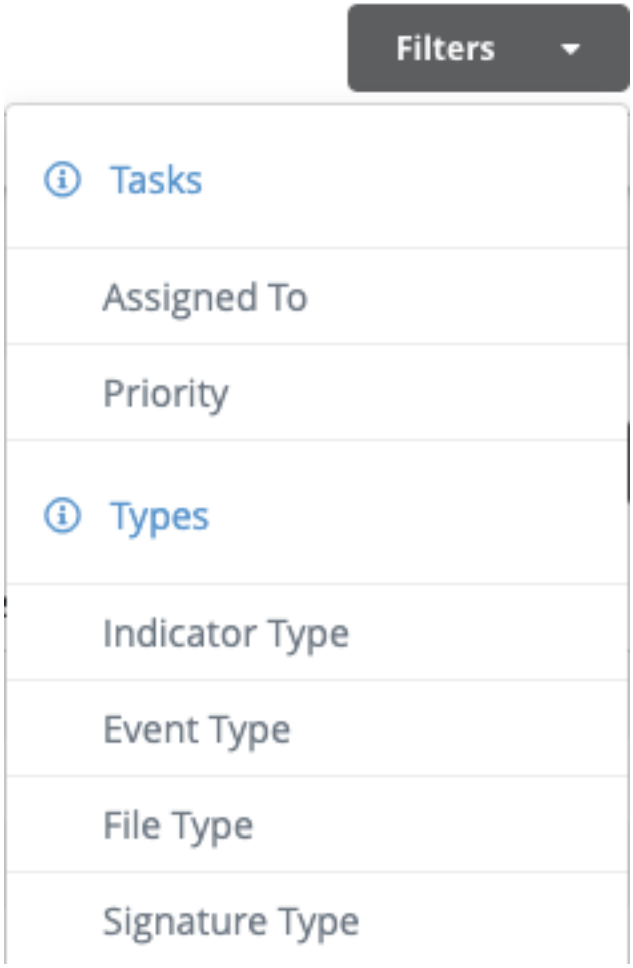
You can filter tasks based on whom they are assigned to.

From the Advanced Search page:

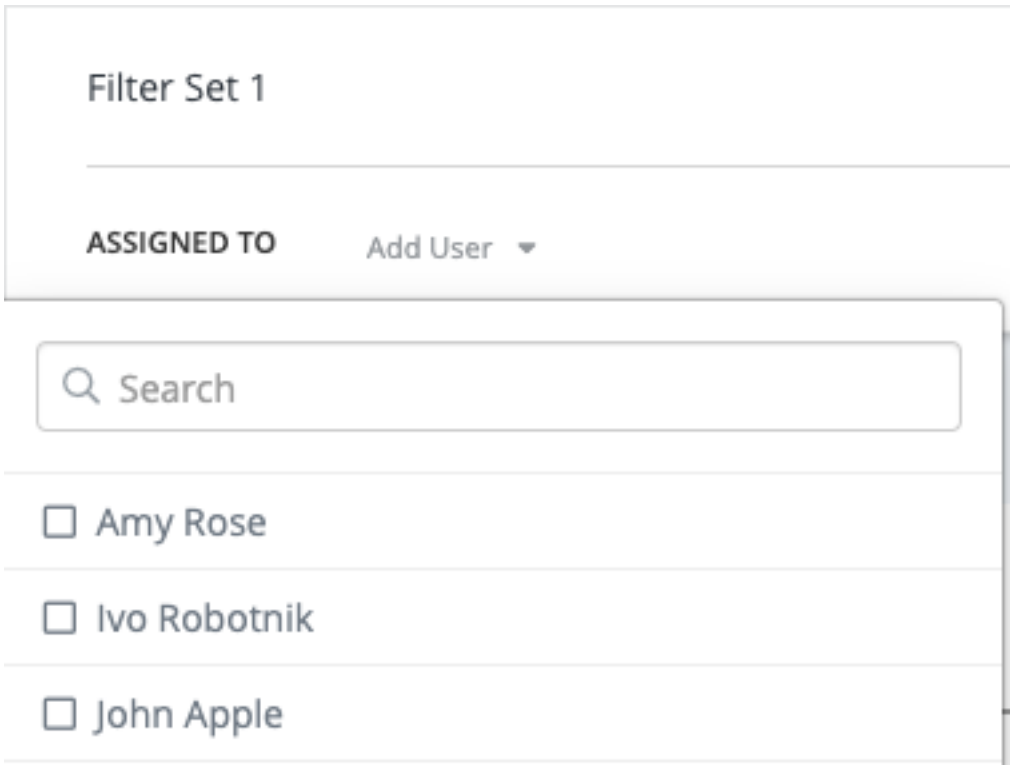
1. Click on the **Tasks** option in the **Threat Library** menu.



2. Click on the **Filters** option and select **Assigned To**.



3. Use the **Add User** dropdown to select the user.

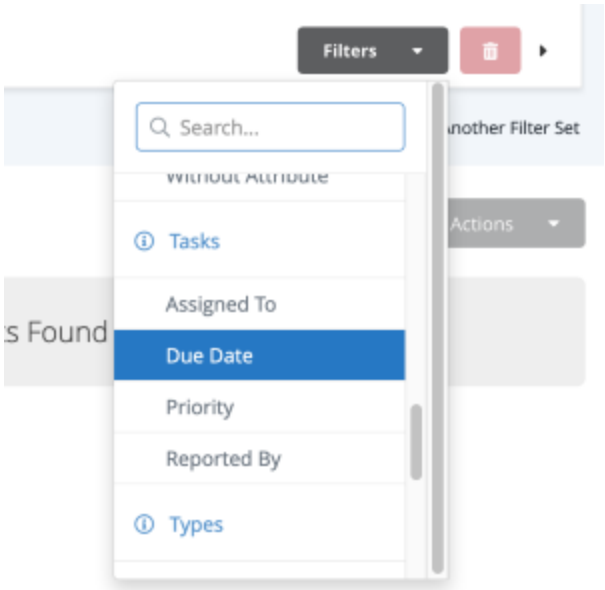


Filtering Tasks by Due Date

You can filter tasks based on its due date.

From the Advanced Search page:

1. Click on the **Filters** option and select **Due Date**.



The Due Date dialog box opens.

2. Select one of the following options to determine how the filter is applied:

Option	Result
is after	Search results include tasks with a due date after a selected date.
is before	Search results include tasks with a due date before a selected date.
is	Search results include tasks with a due date that set between the

Option	Result
between	selected range of dates.
Is within the last	Search results include tasks with a due date within the last user-specified number of days.
Is within the next	Search results include tasks with a due date within the next user-specified number of days.

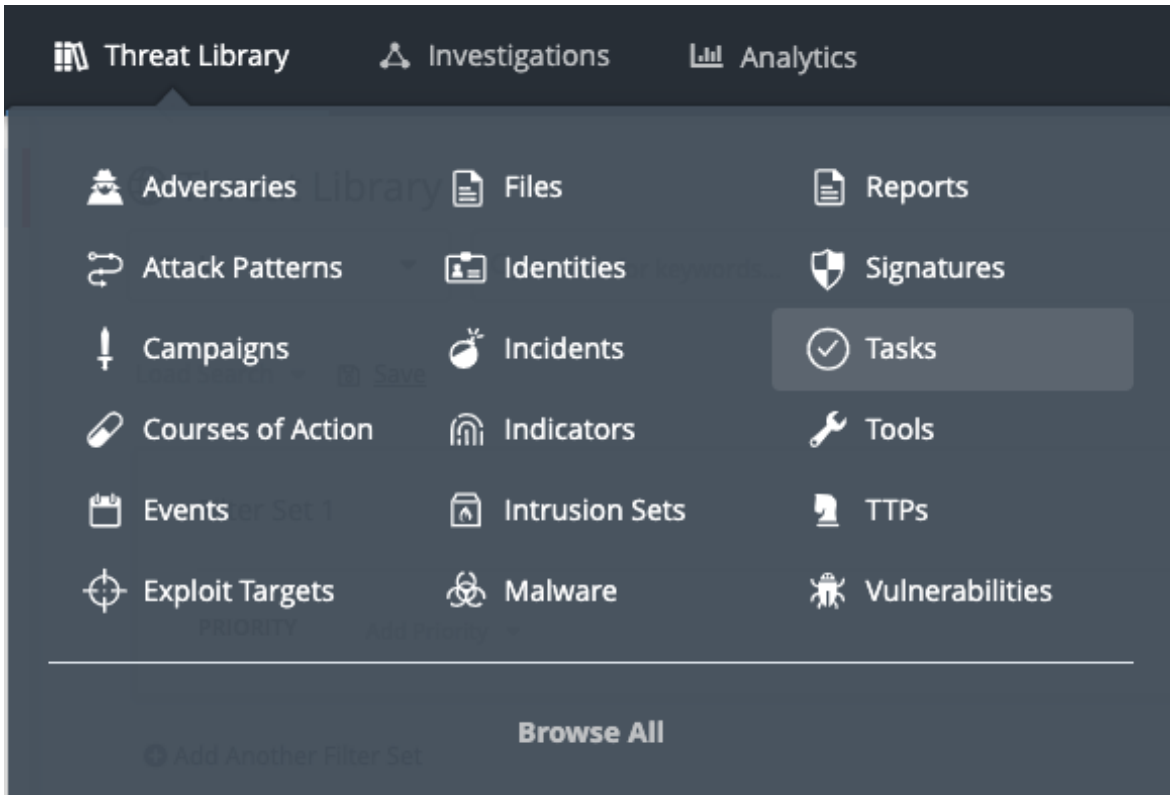
3. Click **Save**.

Filtering Tasks by Priority

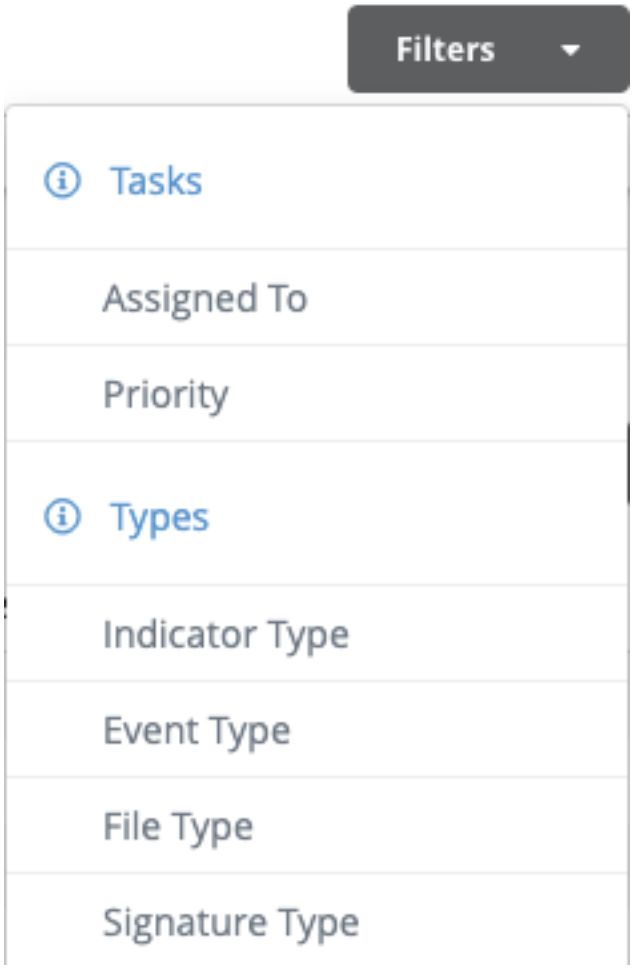
You can filter tasks based on their priority.

From the Advanced Search page:

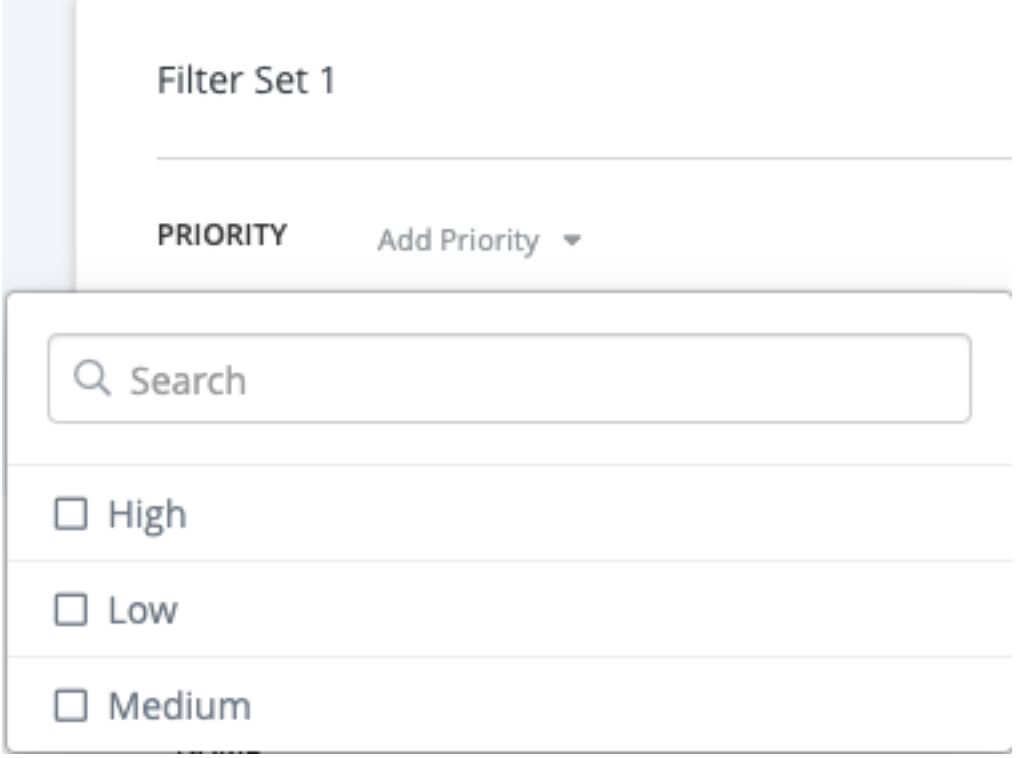
1. Click on the **Tasks** option in the **Threat Library** menu.



2. Click on the **Filters** option and select **Priority**.



3. Use the **Priority** dropdown and select **Add Priority.**

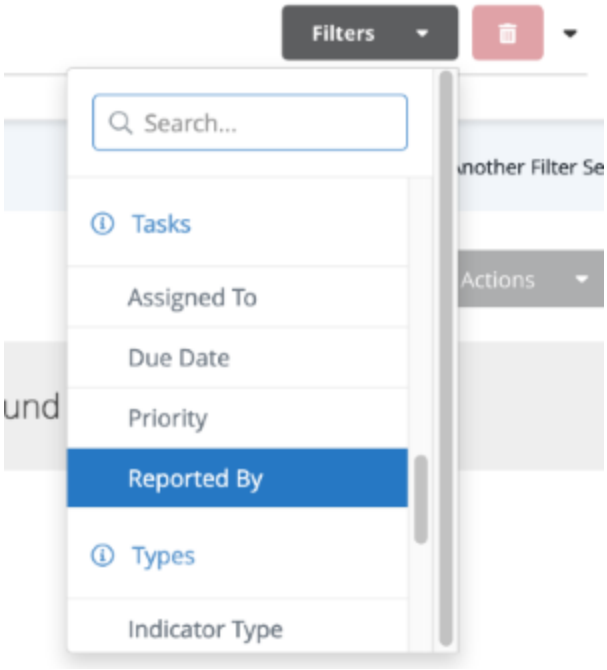


Filtering Tasks by Reported By

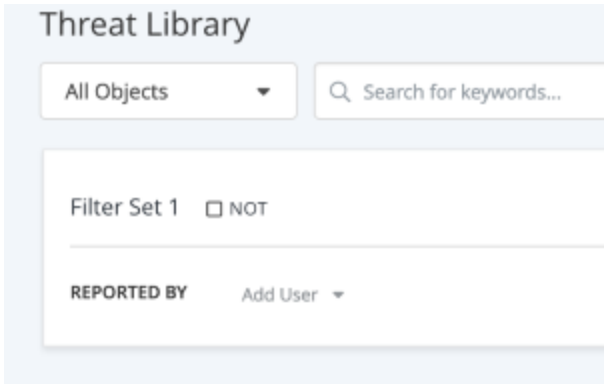
You can filter tasks based on who created it.

From the Advanced Search page:

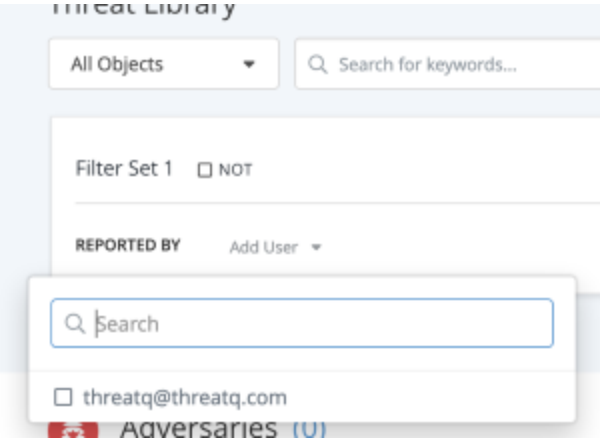
1. Click on the **Filters** option and select **Reported By**.



The Reported By Filter will appear in the filter set.



2. Click on the **Add User** option to select the user.



Types Filters

Types filters allow you to filter advanced search results by object or subtype.

Additional Topics:

- Filtering by Object Type

Filtering by Object Type

You can filter Indicators, Events, Signatures, and Files by specific types of each.

Example: Filter the Signature list to include YARA types only.

To filter by status:

1. Click on the Filters dropdown and select **<Object Type>Type**.

   The Type filter row will appear in the filter set.

2. Click on **Add Type**.

   You can select multiple types using the check boxes.

   The search results will update with the applied filter.

Status Filters

Status filters allow you to filter advanced search results an object's Status.

Only Indicators, Signatures, and Tasks can be filtered by their Status.

Additional Topics:

- Filtering by Status

Filtering by Status

You can filter Indicators, Signatures, and Tasks by Status.

To filter by status:

1. Click on the Filters dropdown and select **<Object Type>Status**.

   The Status filter row will appear in the filter set.

2. Click on **Add Status**.

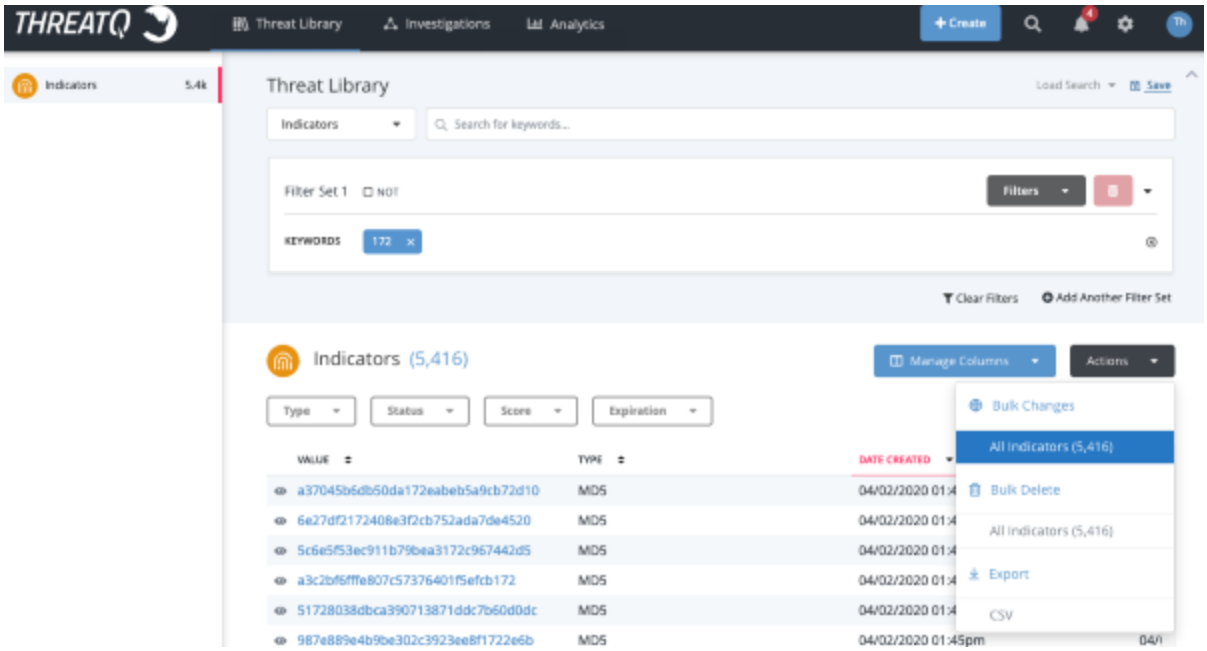
   You can select multiple statuses using the check boxes.

   The search results will update with the applied filter.

Bulk Actions

The Bulk Actions feature gives you the ability to update and delete large groups (1000+) of system objects from the Advanced Search page. Once selected, the job process will run in the background and allow you to continue working within ThreatQ. You can review the status of the job and its results on the Job Management page.

You will also receive in-app notifications, via the Notification Center, when a Bulk Action job has been queued and when it has been completed.



Related Topics:

- Bulk Delete
- Bulk Change Expiration Date
- Bulk Add Source
- Bulk Status Change
- Bulk Add/Remove Attributes
- Bulk Add/Remove Tags
- Bulk Add/Remove Relationships
- Job Management

Bulk Delete

You can use the Bulk Delete option to delete a group of indicators on the Advanced Search page. This feature is only available if you have a maintenance or administrator role.

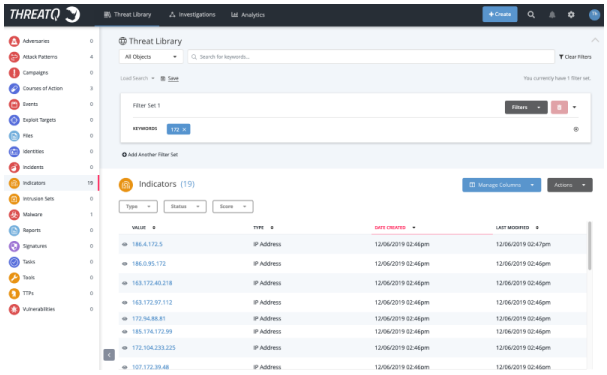
Deleting an indicator also deletes its child records such as attributes and relationships. The number of child records will influence the overall time it takes to complete the job.

The Bulk Delete function **permanently** deletes selected indicators from the system. Once deleted, you will be unable to undo the action. If you are executing a Bulk Delete on a large group of indicators, ThreatQuotient highly recommends performing a backup of your system before performing this function.

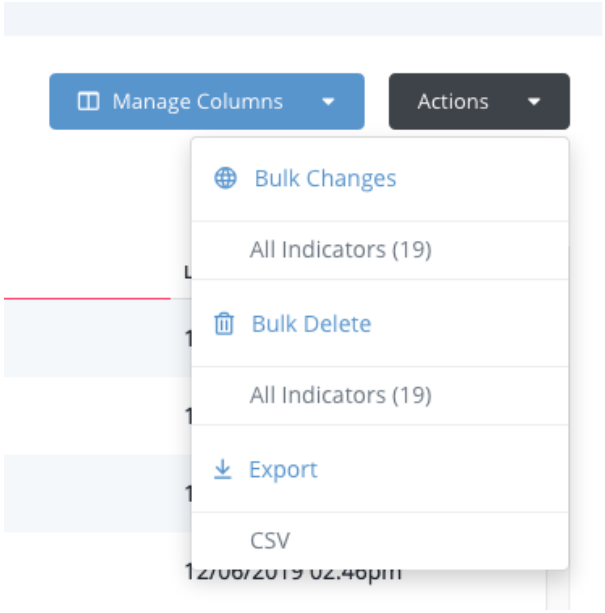
To Perform a Bulk Delete

From the Advanced Search Page:

1. Perform an advanced search and create a filter set to narrow down your results - this step is optional.

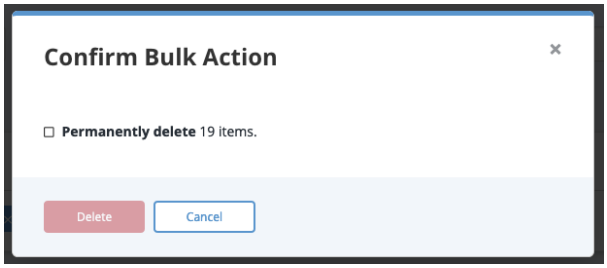


2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Delete* heading.



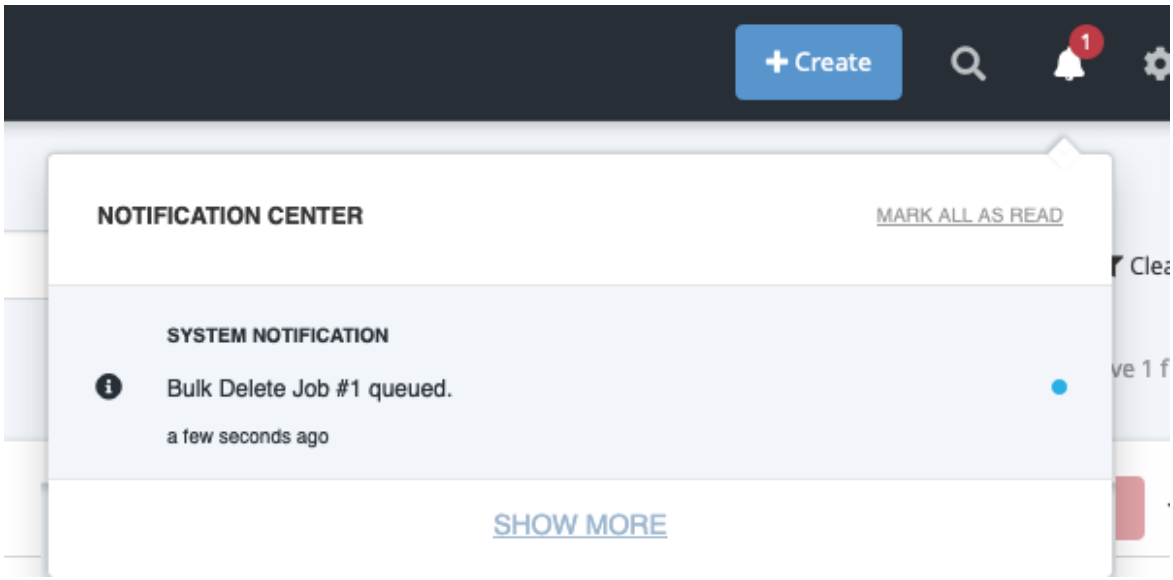
You will see the number of system objects affected next to the link in parentheses.

The Bulk Action Confirmation dialog box will load.

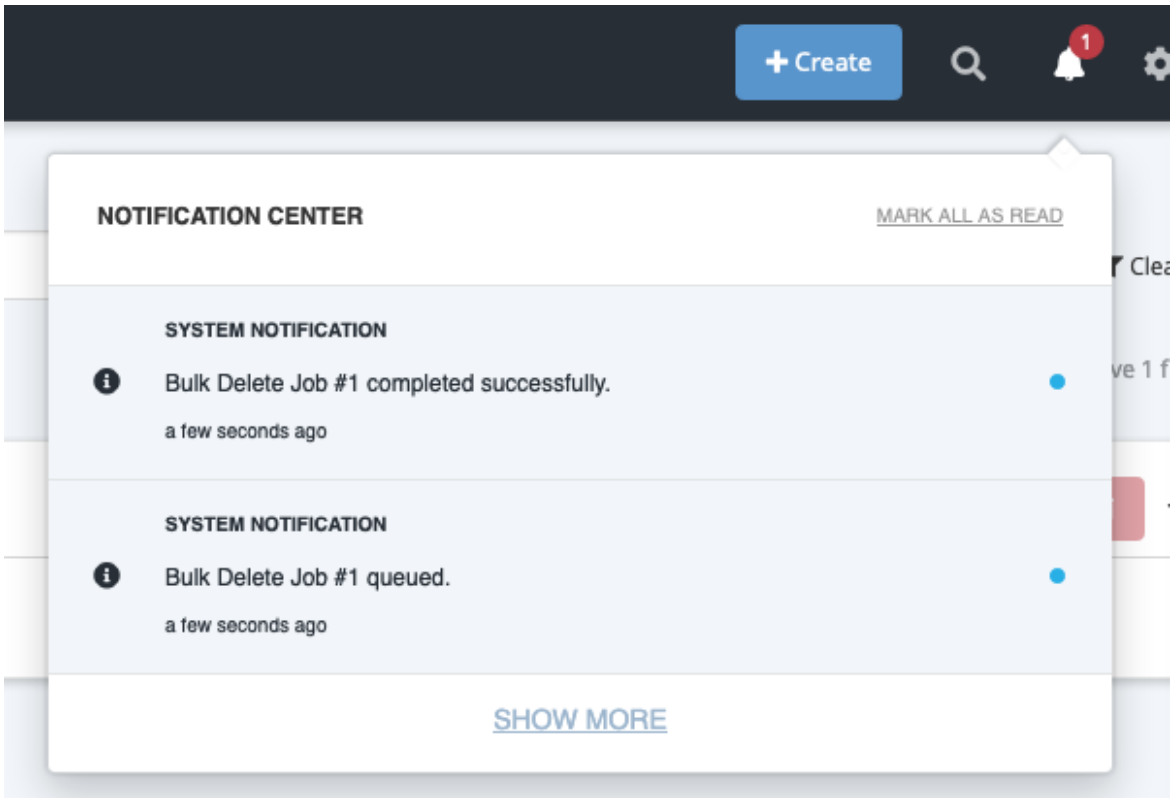


3. Click on the checkbox to confirm deletion and then click on **Delete**.

The job will be queued by the system and you will receive an in-app notification via the Notification Center icon.



The system will also notify you, via the Notification Center, that the job has been completed.



You can also view the status and other details of the job on the Job Management page.

Bulk Change Expiration Date

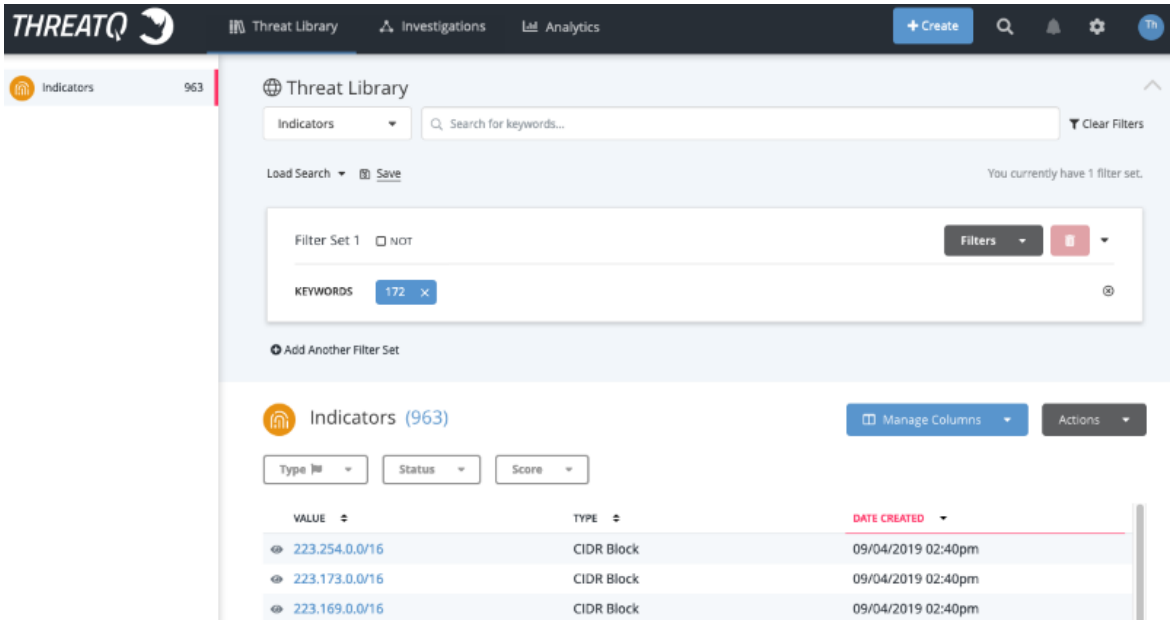
You can use the Bulk Change option to update the expiration for a group of objects on the Advanced Search page.

This function can only be performed on Indicators.

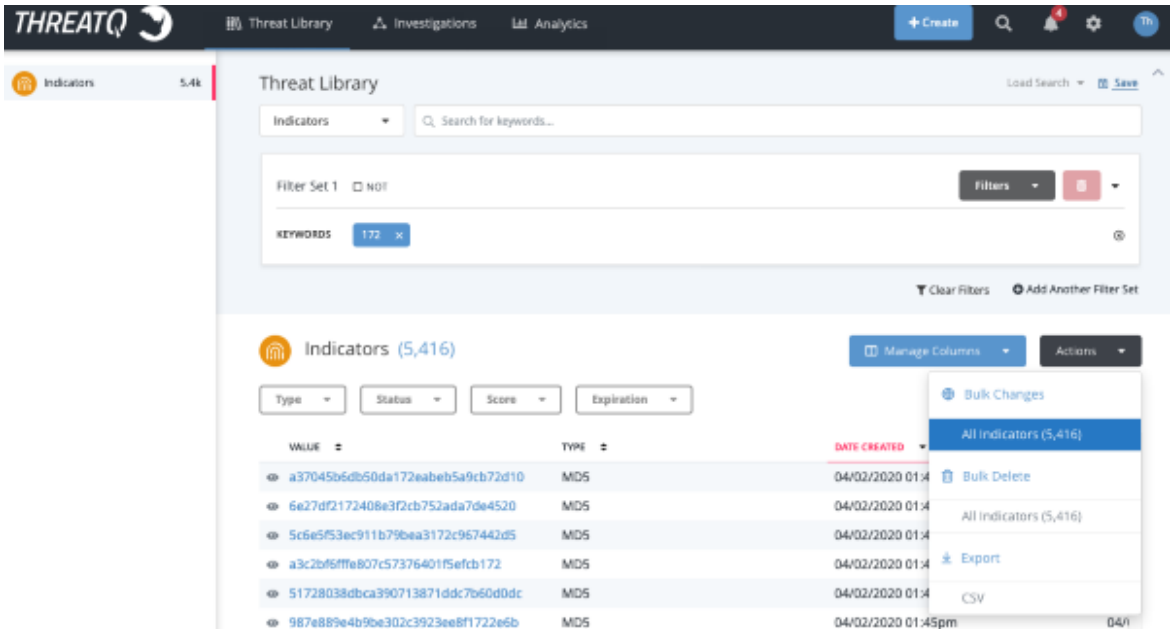
To Perform a Bulk Expiration Update

From the Advanced Search Page:

1. Perform an advanced search and create a filter set to narrow down your results - this step is optional.

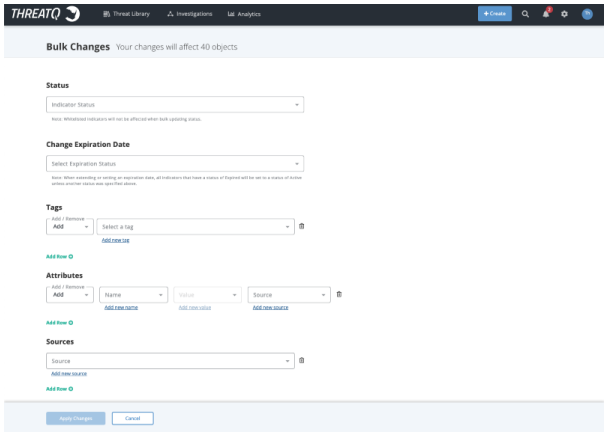


2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



You will see the number of system objects affected next to the link in parentheses.

The Bulk Changes form will load.



3. Select the type of expiration update to perform:

   See the Bulk Change Expiration Date Scenarios topic for specific details and outcomes.

   - Extend expiration date

     The platform will ask you for the number of days to extend the expiration upon selection.

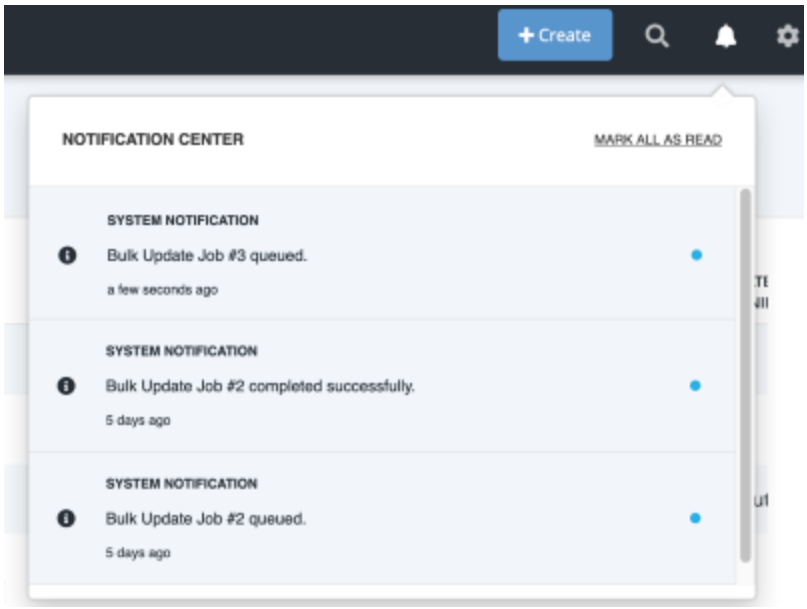
   - Protect from auto-expiration
   - Remove expiration date
   - Set a new expiration date

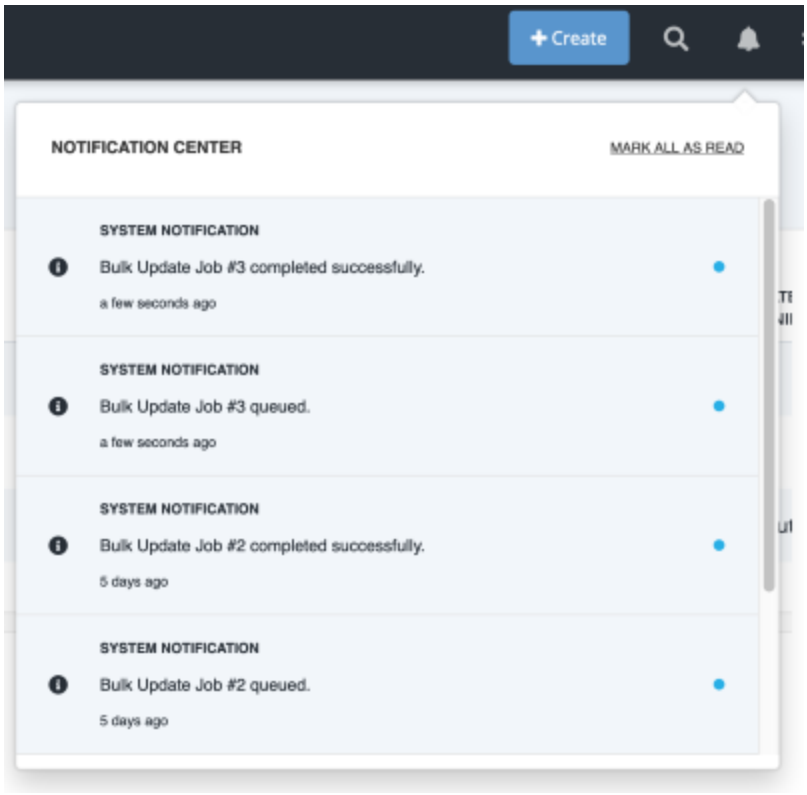
     The platform will ask you to select a new date using a date picker upon selection.

4. Click on **Apply Changes** located at the bottom of the form.

The job will be queued by the system and you will receive an in-app notification via the Notification Center icon.



The system will also notify you, via the Notification Center, that the job has been completed.



You can also view the status and other details of the job on the Job Management page.

Bulk Change Expiration Date Scenarios

The following scenarios describe the behavior of the Bulk Expiration Update feature.

Scenario #1 - Expiration isn't part of the form if indicators are not part of the result set

1. The user attempts to make bulk expiration changes to system objects other than indicators.
2. The Change Expiration Date option will not be listed on the Bulk Changes form.

Scenario #2 - Setting expiration policy to a specific day

1. The user selects a set of indicators using the advanced search.

2. The user selects **Set a New Expiration Date** from the Change Expiration option.
3. The users selects a day using the date picker.

   The date selected must be a future date.

4. After submitting the request, all indicators as part of that record set have the new expiration date.

Scenario #3 - Extending the expiration policy by a number of days

1. The user selects a set of indicators using the advanced search.
2. The user selects **Extend Expiration Date** from the Change Expiration option.
3. The user enters the number of days to extend.
4. After submitting the request, all indicators in that record set will now have their expiration date extended by that number of days specified.

Scenario #4 - Removing an expiration policy

1. The user selects a set of indicators using the advanced search.
2. The user selects **Remove Expiration Date** from the Change Expiration option.
3. After submitting the request, all indicators in that record set will no longer have an expiration date.

Scenario #5 - Protecting items from auto-expiration

1. The user selects a set of indicators using the advanced search.
2. The user selects **Protect from Auto-Expiration** from the Change Expiration option.
3. After submitting the request, all indicators in that record set will have the **protect from auto-expiration** expiration policy applied.

Scenario #6 - Extending / Setting an expiration date on an indicator with a status of Expired

1. The user selects a set of expired indicators using the advanced search.
2. The user selects **Set a New Expiration Date** from the Change Expiration option.
3. The users selects a day using the date picker.

   The date selected must be a future date.

4. After submitting the request, the expired indicators in that record set are then changed to a status of Active and the expiration date is set to the date indicated with the date picker.

Scenario #7 - Extending / Setting an expiration date on an indicator with a status of Whitelisted

All whitelisted indicators included in a Expiration Change set will be skipped.

Scenario #8 - Removing an expiration date on a previously expired indicator

1. The user selects a set of expired indicators using the advanced search.
2. The user selects **Remove Expiration Date** from the Change Expiration option.
3. The expired indicators in the set are skipped.

Bulk Add Source

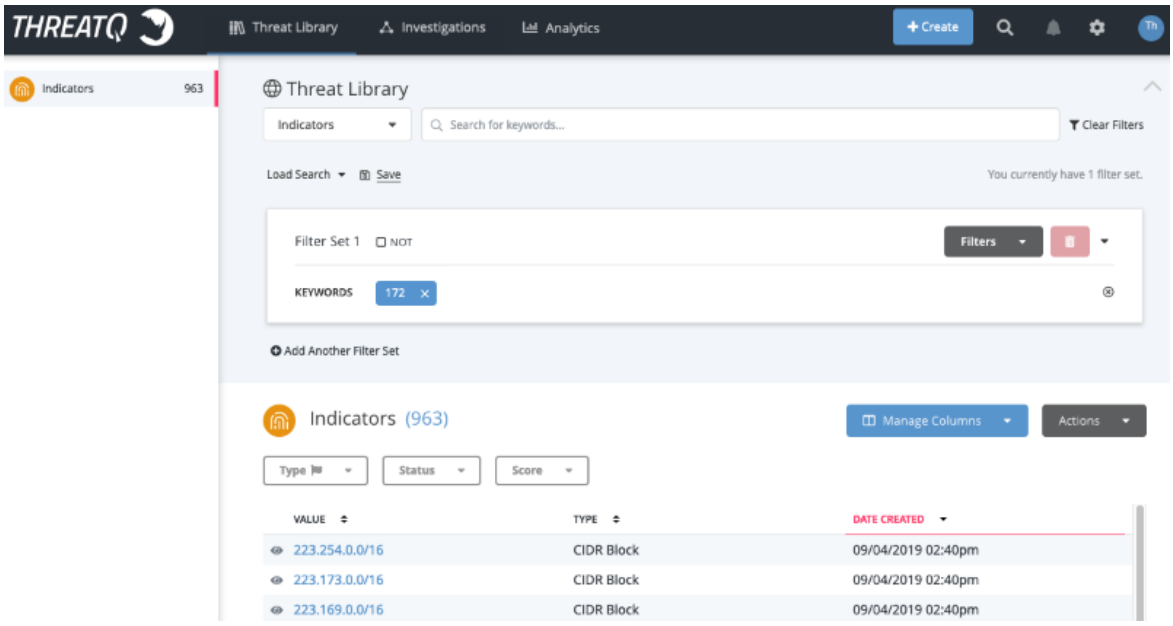
You can use this Bulk Action option to add a source to a set of selected objects on the Advanced Search page.

If an object is already associated with the source selected for the Bulk Add Sources action, the object will be skipped during the bulk process.

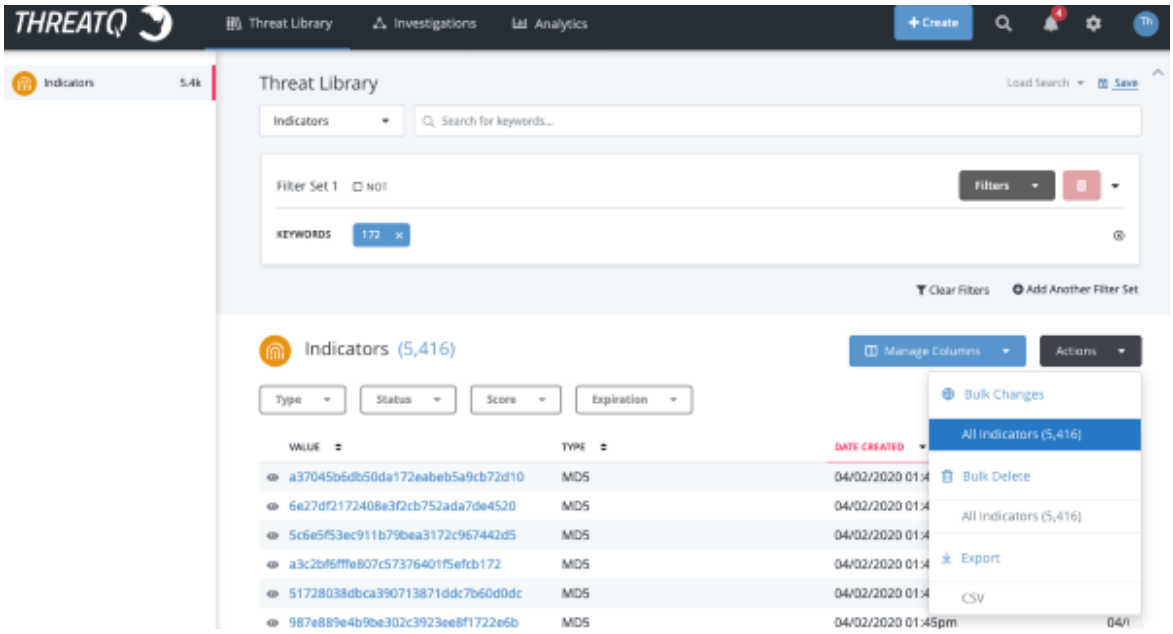
To Perform a Bulk Add Source

From the Advanced Search Page:

1. Perform an advanced search and create a filter set to narrow down your results - this step is optional.

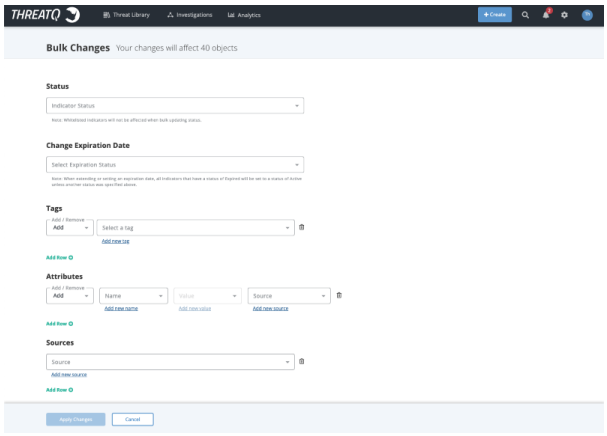


2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



> You will see the number of system objects affected next to the link in parentheses.

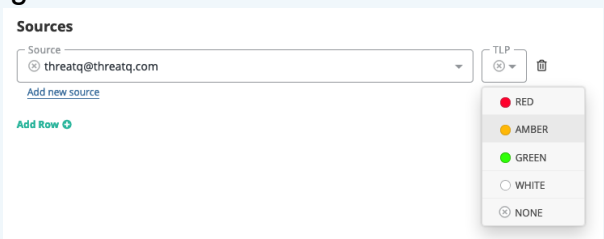
The Bulk Changes form will load.



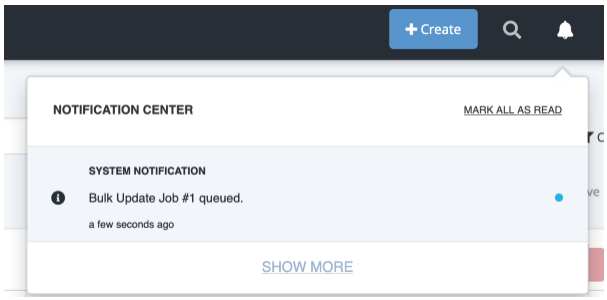
3. Click on **Add Row** under the **Source** heading.

   A new row with a dropdown option will load.

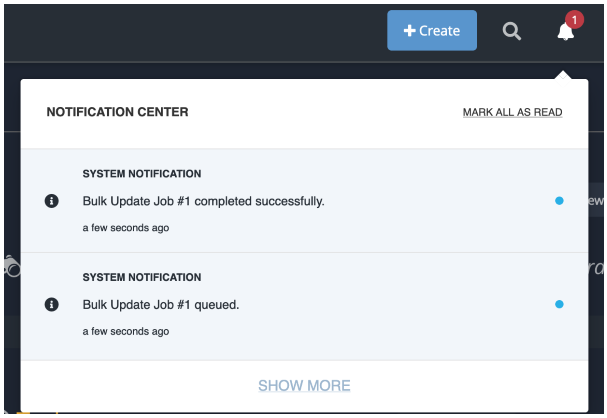
4. Use the dropdown to select the source to add to the selected objects. You can also use the **Add New Source** link to add a source that is not listed in the dropdown.

> If you have TLP enabled, you will also be able to update the designation for the source selected or keep the source-default designation.
>
> 
>

5. The job will be queued by the system and you will receive an in-app notification via the Notification Center icon.



The system will also notify you, via the Notification Center, that the job has been completed.



You can also view the status and other details of the job on the Job Management page.

Bulk Status Change

You can use the Bulk Change option to update the status for a group of objects on the Advanced Search page.

This function can only be performed on objects that use the status field such as Indicators, Signatures, etc.

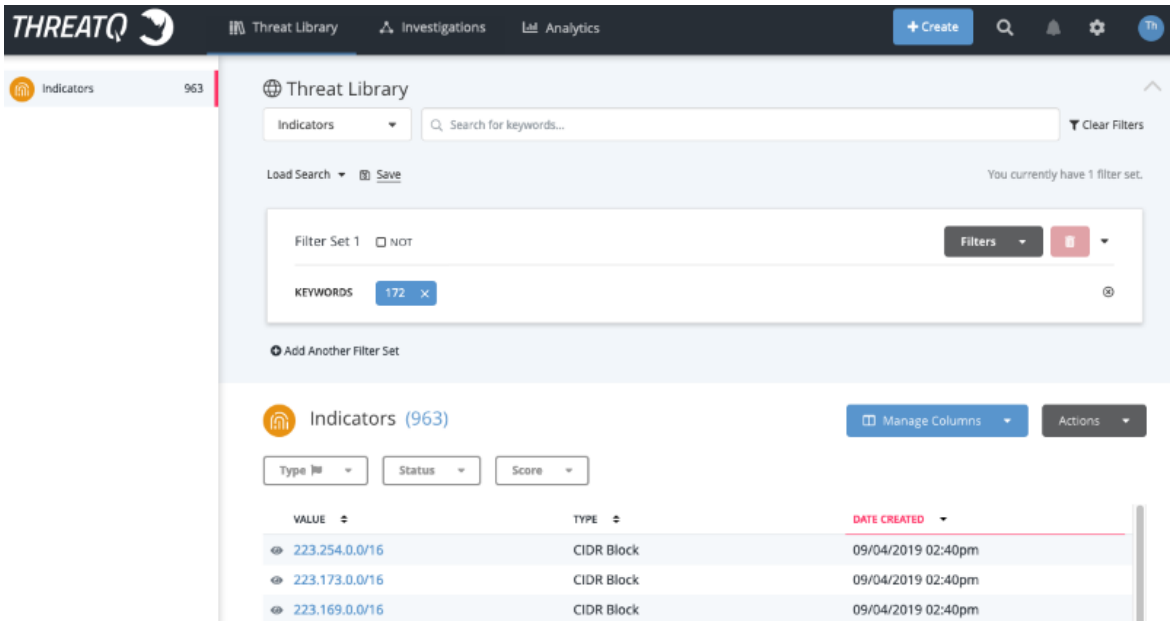
Whitelisted Indicators are not affected by Bulk Status Change. If a Whitelisted Indicator is included in the set of system objects selected for a Bulk

Status Change, the platform will skip the object without making a status change.

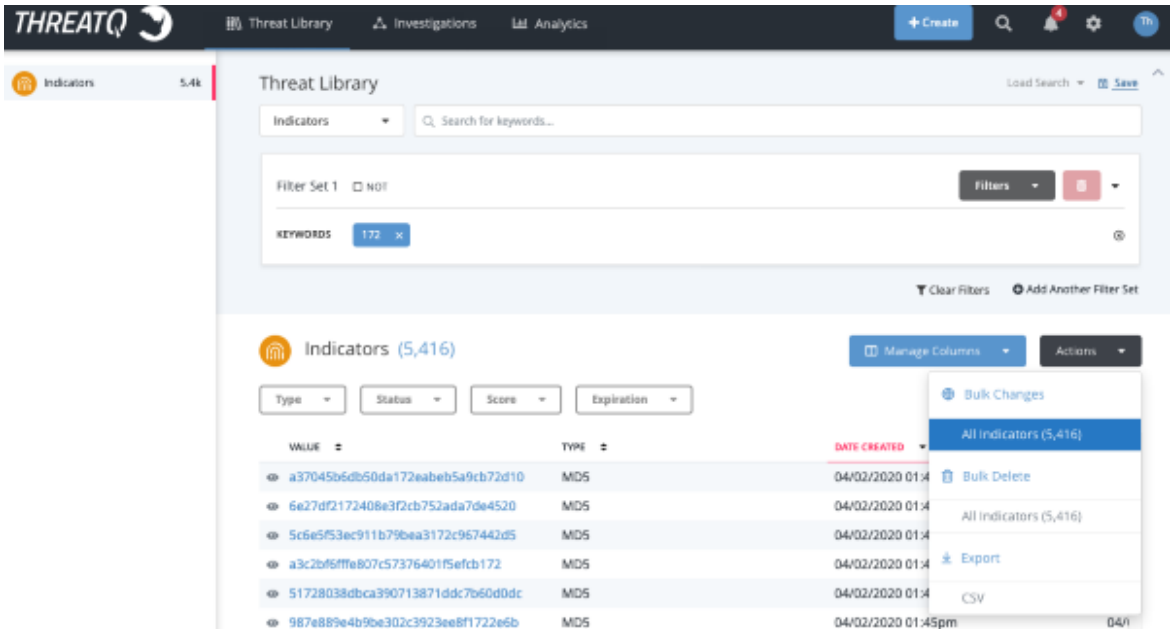
To Perform a Bulk Status Change

From the Advanced Search Page:

1. Perform an advanced search and create a filter set to narrow down your results - this step is optional.

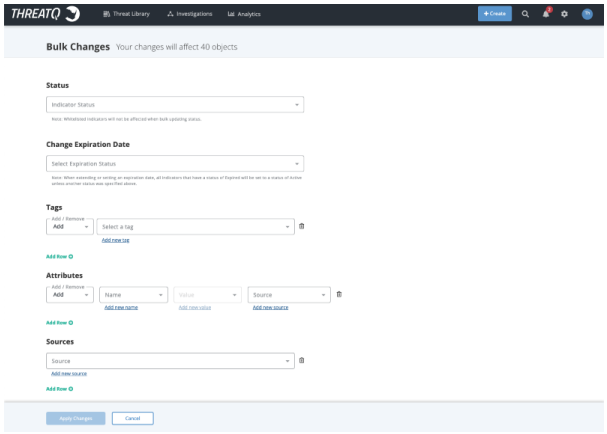


2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



You will see the number of system objects affected next to the link in parentheses.

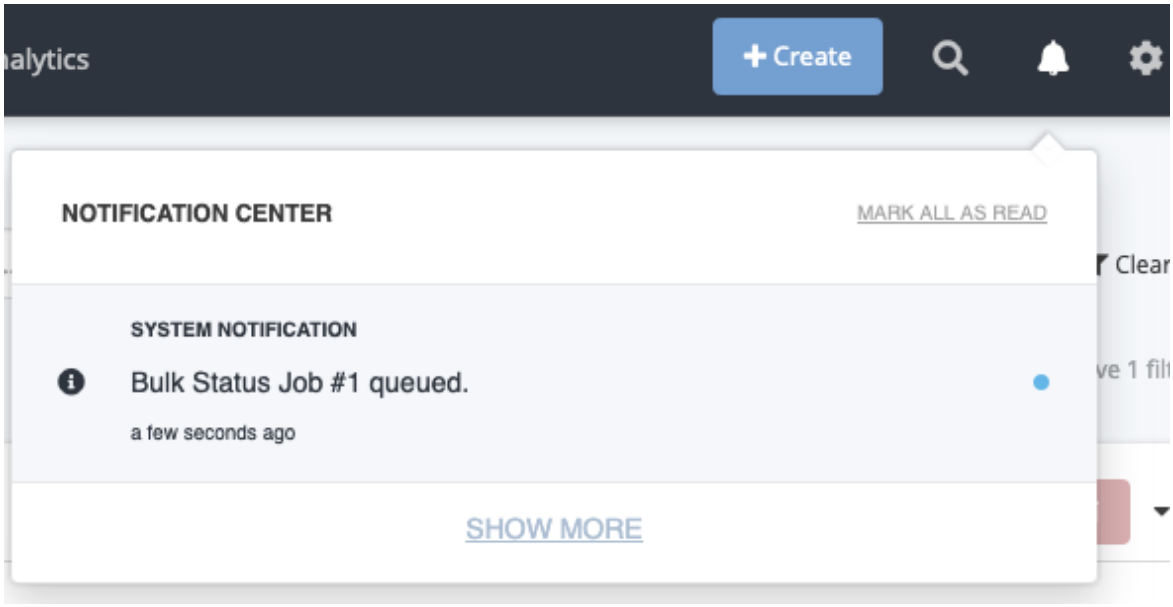
The Bulk Changes form will load.



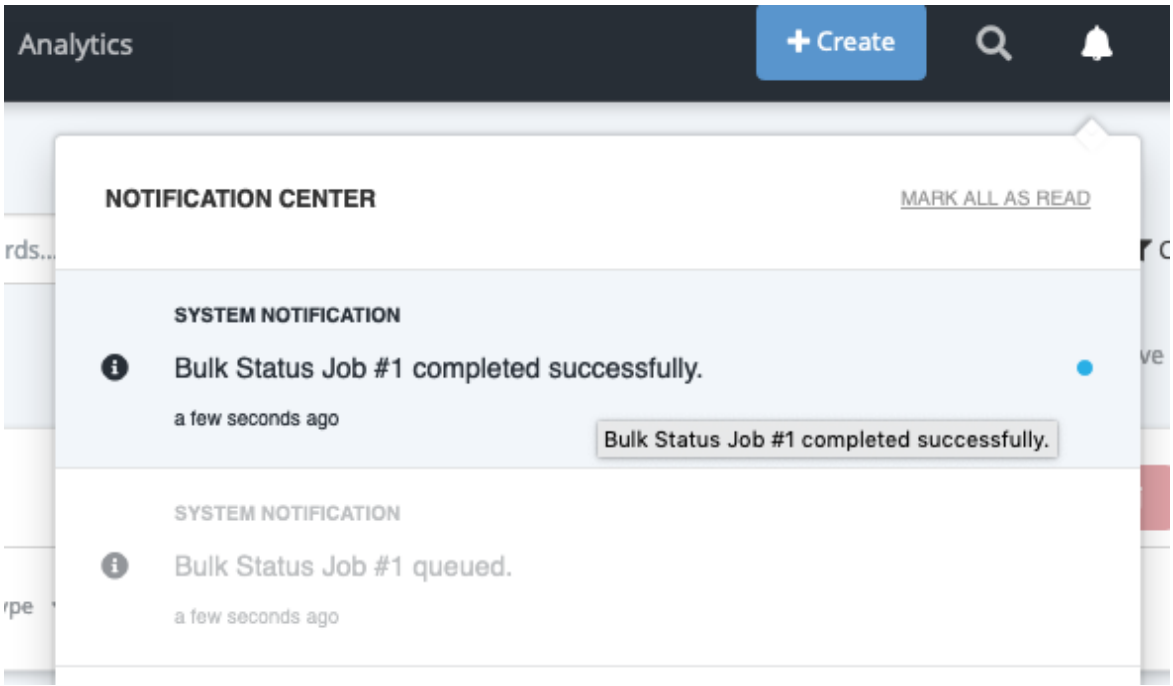
3. Use the dropdown provided to select a new status to be applied to the selected objects.

4. Click on **Apply Changes** located at the bottom of the form.

   The job will be queued by the system and you will receive an in-app notification via the Notification Center icon.



   The system will also notify you, via the Notification Center, that the job has been completed.



You can also view the status and other details of the job on the Job Management page.

Bulk Add/Remove Relationships

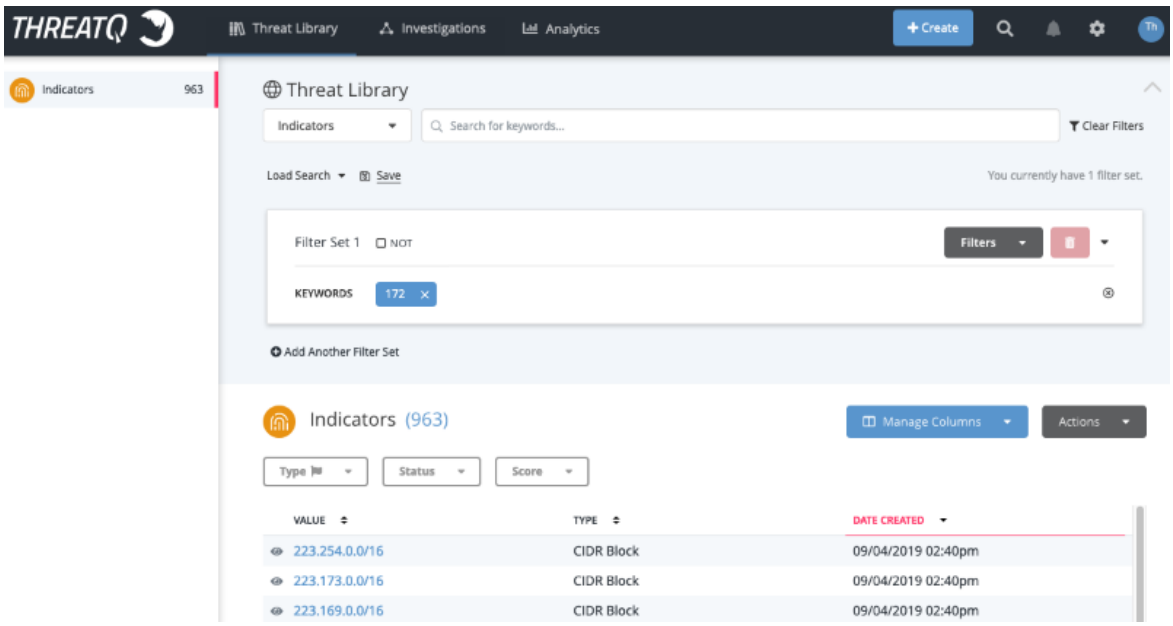
You can use the Bulk Change option to add/remove relationships for a group of objects, per object type, on the Advanced Search page.

If an object is already associated with the source selected for the Bulk Add Relationships action, the object will be skipped during the bulk process.

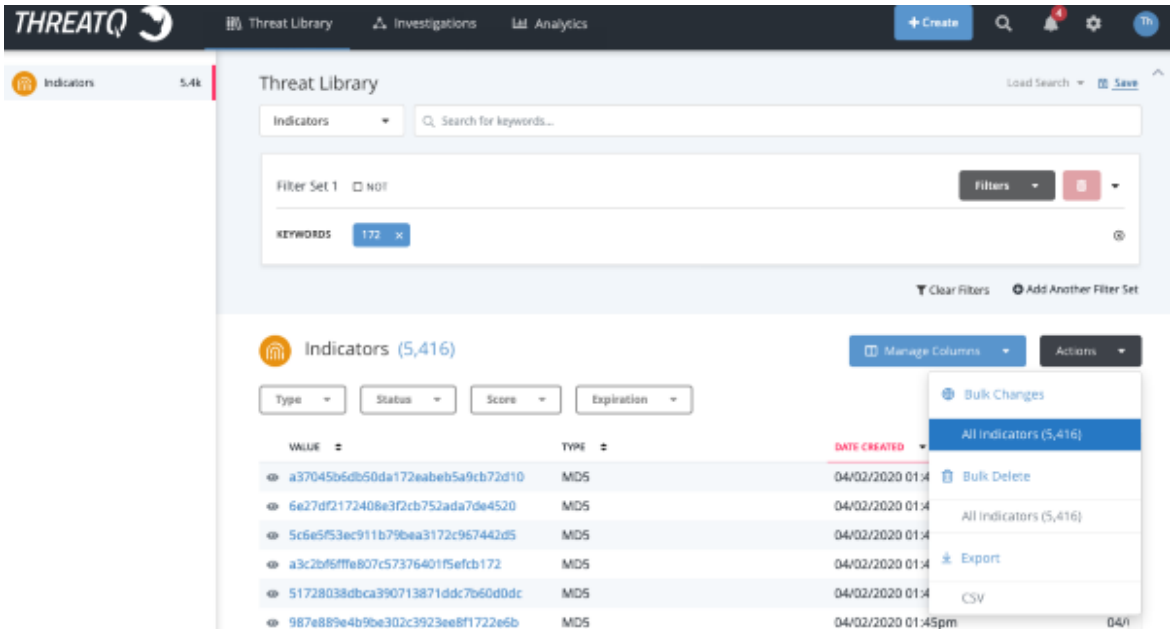
To Perform a Bulk Add Relationship

From the Threat Library:

1. Perform an advanced search and create a filter set to narrow down your results - this step is optional.

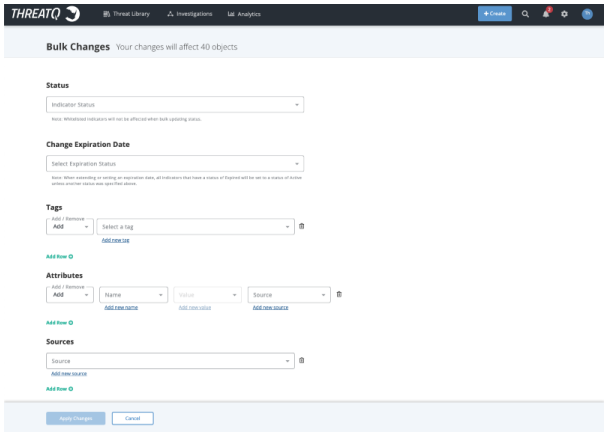


2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



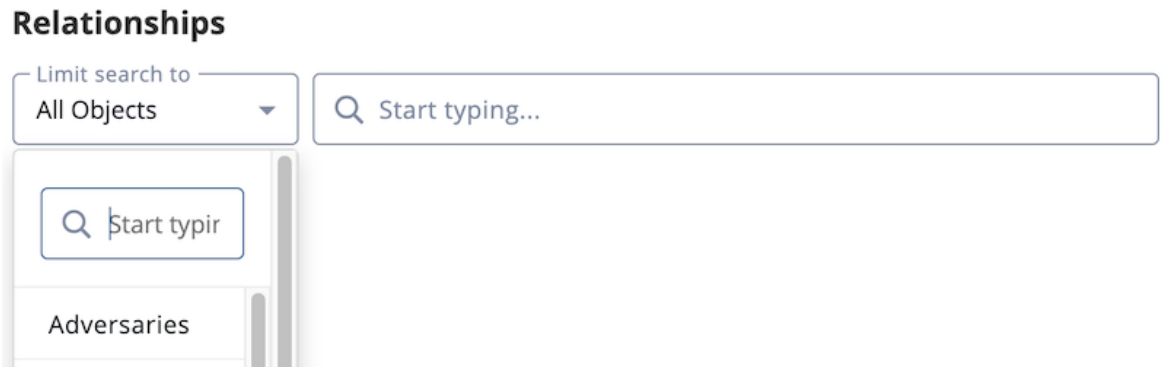
You will see the number of system objects affected next to the link in parentheses.

The Bulk Changes form will load.



Only the Bulk Actions that relate to the type of system object you selected will load on the Bulk Changes form. **Example:** Bulk Expiration Change will not load for non-indicators.

3. Locate the Relationships heading and optionally select **Limit Search To** to select an object type.

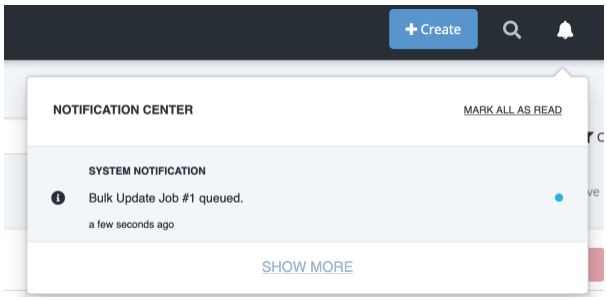


Enter an object name.

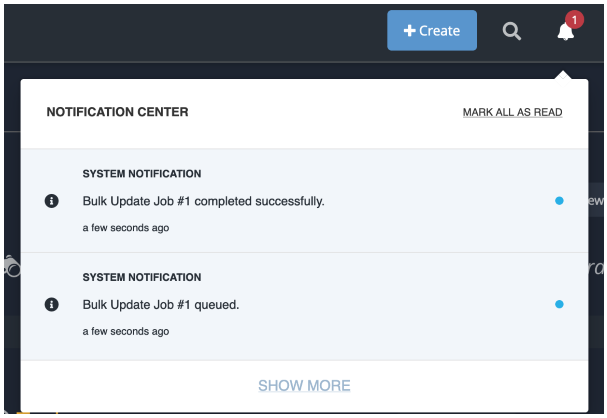
The Add/Remove option appears.

4. Select either **Add** or **Remove**.
5. Use the dropdown to select the source to add to the selected objects. You can also use the **Add New Source** link to add a source that is not listed in the dropdown.
6. Click on **Apply Changes** located at the bottom of the form.

The job will be queued by the system and you will receive an in-app notification via the Notification Center icon.



The system will also notify you, via the Notification Center, that the job has been completed.



You can also view the status and other details of the job on the Job Management page.

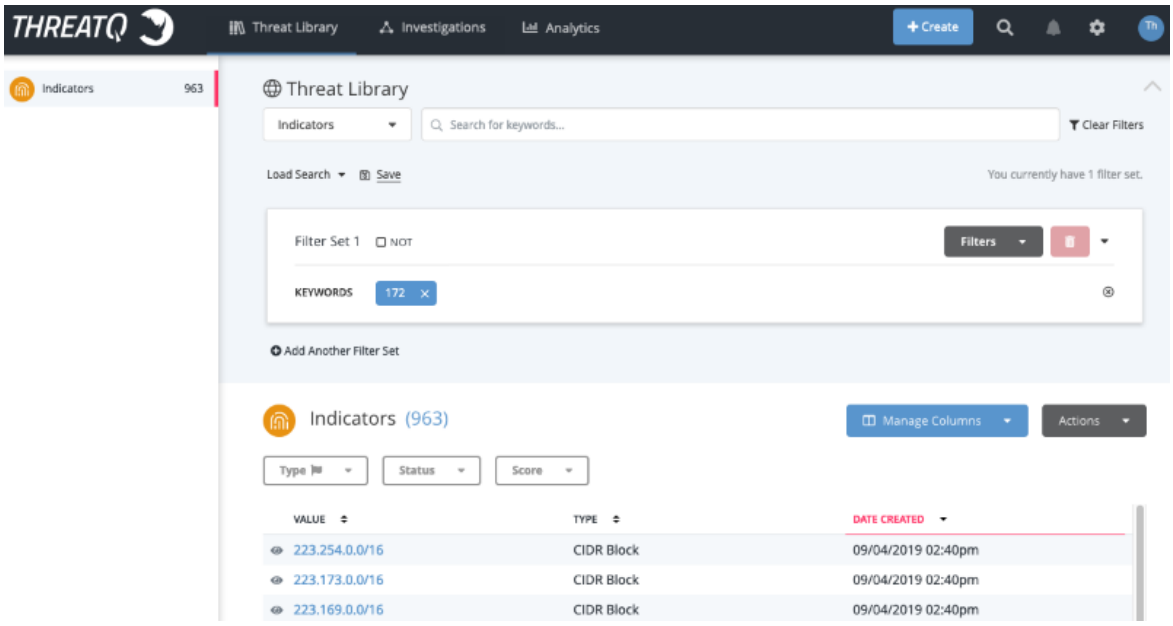
Bulk Add/Remove Tags

You can use the Bulk Change option to add/remove tags for a group of objects, per object type, on the Advanced Search page.

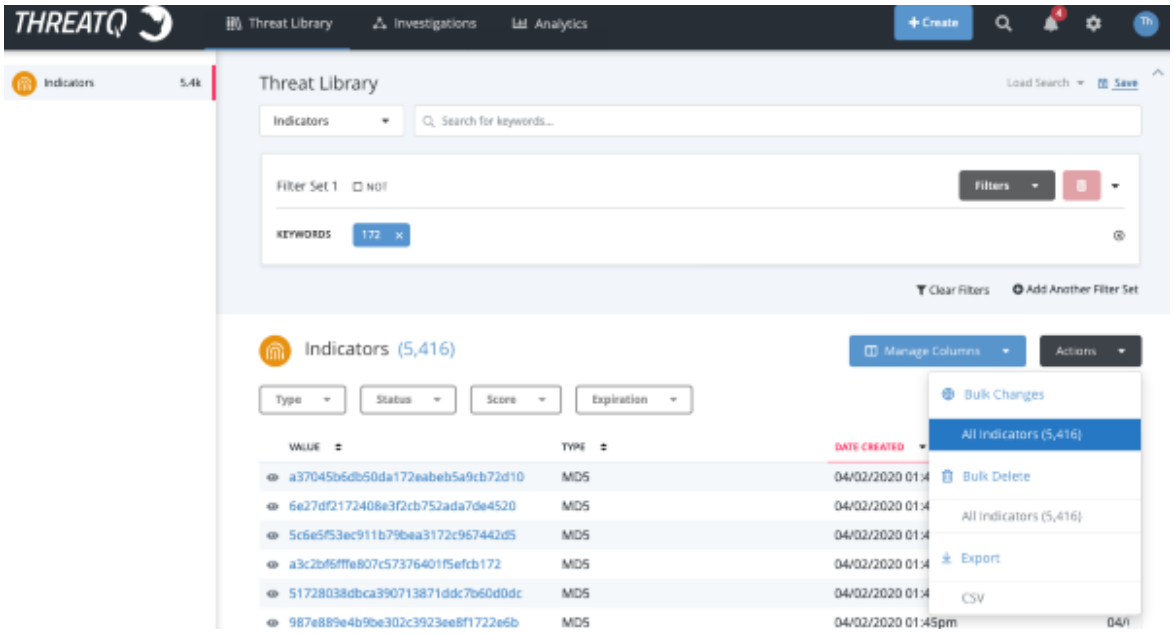
To Perform a Bulk Status Change

From the Advanced Search Page:

1. Perform an advanced search and create a filter set to narrow down your results - this step is optional.

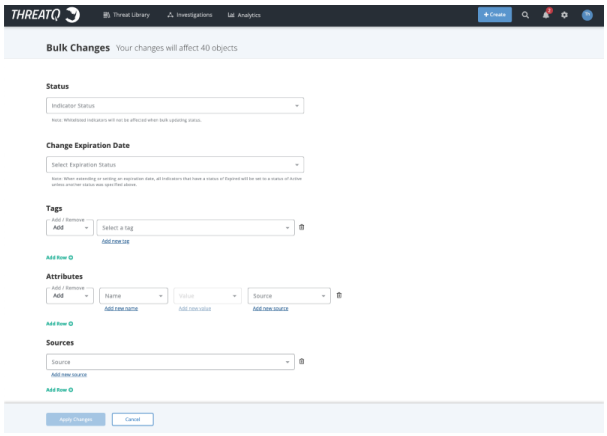


2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.

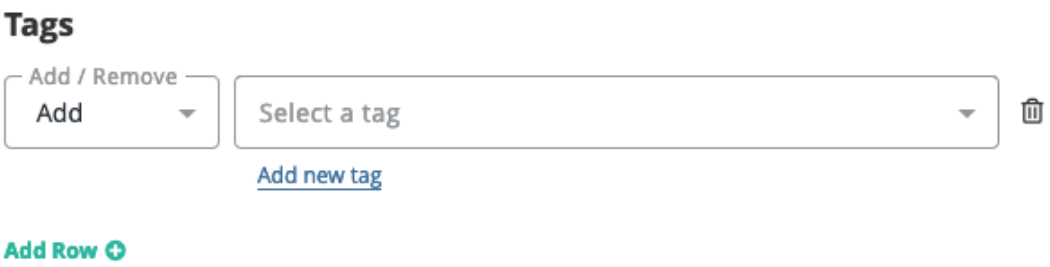


You will see the number of system objects affected next to the link in parentheses.

The Bulk Changes form will load.



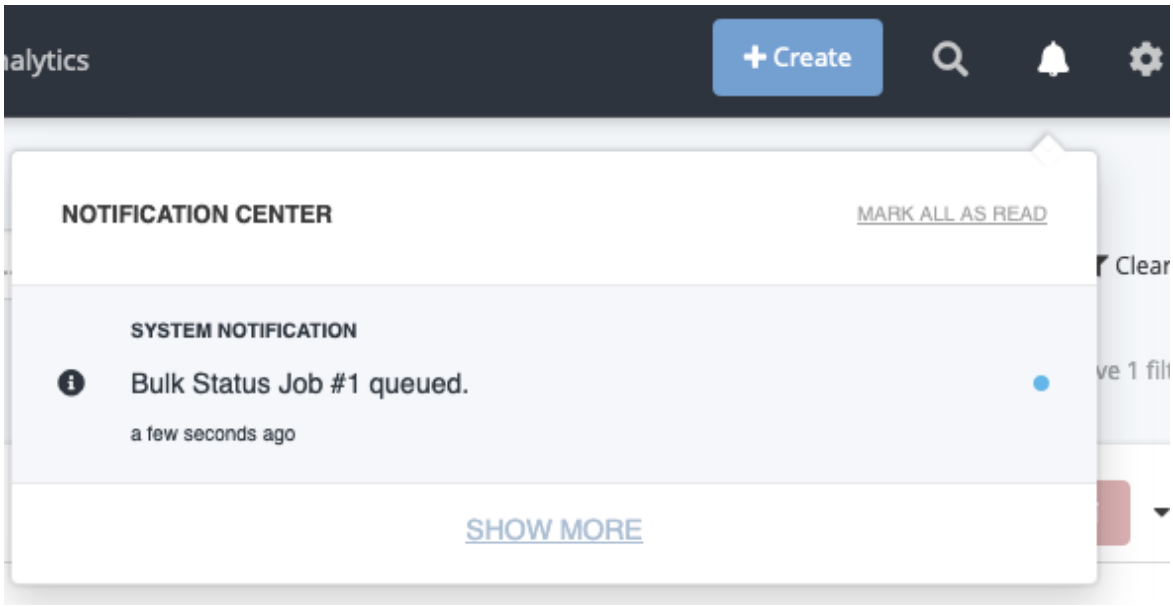
3. Select whether either the **Add** or **Remove** function and the **Tag**. You can also use the **Add New Tag** option if the desired tag is not listed in the dropdown.



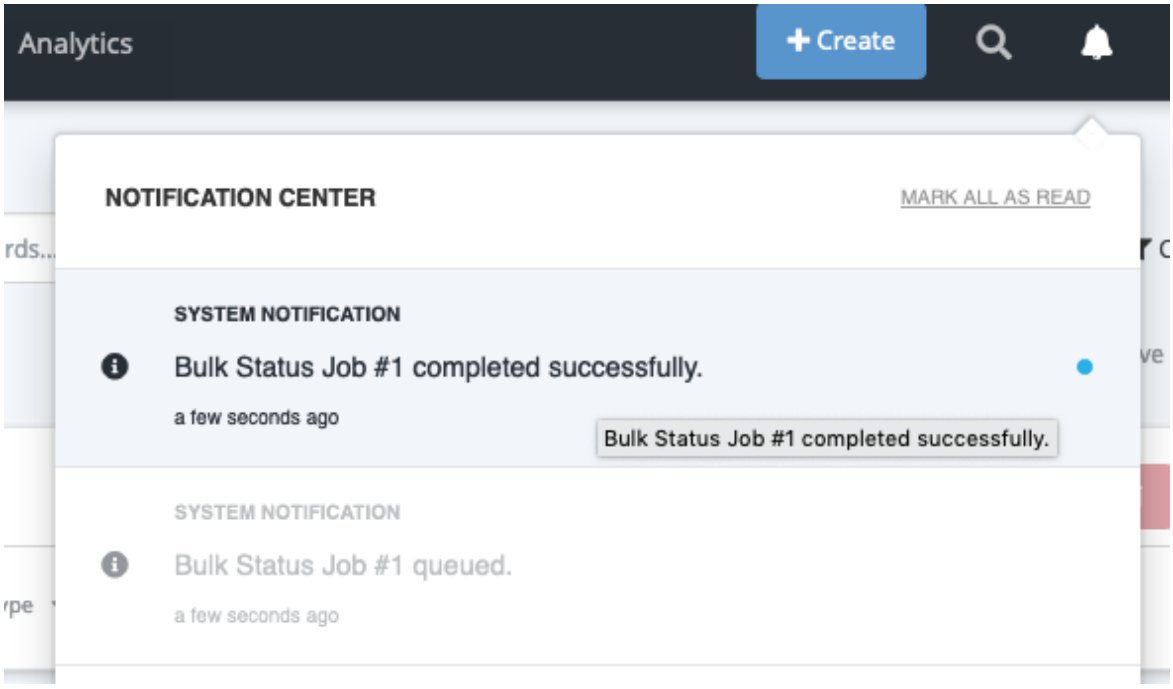
Click on **Add Row** and repeat step 3 to add/remove multiple tags.

4. Click on **Apply Changes** located at the bottom of the form.

The job will be queued by the system and you will receive an in-app notification via the Notification Center icon.



The system will also notify you, via the Notification Center, that the job has been completed.



You can also view the status and other details of the job on the Job Management page.

Bulk Add/Remove Attributes

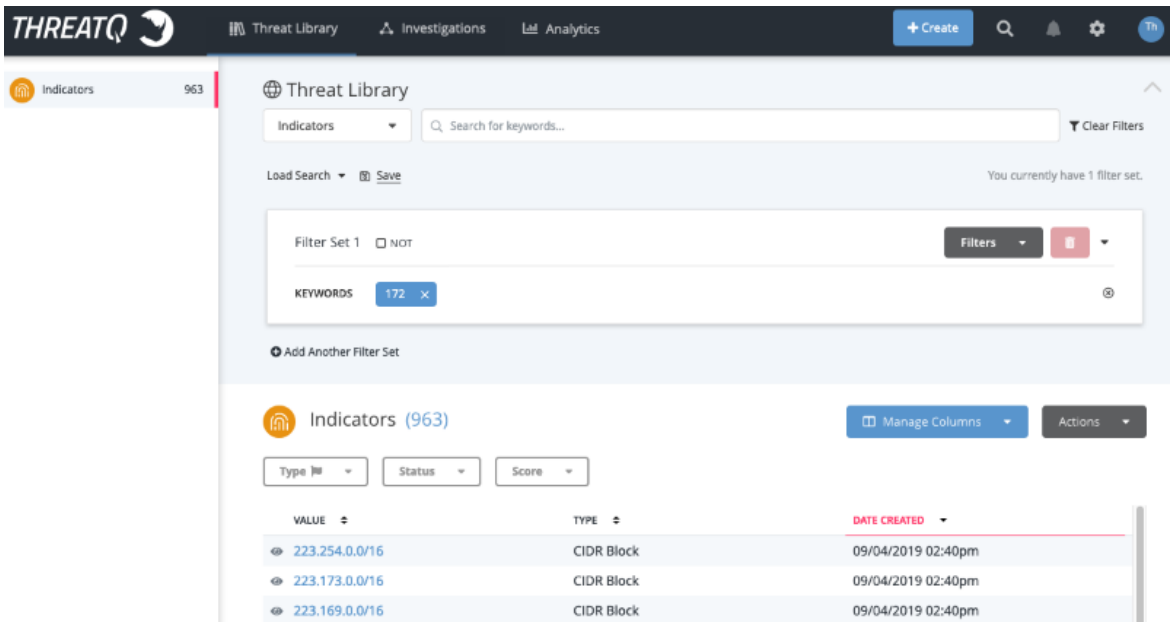
You can use the Bulk Change option to add/remove attributes for a group of objects, per object type, on the Advanced Search page.

> Using Bulk Actions to remove an attribute from the selected objects will remove the full attribute record regardless of how many sources the attribute may have.

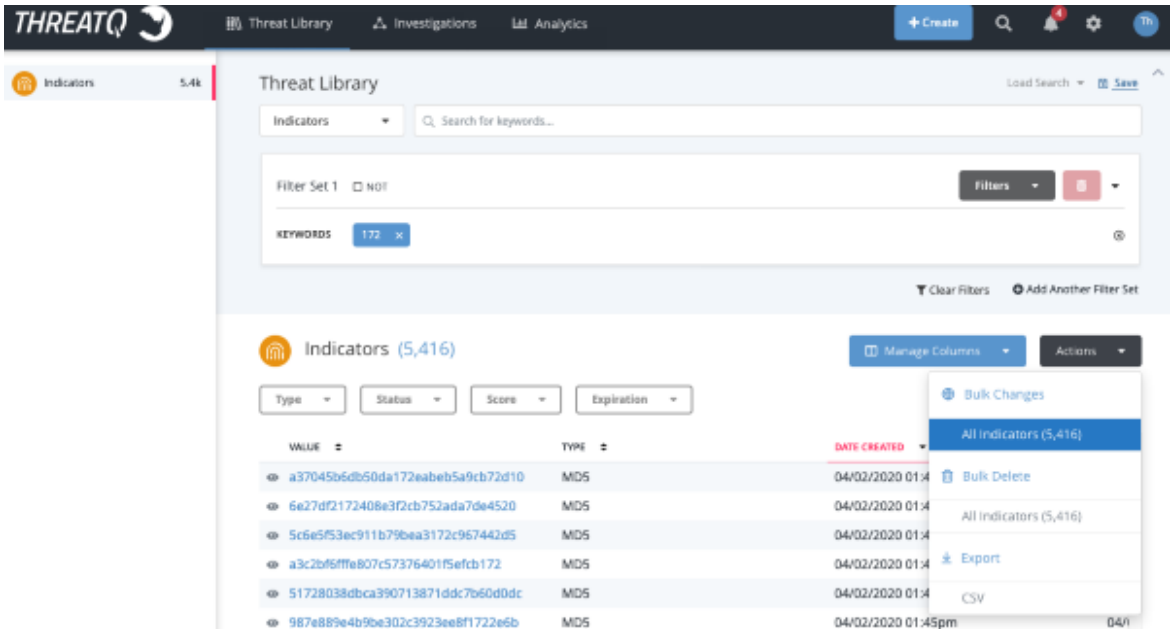
To Perform a Bulk Add Attribute

From the Advanced Search Page:

1. Perform an advanced search and create a filter set to narrow down your results - this step is optional.

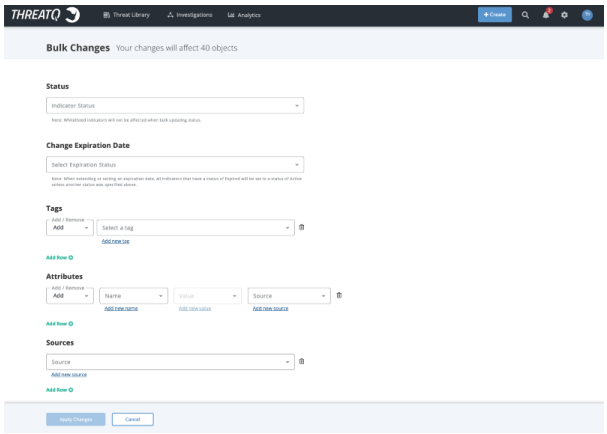


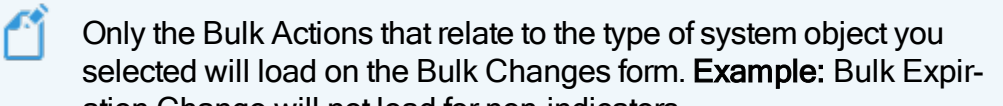
2. Click on the **Actions** dropdown and select **All <System Object>** under the *Bulk Changes* heading.



You will see the number of system objects affected next to the link in parentheses.

The Bulk Changes form will load.

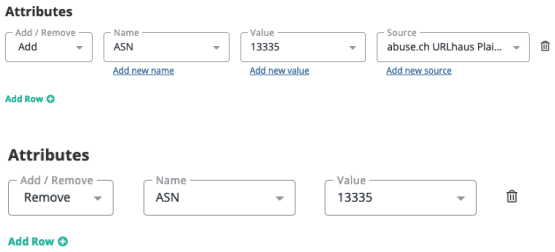




Only the Bulk Actions that relate to the type of system object you selected will load on the Bulk Changes form. **Example:** Bulk Expiration Change will not load for non-indicators.

3. Locate the Attributes heading and select either **Add** or **Remove**.

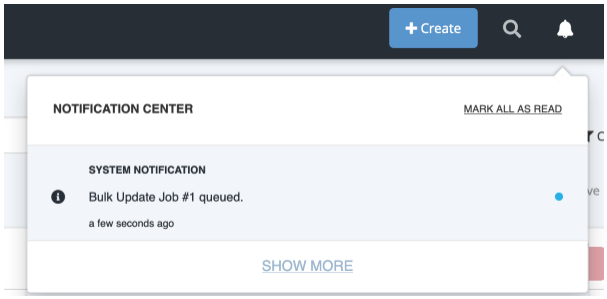
4. Select the attribute **Name** and **Value**. You can also use the **Add New Name** and **Add New Value** options to create new attributes. If you are adding an attribute, you will also select a **Source**. If you do not select a **Source**, the Source default will automatically be used.



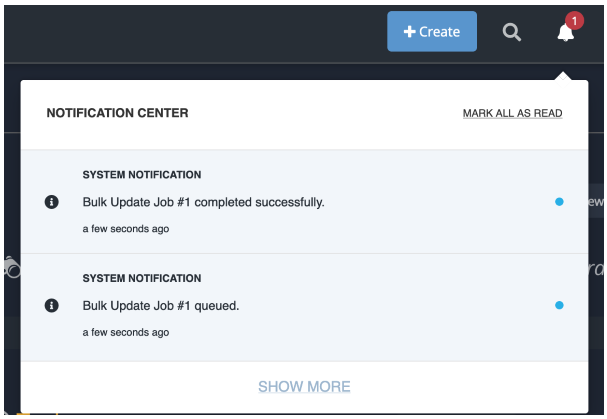
> Click on **Add Row** and repeat steps 3-4 to add/remove multiple attributes. See the Scenarios section below for more details.

5. Click on **Apply Changes** located at the bottom of the form.

   The job will be queued by the system and you will receive an in-app notification via the Notification Center icon.



The system will also notify you, via the Notification Center, that the job has been completed.



You can also view the status and other details of the job on the Job Management page.

Scenarios

Add Multiple Attributes

1. The user narrows down the Threat Library using advanced search filters.
2. The user selects **Bulk Changes** from the **Actions** dropdown.
3. The user enters the **Attribute Name**, **Value**, and **Source** for the first row in the *Attributes* section.
4. The user clicks on **Add Row**.
5. The user enters the **Attribute Name**, **Value**, and **Source** for the new row.
6. The user clicks on **Apply Changes**.

Results

- All objects with in the list will have those attributes added

The attributes will be listed in the audit log mentioning that this. The author of the action will be "Job ID <job_id_number> (<username>)"

Remove Multiple Attributes

1. The user narrows down the Threat Library using advanced search filters.
2. The user selects **Bulk Changes** from the **Actions** dropdown.
3. The user selects **Remove** from the dropdown in the *Attributes* section and then enters the **Attribute Name**, **Value**, and **Source** for the first row.
4. The user clicks on **Add Row**.
5. The user selects **Remove** from the dropdown and then enters the **Attribute Name**, **Value**, and **Source** for the second row.
6. The user clicks on **Apply Changes**.

Results

- All objects in that change set that have the attributes specified (exact Name, Value, Source) will have them removed

  The attributes will be listed in the audit log mentioning that this. The author of the action will be "Job ID <job_id_number> (<username>)"

- Any object that does not have the attributes specified (exact Name, Value, Source) will be skipped.

  There will be no mentions of the job in the audit log for those objects because no changes were made.

Add and Remove Attributes

In this scenario, the platform will execute the Bulk Changes in the following order:

1. Add Attributes - See the Add Multiple Attributes Scenario above.
2. Remove Attributes - See the Remove Multiple Attributes Scenario above.

Managing Saved Searches

If you are following a particular area of interest, you can create a Saved Search. Saved Searches can then be run at any time.

Related Topics:

- Saving Searches
- Running Saved Searches
- Deleting Saved Search

Saving Searches

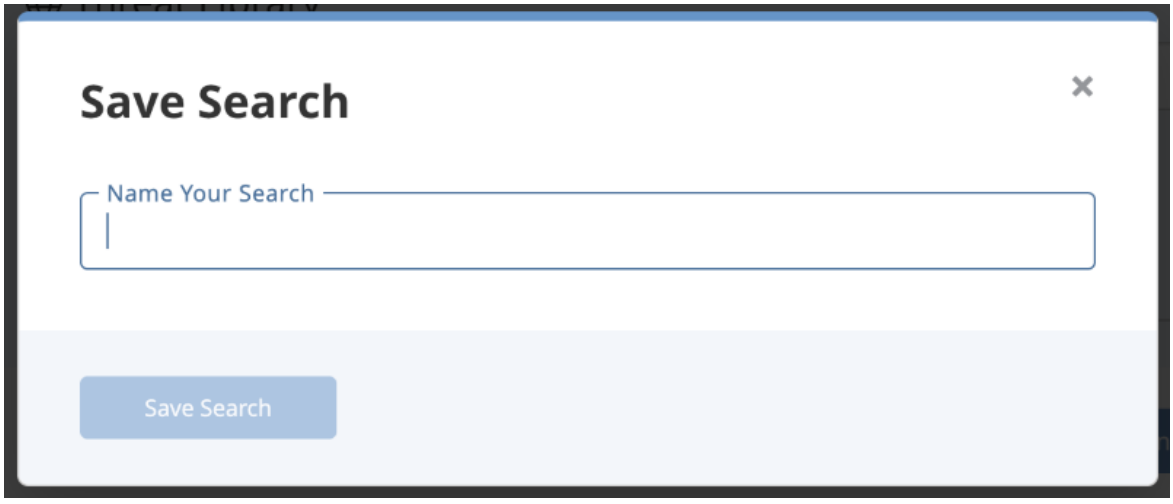
To save a search:

1. Choose the **Search** icon.
2. In the Search dialog box, choose **Advanced Search**.

   > You can also select **Threat Library** > **Object Type** to navigate to the advanced search page for a specific object type.

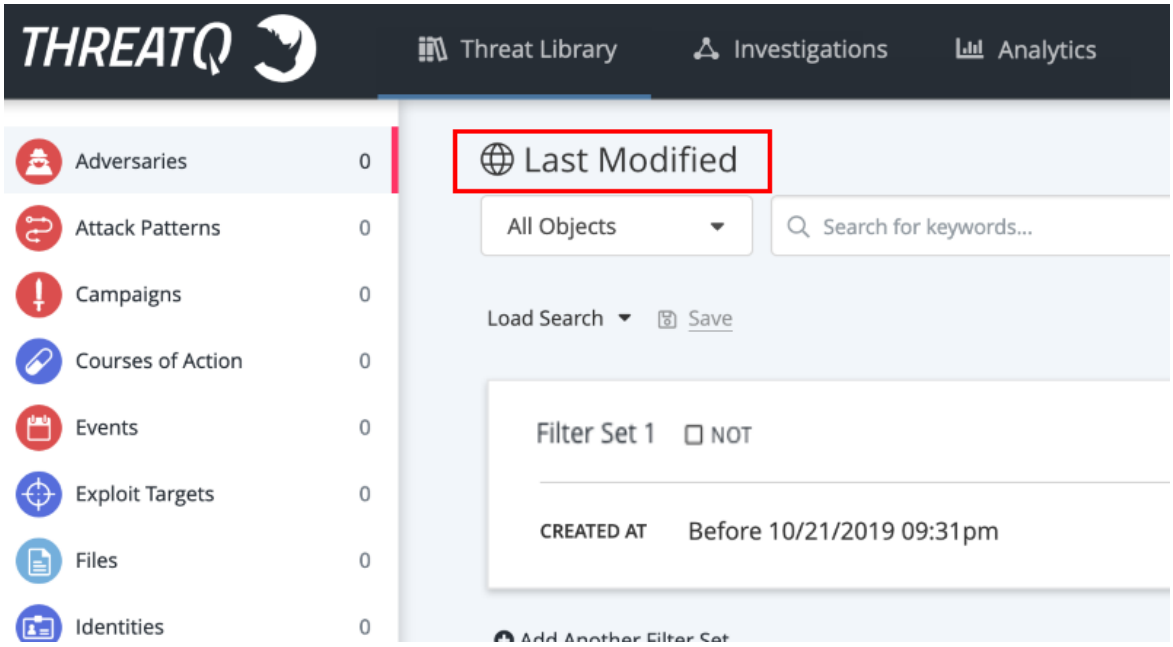
3. Perform an Advanced Search.
4. Choose **Save**.

   The Save Search dialog box opens.



5. Enter a name for the search in the Save Search dialog box.
6. Choose **Save Search**.

   The name of the saved search will appear at the top of the page.

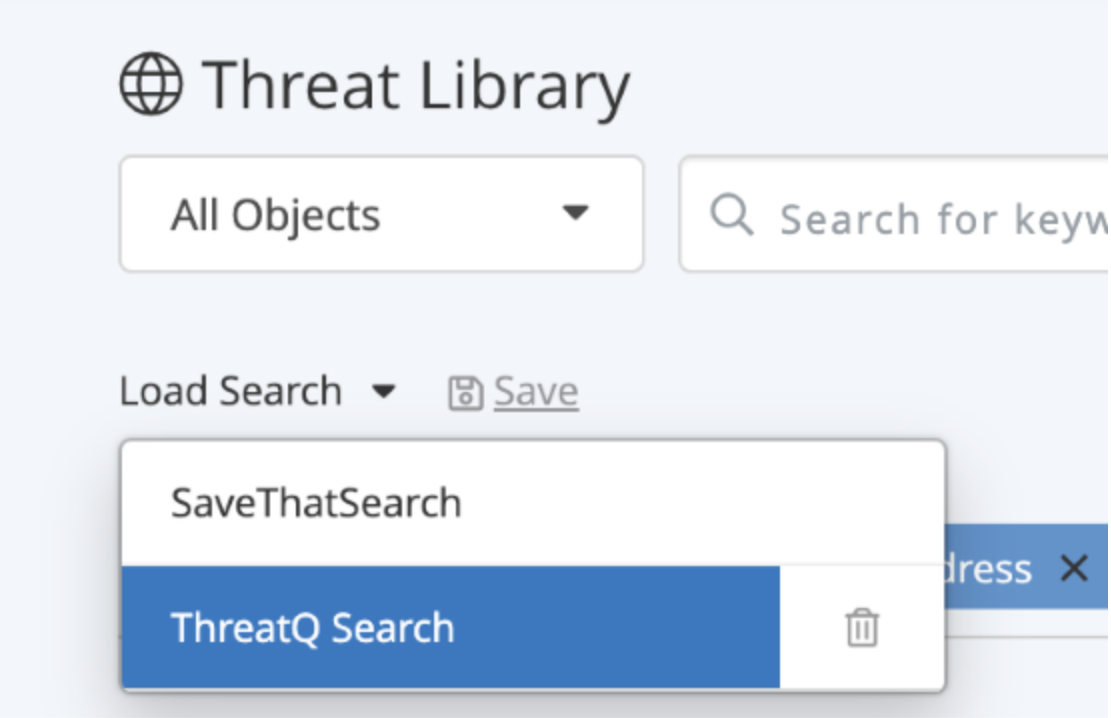


Running Saved Searches

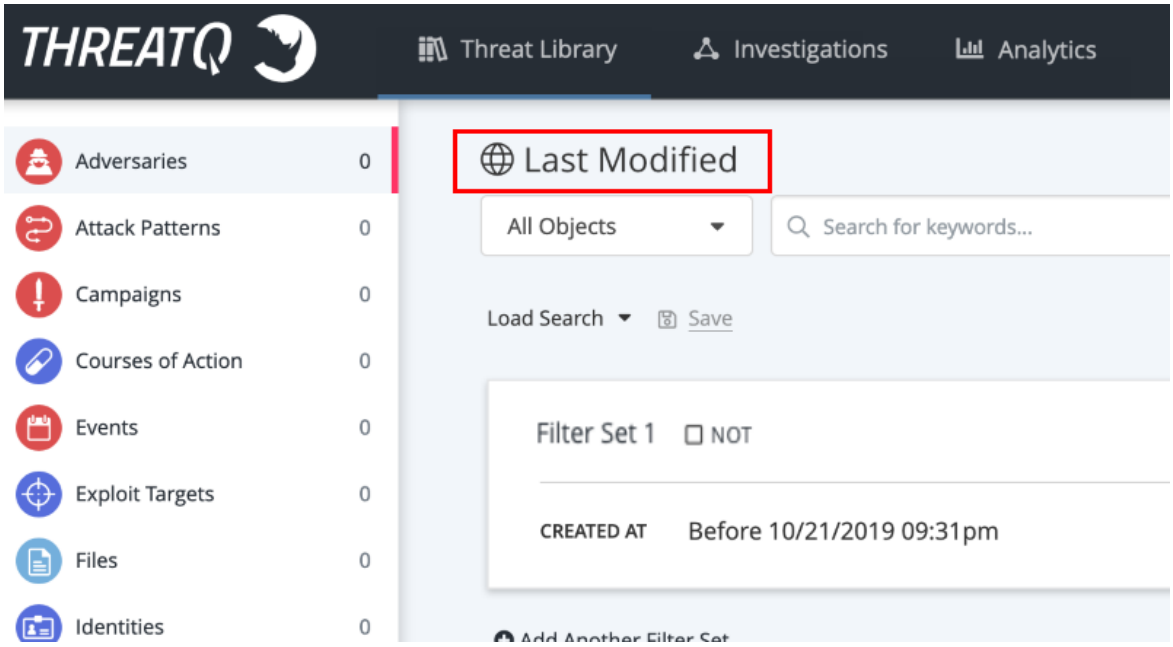
To run a saved search:

1. Navigate to the Advanced Search page.

2. Click on the **Load Search** dropdown list and then select the desired saved search from the list.



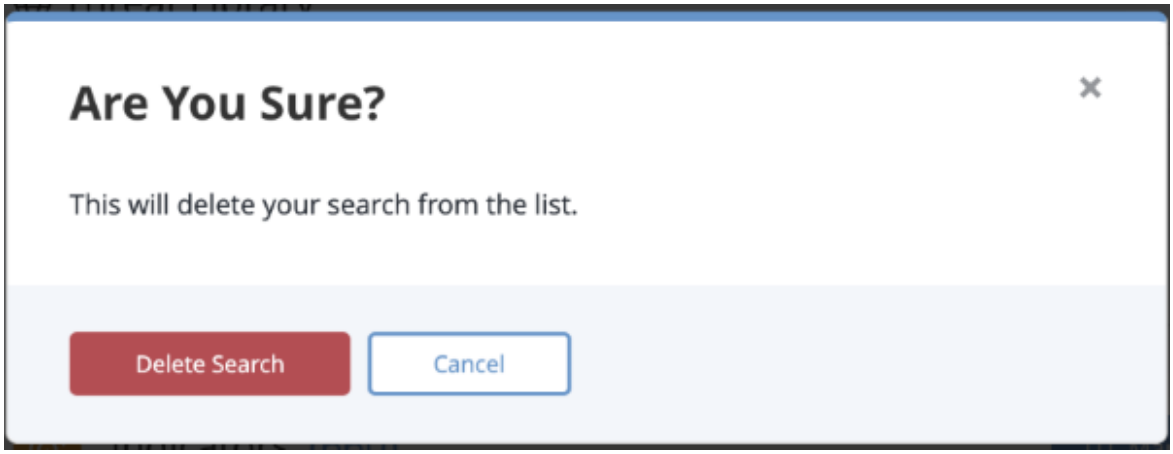
3. The saved search will load. The name of saved search will appear at the top of the page.



Deleting Saved Search

To delete a saved search:

1. Navigate to the Advanced Search page.
2. Click on the **Load Search** dropdown, hover the mouse over the saved search to delete, and click on the icon.
3. Click on **Delete Search** to confirm.



Exporting Search Results to CSV

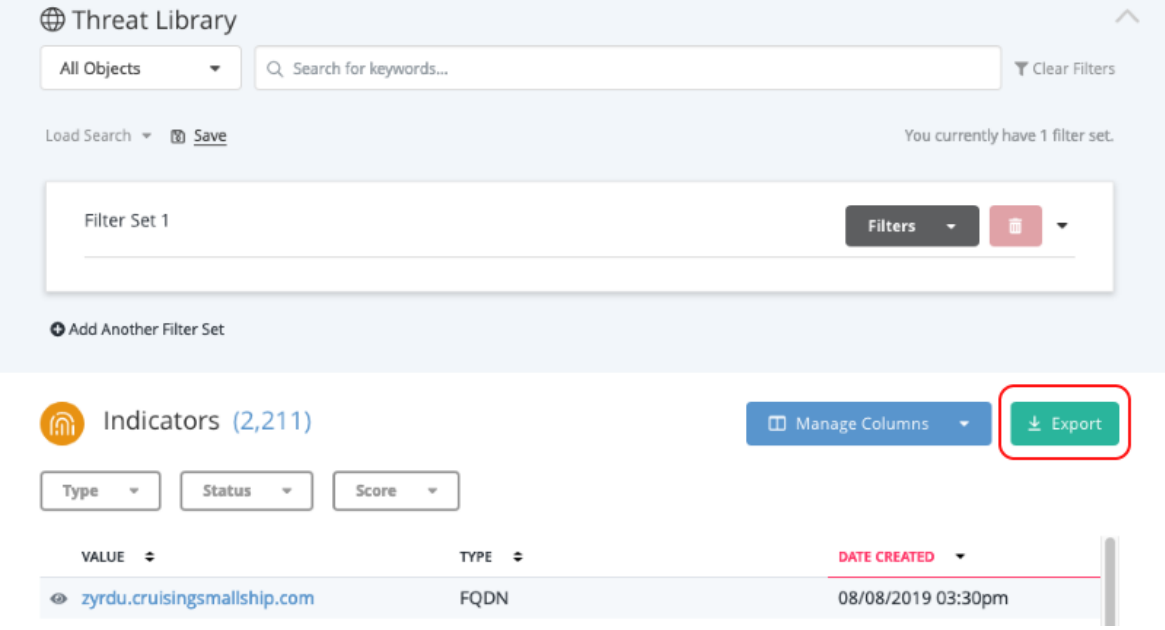
You can export your search results as a CSV file, which allows you to use the data in another application, such as external spreadsheet software.

If you export a file with too many search results, the file may be too large to open in desktop applications. If you encounter this issue, you should separate your exports into smaller chunks of data.

When exporting search results to a CSV file, if you include additional columns beyond the default, this modification will impact the performance of the export process.

To export search results to a CSV file:

1. Navigate to the Advanced Search page.
2. Perform your search.
3. Choose **Export**.



The CSV file downloads to your desktop.

System Objects

Threat data, both ingested and manually added, is referred to as System Objects and is sorted and categorized by object type.

See the topics below to learn more about each object type and how to manage them.

System Objects:

- Adversaries
- Events
- Files
- Indicators

- Signatures
- STIX Overview

Adversaries

Adversaries are the suspected groups that are attempting to do malicious activity.

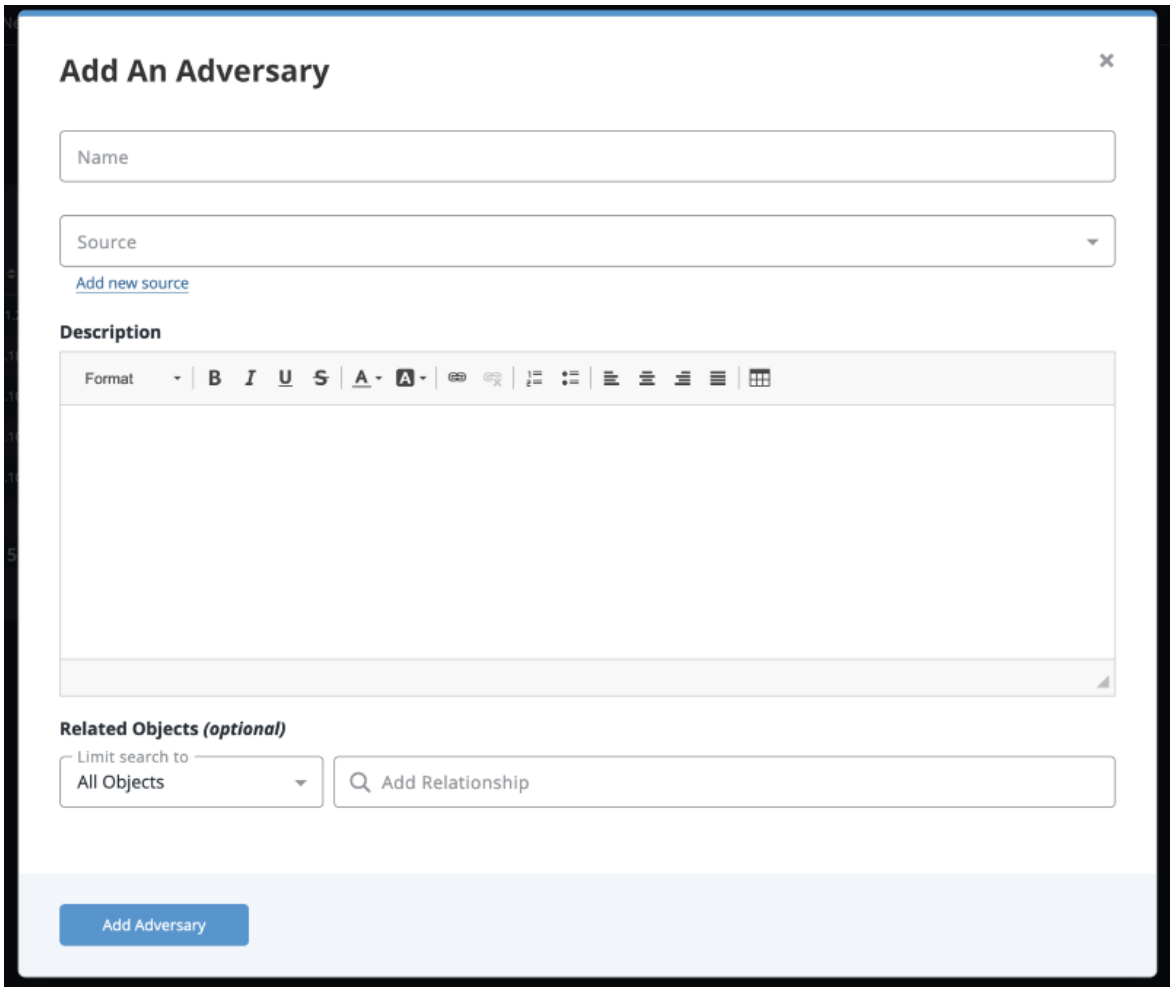
Related Topics

- Adding Adversaries
- Editing Adversaries
- Deleting Adversaries

Adding Adversaries

To create an Adversary:

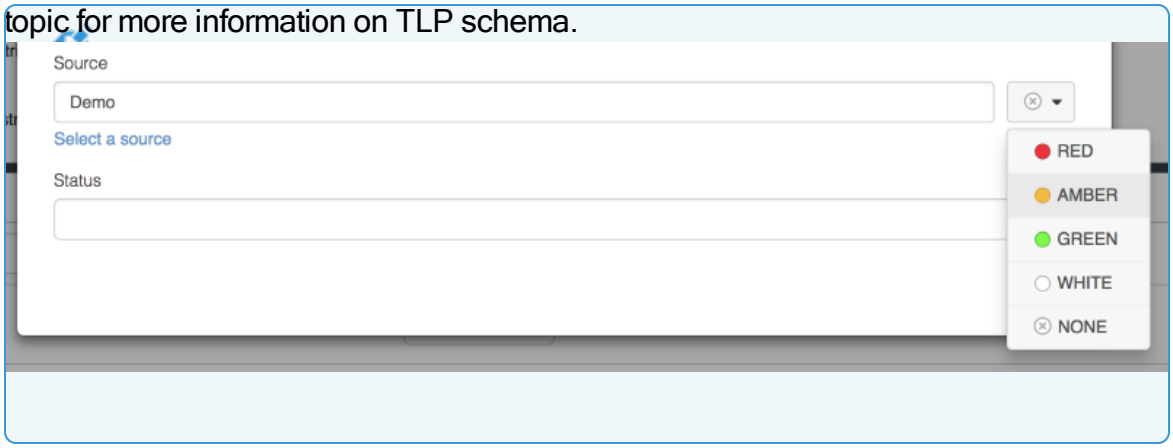
1. Go to **Create > Adversary**.
   The Add an Adversary dialog box opens.



2. Enter a name.
3. Select a **Source** from the dropdown provided.

> You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP designation light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP)

topic for more information on TLP schema.

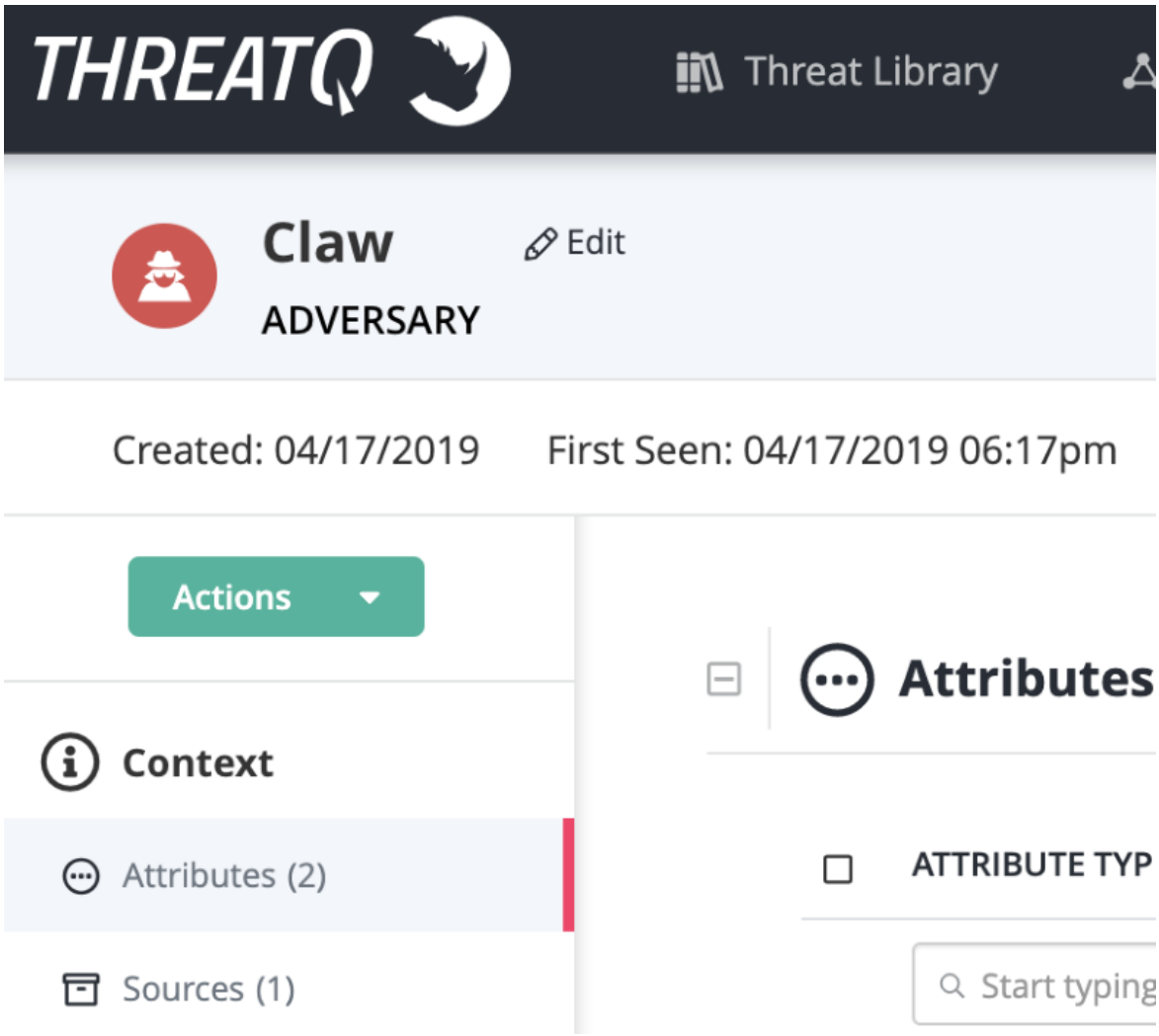


4. Enter a description.
5. Select any **Related Objects** you need to link to the adversary. This field is optional.
6. Click **Add Adversary**.

Editing Adversaries

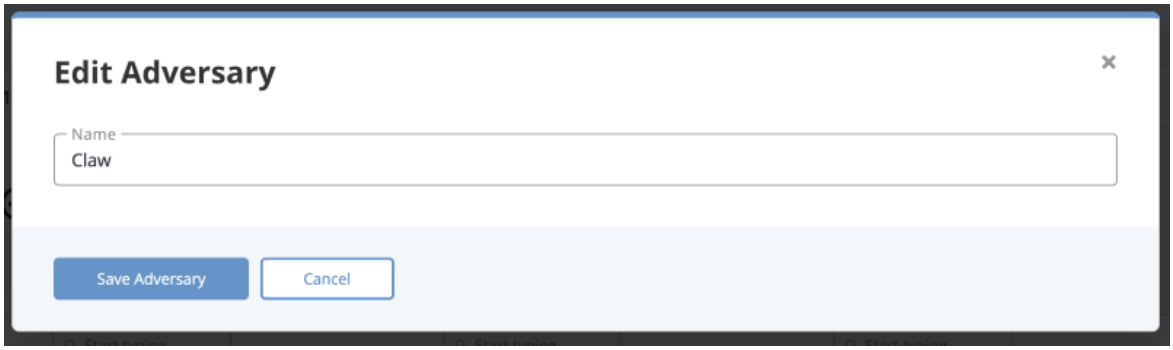
To edit the name of an Adversary:

1. Locate and click the adversary.
   The Adversary Details page opens.



2. Click on **Edit** next to the Adversary name.

   The Edit Adversary dialog box opens.



3. Make the desired change to the Adversary name.

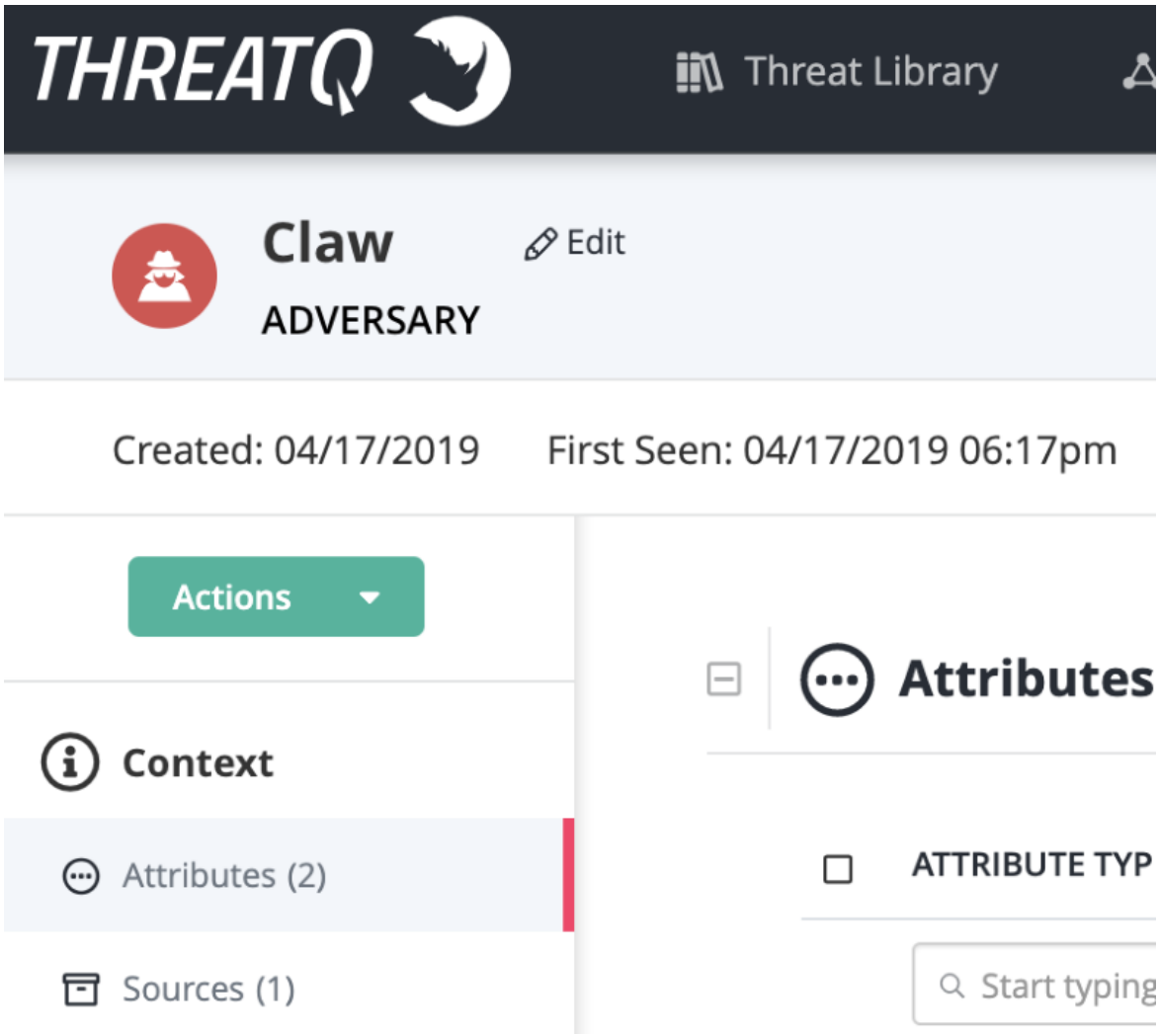
4. Click on **Save Adversary**.

Deleting Adversaries

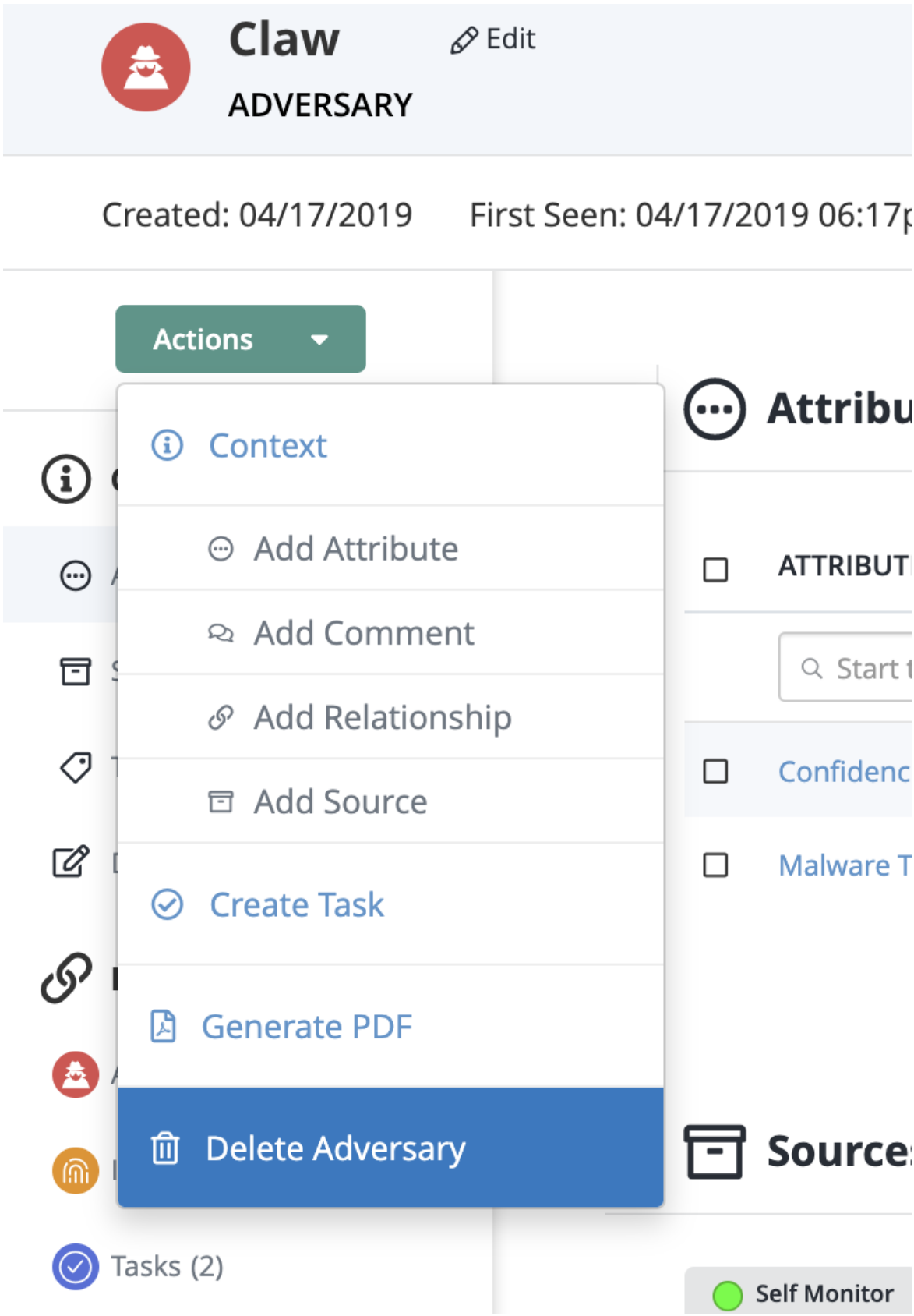
To delete an Adversary:

1. Locate and click on the adversary.

   The Adversary Details page opens.


THREATQ
Threat Library
Claw
Edit
ADVERSARY
Created: 04/17/2019
First Seen: 04/17/2019 06:17pm
Actions
Attributes
Context
ATTRIBUTE TYP
Attributes (2)
Start typing
Sources (1)

2. Click on the **Actions** menu and select **Delete Adversary**.


Claw
Edit
ADVERSARY
Created: 04/17/2019
First Seen: 04/17/2019 06:17p
Actions
Context
Add Attribute
Add Comment
Add Relationship
Add Source
Create Task
Generate PDF
Delete Adversary
Attribu
ATTRIBUT
Start t
Confidenc
Malware T
Source
Tasks (2)
Self Monitor

A confirmation dialog box appears.

3. Click on **Delete Adversary**.

Events

Events are observations made by the threat intelligence community of adversaries' malicious attempts.

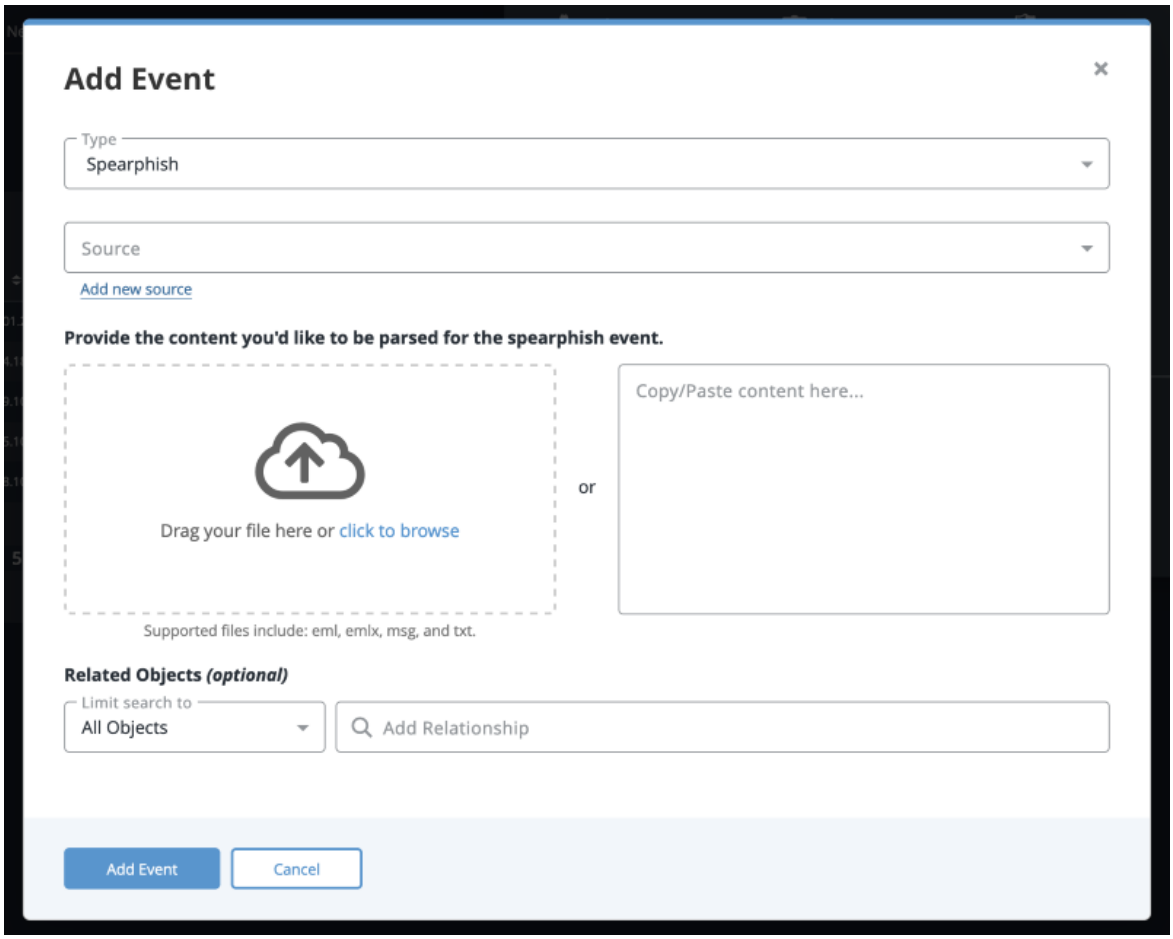
Related Topics:

- Adding Events
- Editing Events
- Deleting Events

Adding Events

To add an Event:

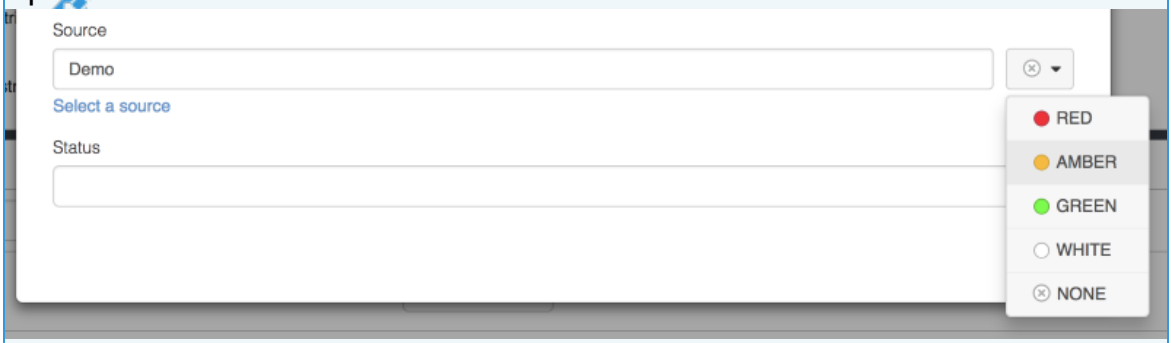
1. Go to **Create > Event**.
   The Add Event dialog box opens.



2. Select the **Event Type**.
3. Select a **Source** from the dropdown list provided.

> You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP designation light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP)

topic for more information on TLP schema.



4. Add the date and time the event occurred in the **Date of Occurrence** fields.
5. Add an **Event Title**.
6. Select any **Related Objects** you need to link to the event. This field is optional.
7. Click **Add Event**.

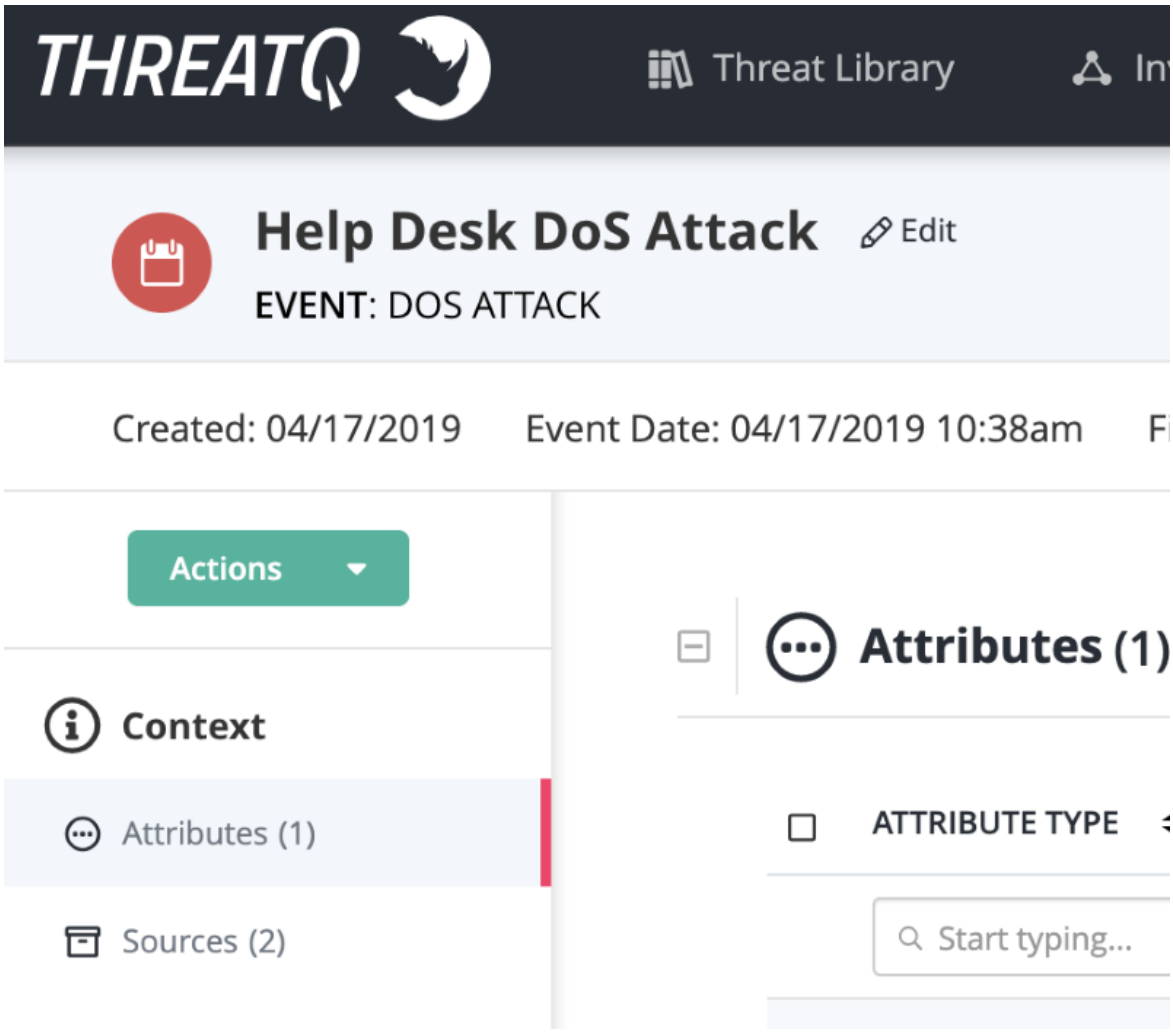
Editing Events

To edit an Event:

You can also update the Event Type by clicking on the **Type** dropdown located to the top-right of the Event's Object Details page.

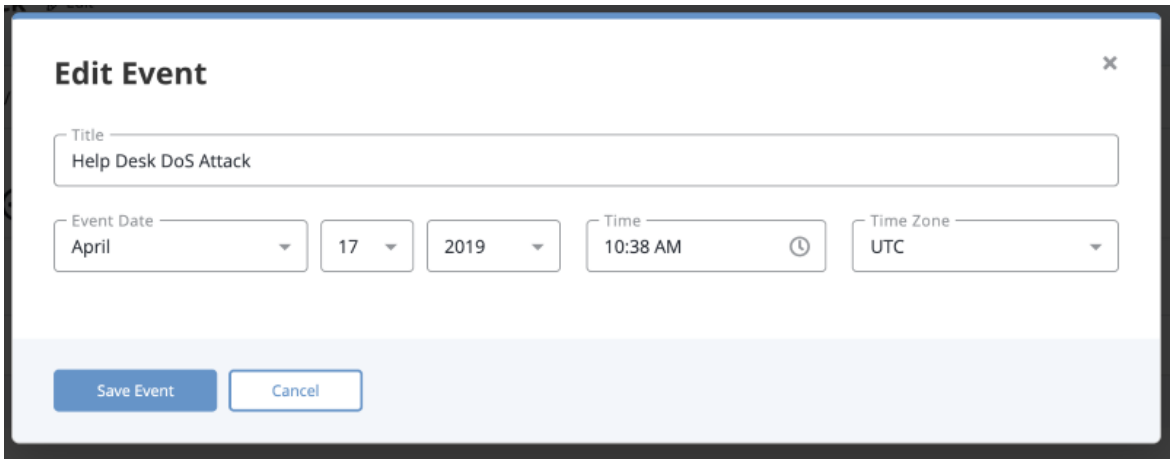
1. Locate and click on the event.

   The Event Details page opens.


THREATQ
Threat Library
Help Desk DoS Attack
Edit
EVENT: DOS ATTACK
Created: 04/17/2019
Event Date: 04/17/2019 10:38am
Actions
Context
Attributes (1)
Sources (2)
Attributes (1)
ATTRIBUTE TYPE
Start typing...

2. Click on **Edit** next to the Event name.

   The Edit Event dialog box opens.



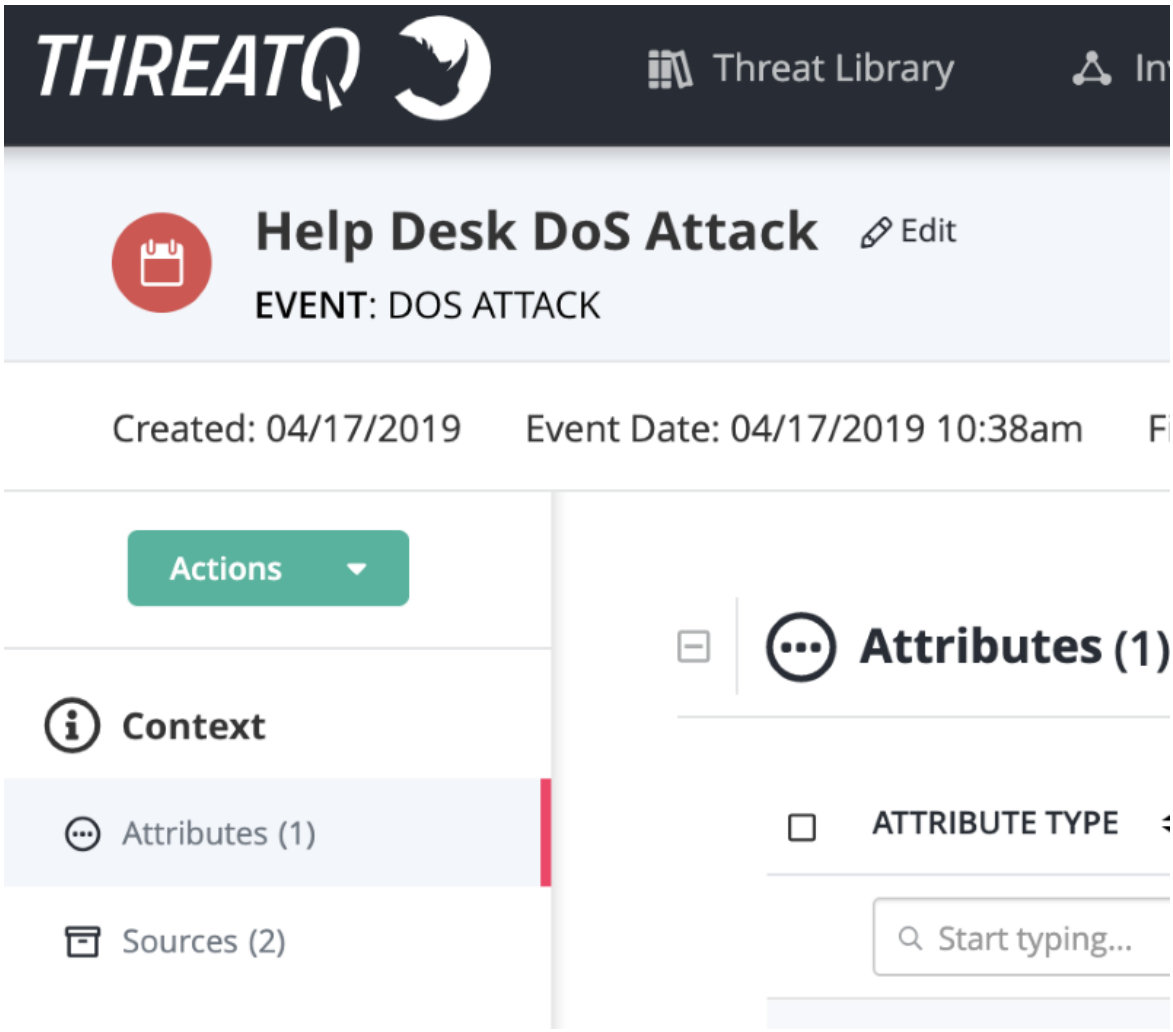
3. Make the desired change to the Event Name and Event Date.
4. Click on **Save Event**.

Deleting Events

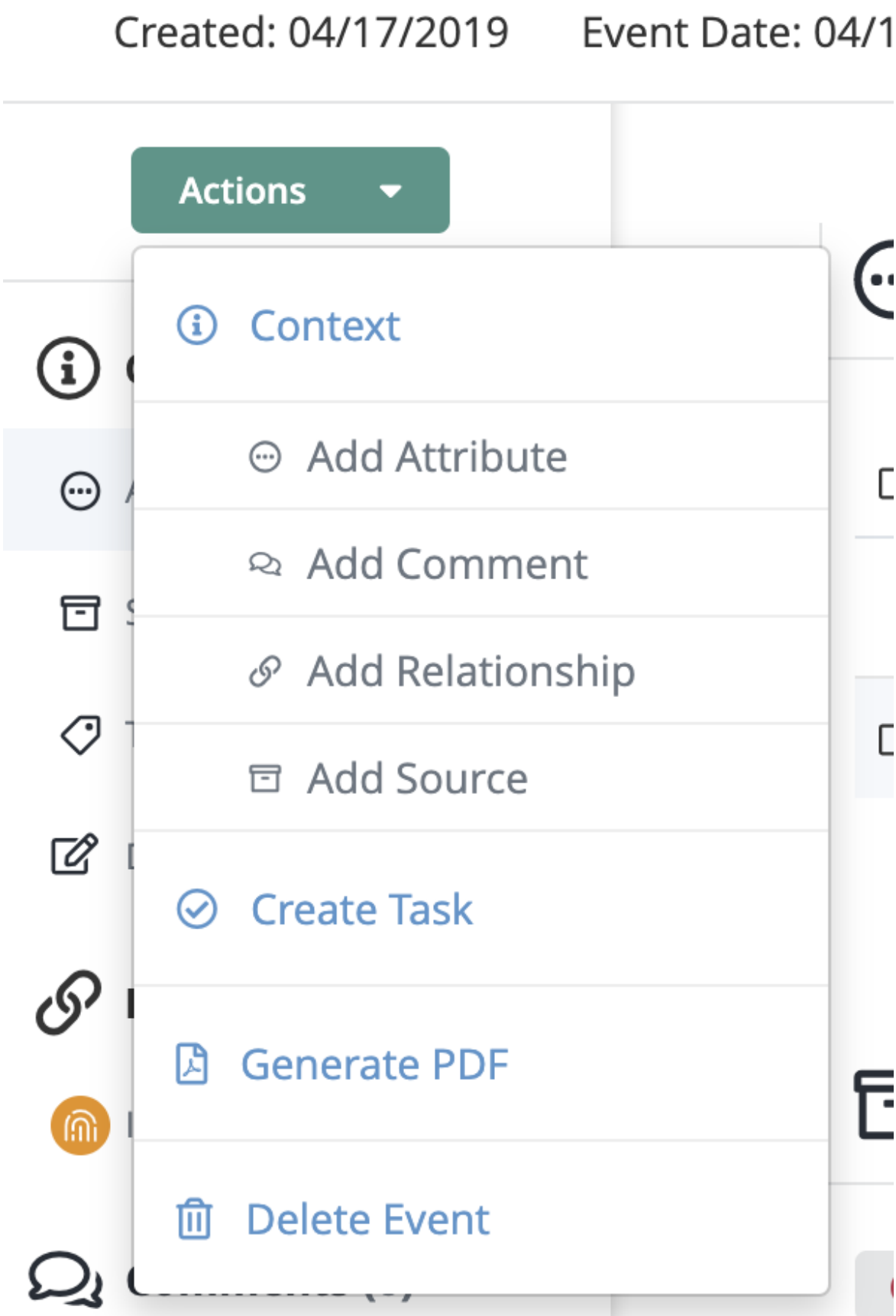
To delete an Event:

1. Locate and click the event.

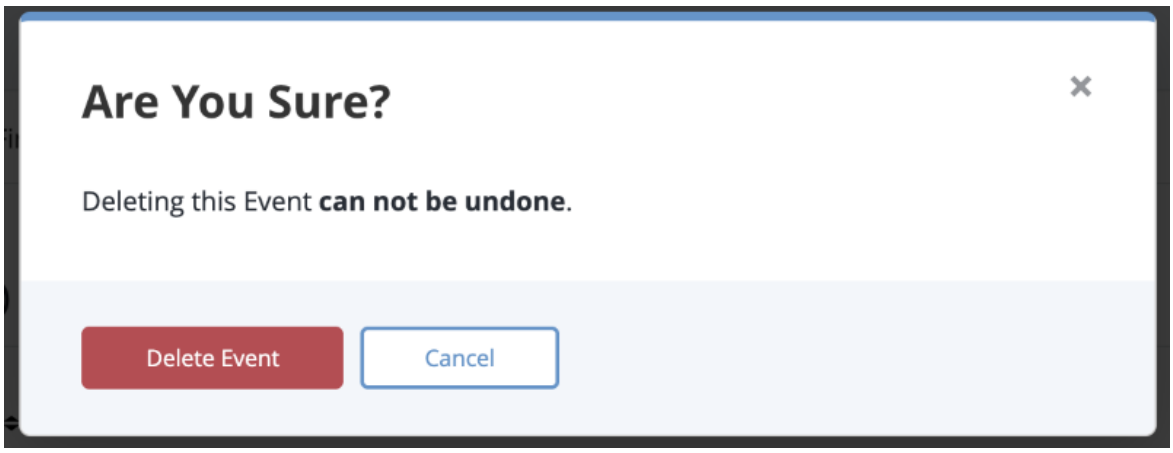
   The Events Details page opens.


THREATQ
Threat Library
Help Desk DoS Attack
Edit
EVENT: DOS ATTACK
Created: 04/17/2019
Event Date: 04/17/2019 10:38am
Actions
Context
Attributes (1)
Sources (2)
Attributes (1)
ATTRIBUTE TYPE
Start typing...

2. Click on the **Actions** menu and select **Delete Event**.


Created: 04/17/2019
Event Date: 04/1
Actions
Context
Add Attribute
Add Comment
Add Relationship
Add Source
Create Task
Generate PDF
Delete Event

A confirmation dialog box appears.



3. Click on **Delete Event**.

Files

Files are received from various intelligence providers and contain information on indicators, adversaries, and events within ThreatQ.

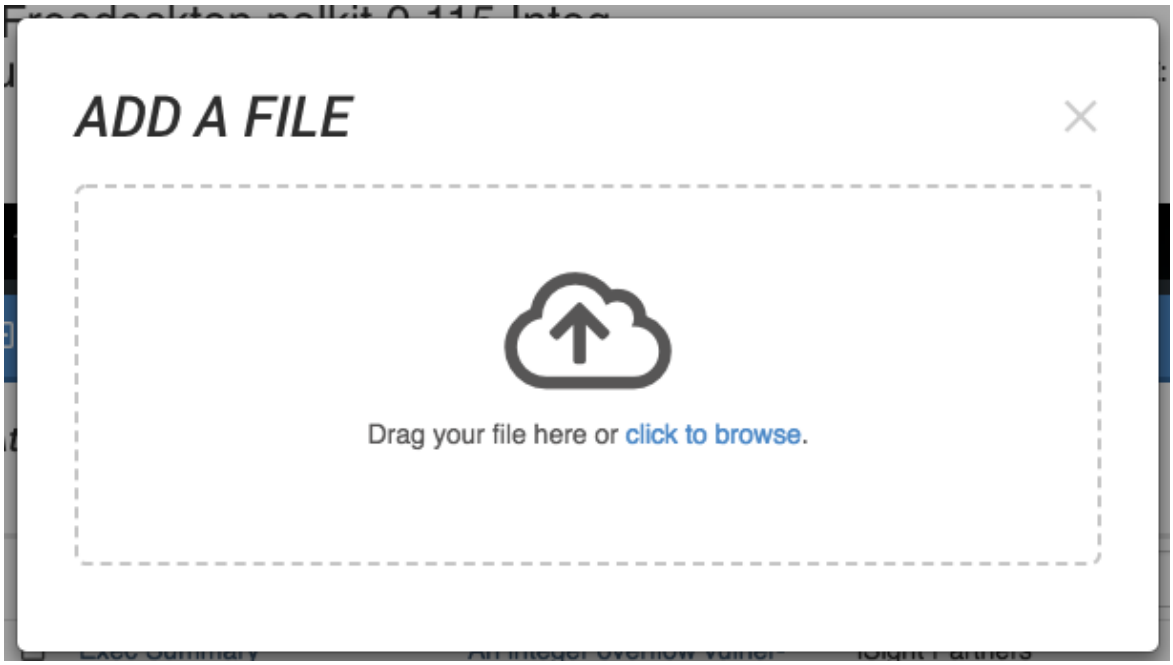
Related Topics:

- Adding Files
- Editing Files
- Deleting Files

Adding Files

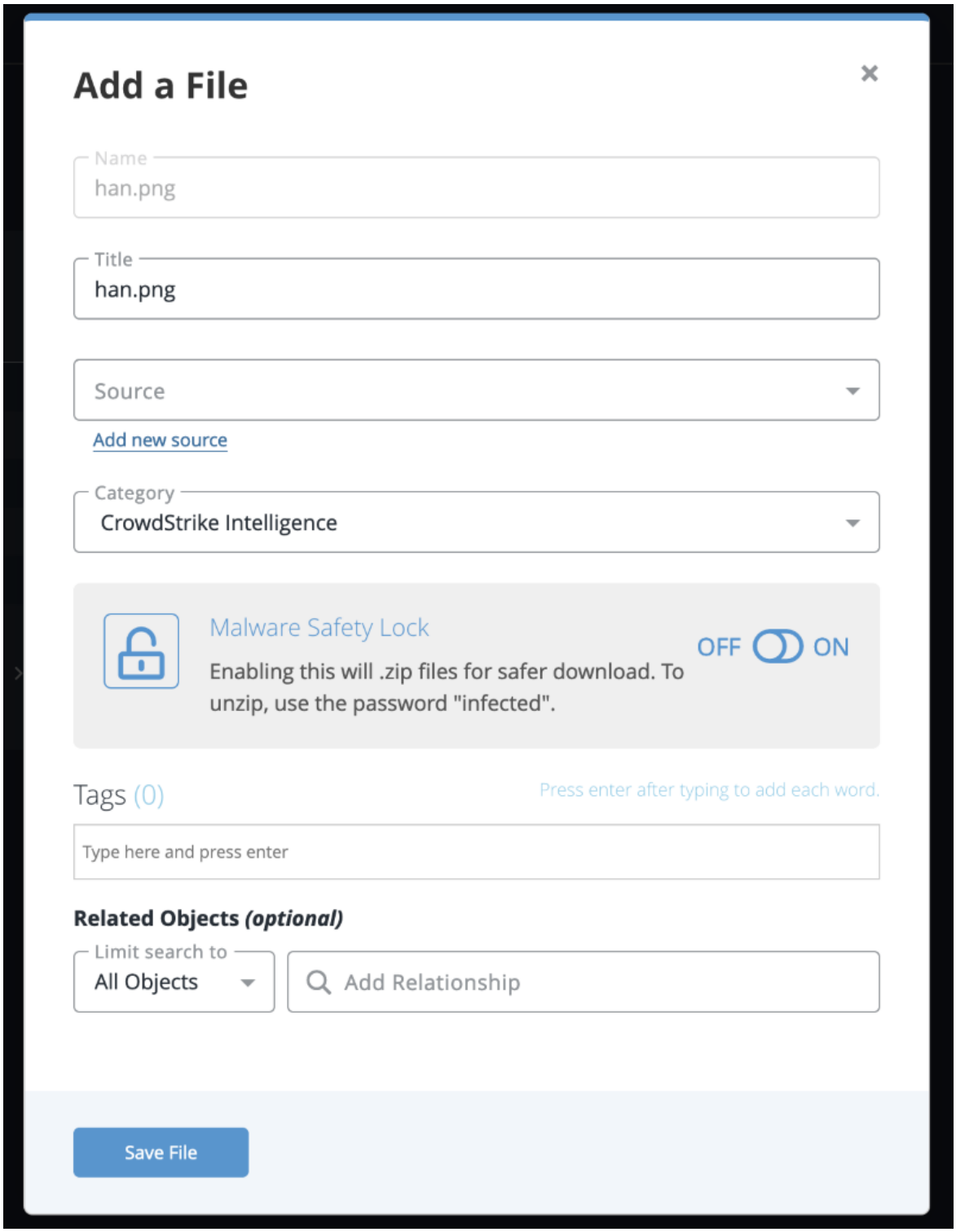
To add a File:

1. Click **Create New > File**.
   The Add a File dialog box opens.


ADD A FILE
Drag your file here or click to browse.

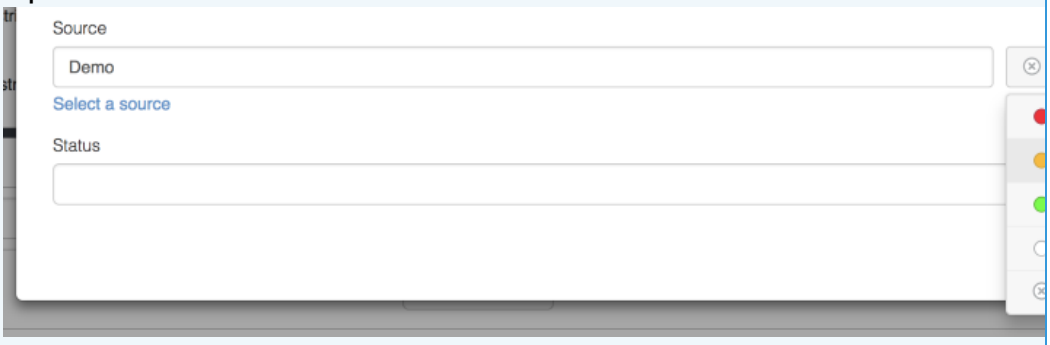
2. Drag the file into the dialog box or browse and locate the file.

   The Add a File Dialog box will update.



3. Update the **Title** if desired.
4. Select a **Source** from the dropdown list provided.

You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP designation light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



5. Select a **Category**.
6. Select whether to have the **Malware Safety Lock** on or off.

Enabling the safety lock will create a password-protected .zip file so any malware is safer for download. The system default password is "**infected**."

7. Add any desired tags.

Tags added appear on the File Details page.

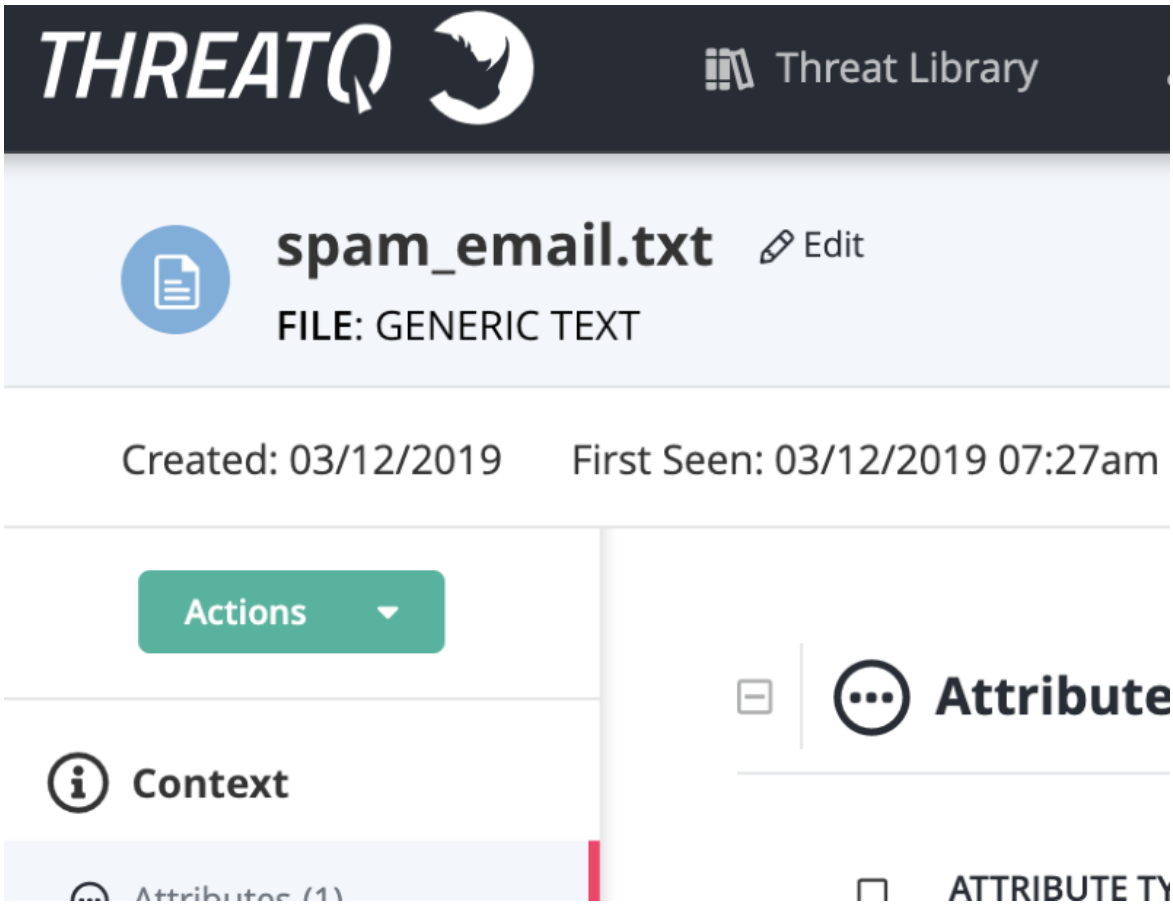
8. Select any **Related Objects** you need to link to the file. This field is optional.
9. Click **Save File**.

Editing Files

To edit a File Name:

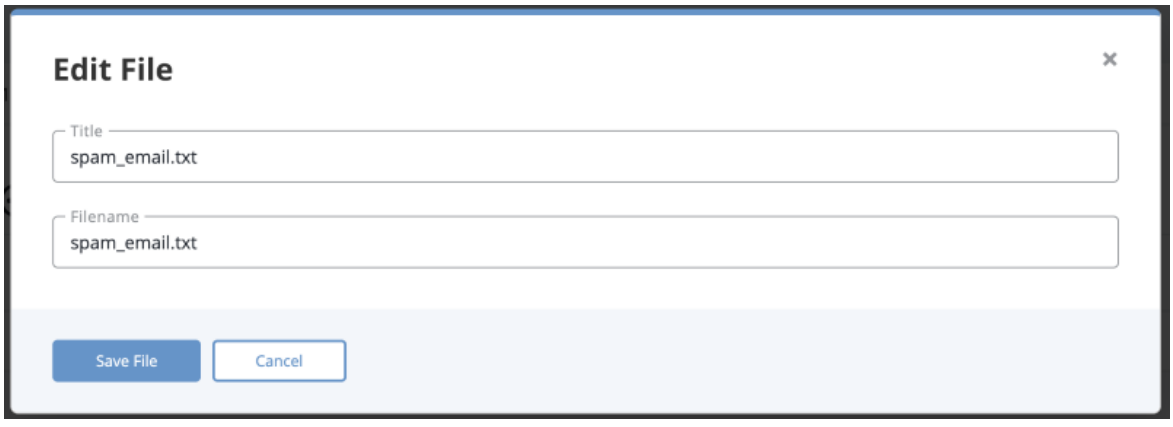
1. Locate and click on the file.

   The File Details page opens.



2. Click on **Edit** next to the File name.

   The Edit File dialog box opens.



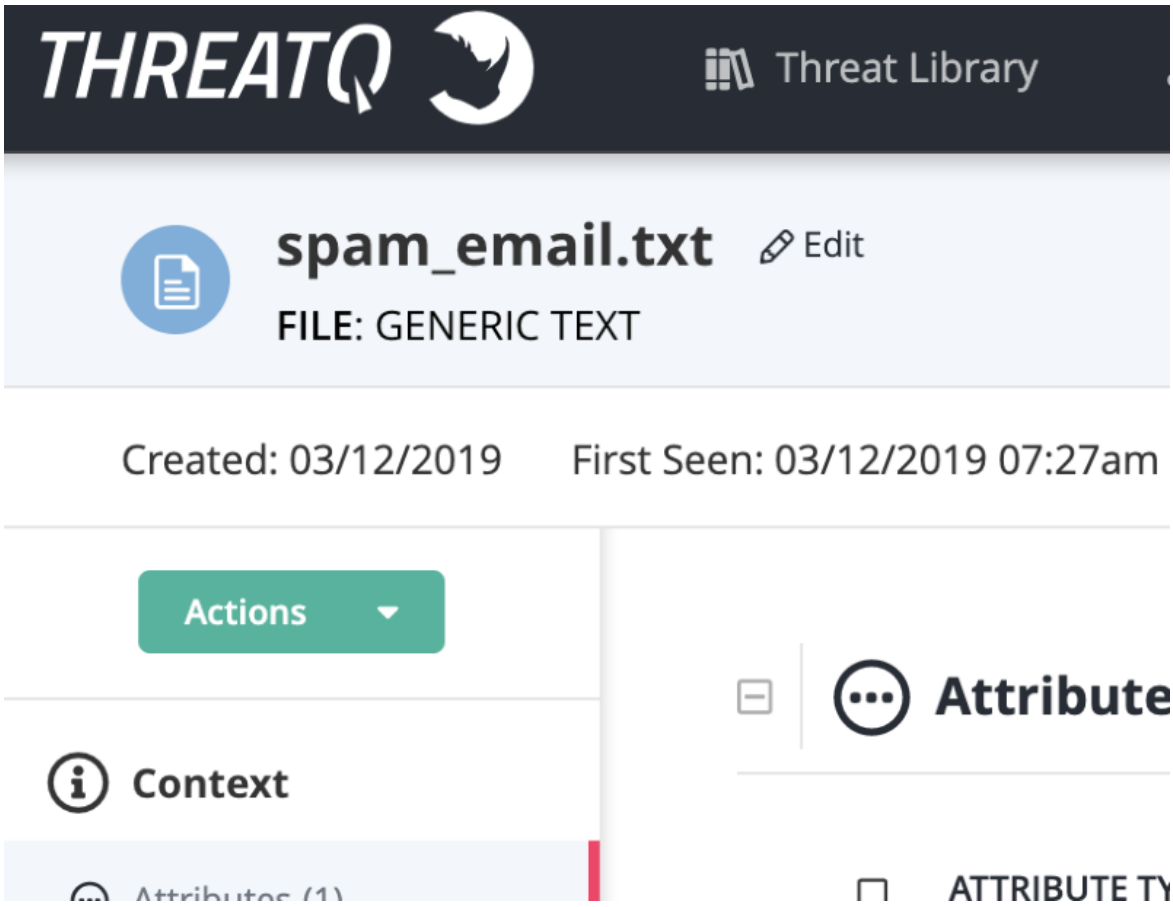
3. Make the desired change to the File Name.

4. Click on **Save File**.

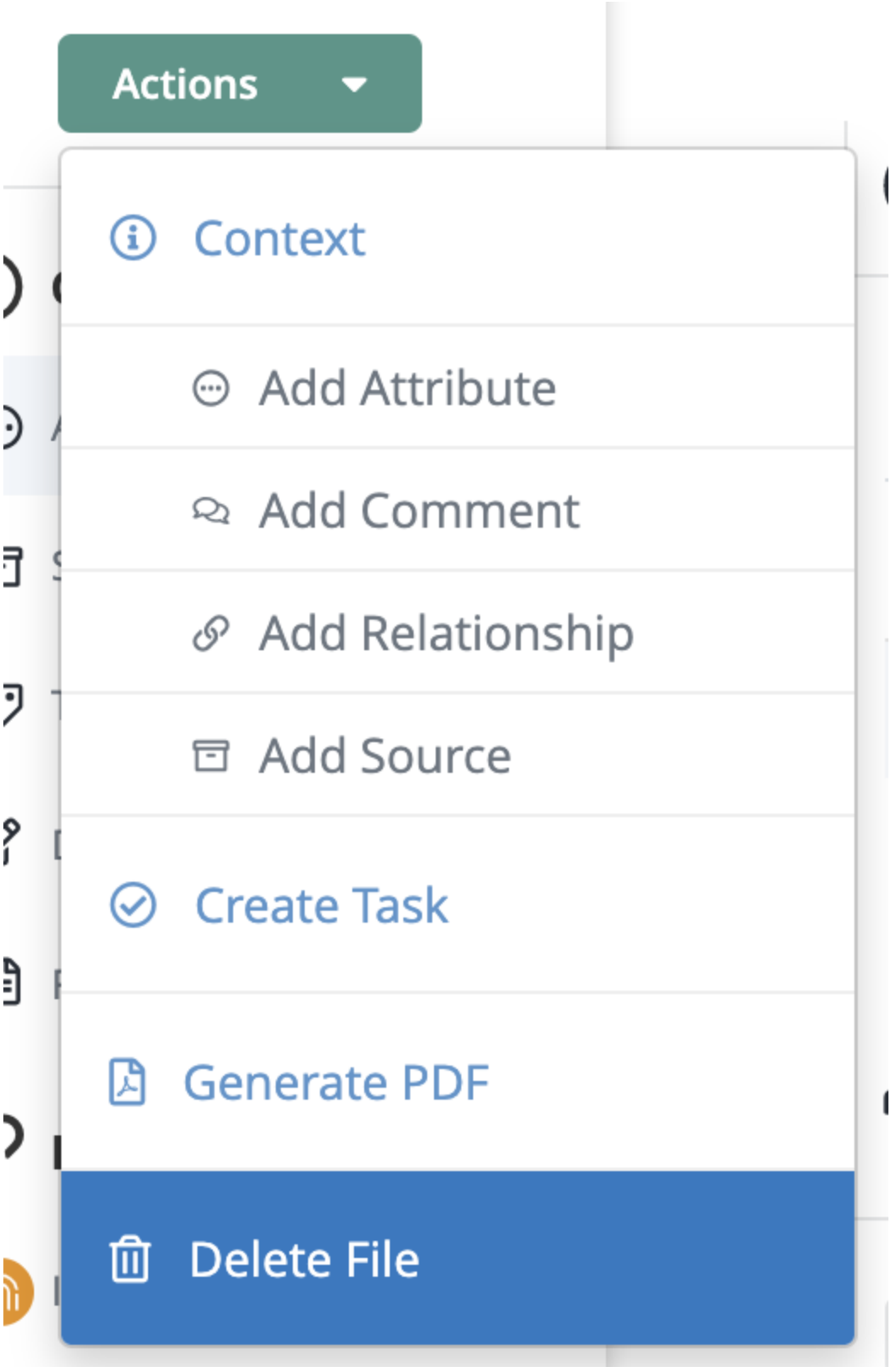
Deleting Files

To delete a File:

1. Locate and click the file.
   The File Details page opens.


THREATQ
Threat Library
spam_email.txt
Edit
FILE: GENERIC TEXT
Created: 03/12/2019
First Seen: 03/12/2019 07:27am
Actions
Context
Attribute

2. Click on **Actions** menu and select **Delete File**.



A confirmation dialog box appears.

3. Click on **Delete File**.

Indicators

Indicators are the so called "finger prints" associated with a malicious attempt or adversary group.

Indicators can be scored to allow you to apply weighting using contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. You can also set a manual score per indicator.

You can also apply expiration dates to an indicator to when it is determined to pose less of a threat to your infrastructure than other indicators.

Related Topics:

- Adding an Indicator
- Parsing for an Indicator
- Indicator Search
- Indicator Expiration
- Automatic Expiration and Policies
- Indicator Scoring

- Whitelisted Indicators
- Indicator URL Normalization

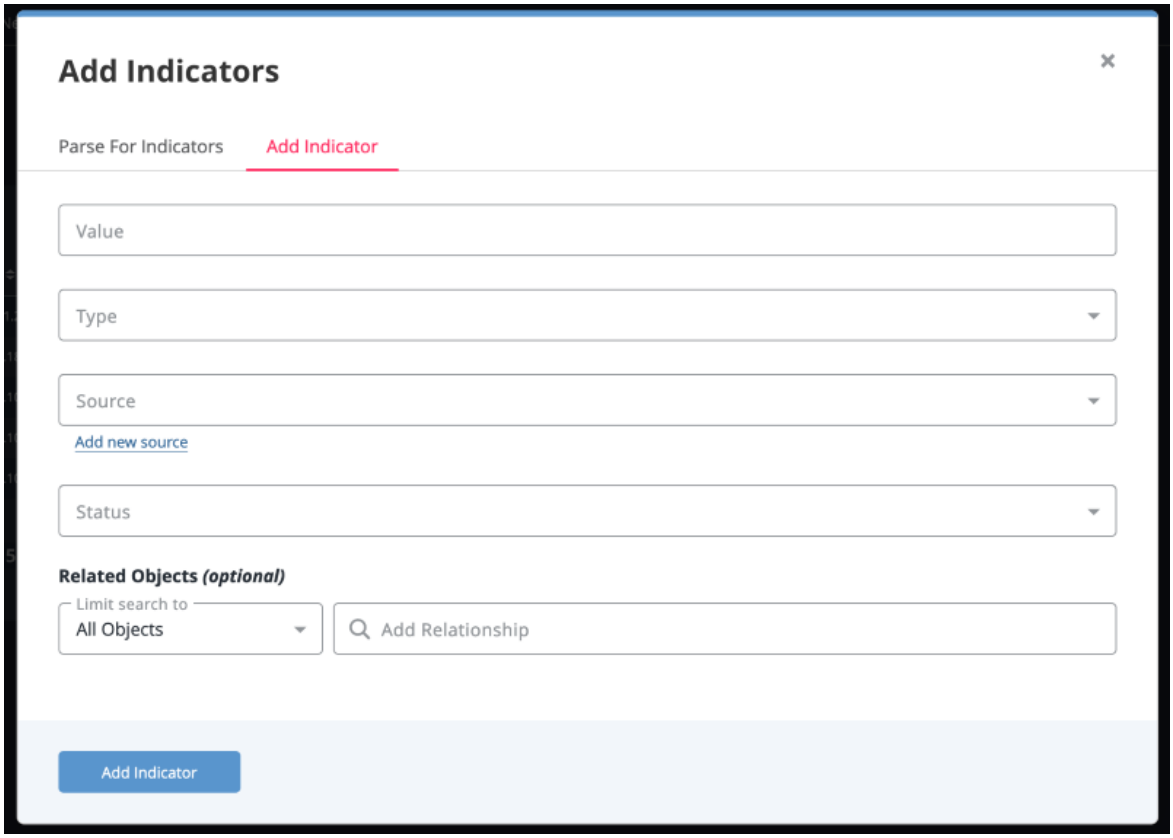
Adding an Indicator

To add an Indicator:

1. Click on **Create > Indicator**.

   You can also select **Indicator Parser** from the Create menu if importing a file. The option is located under the Import section of the Create menu. See the Parsing for an Indicator topic.

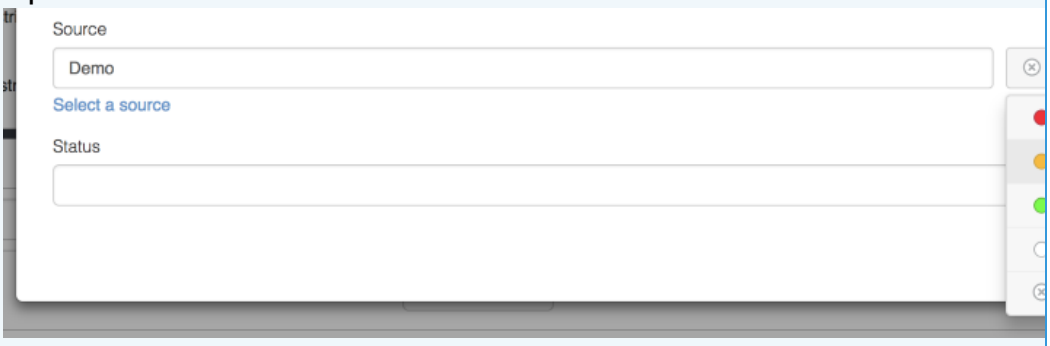
   The Add Indicators dialog box opens.



2. Enter a value in the **Value** field.
3. Select the **Type** of Indicator.

4. Select a **Source** from the provided dropdown list.

You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP designation light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



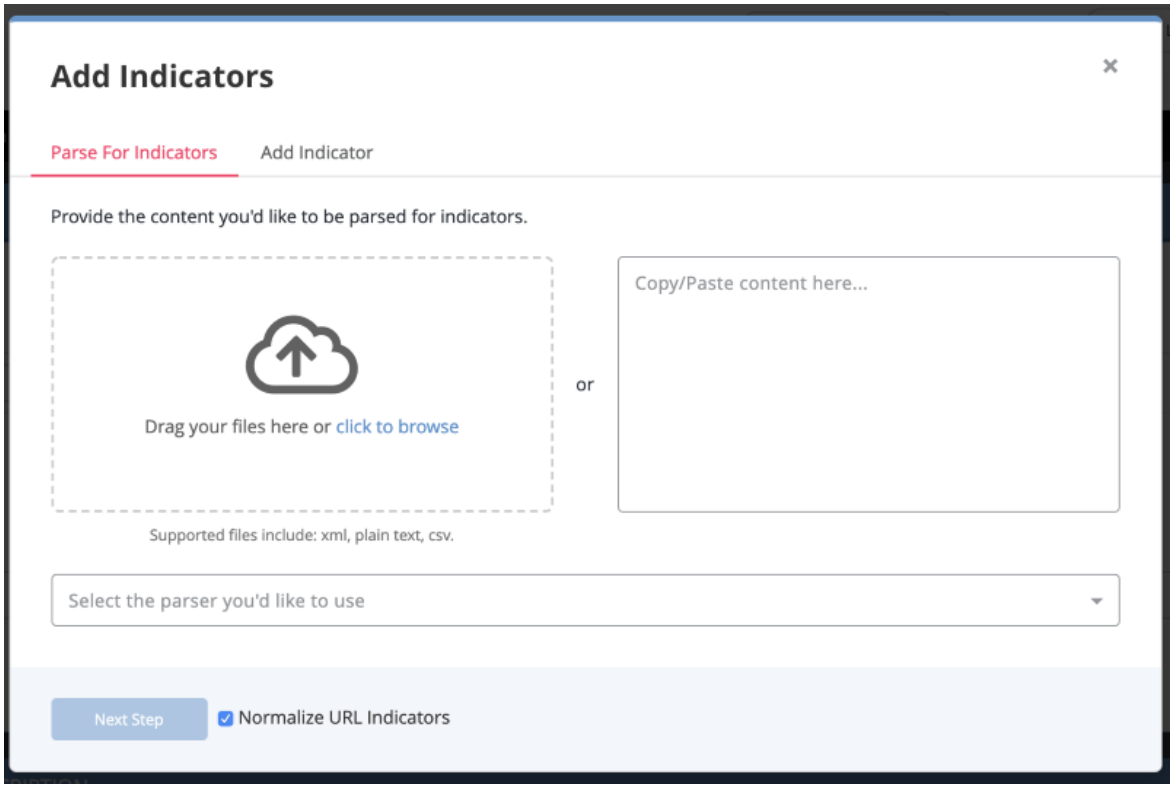
5. Select a **Status** for the indicator.
6. Select any **Related Objects** you need to link to the indicator. This field is optional.
7. Click **Add Indicator**.

Parsing for an Indicator

1. Click on the **Create** button, located at the top of the dashboard and select **Indicator Parser** under the *Import* heading.

You can also click on **Create** > **Indicator** and then select the **Parse for Indicators** option at the top of the **Add Indicators** modal.

The Add Indicators dialog box will load.



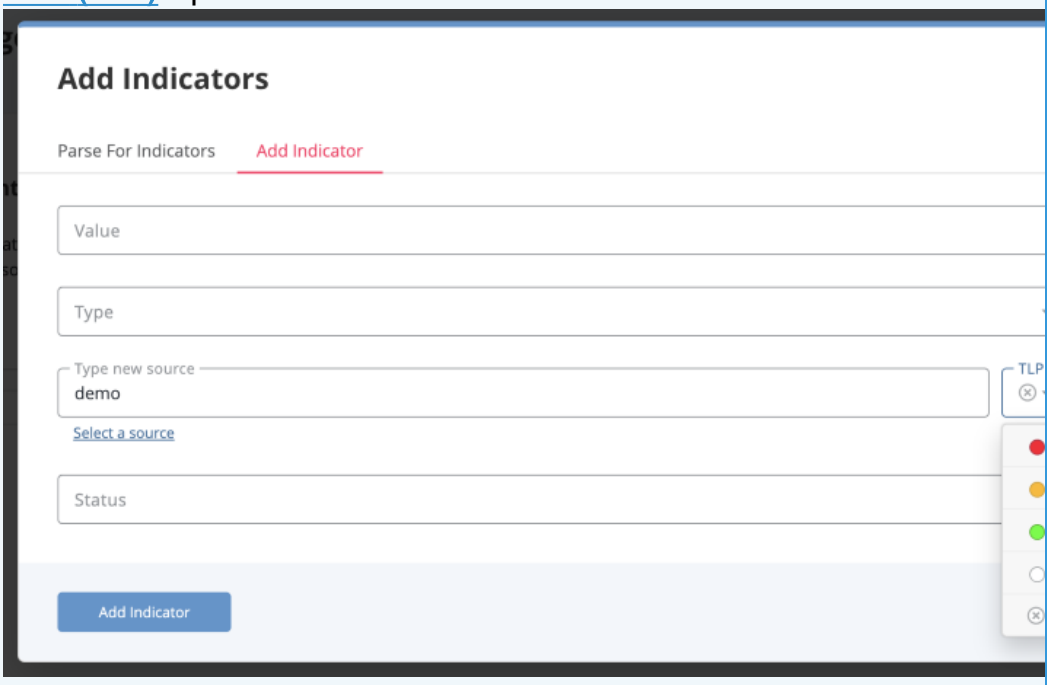
2. Do one of the following:
   - Drag your file(s) into the left pane.
   - Click on **Click to Browse**, and locate the file you wish to upload.
   - Copy/paste the content in the right pane.
3. Select the **Parser** to use and click on **Next Step**.
4. Select whether to save or delete the file after the import.

   Steps 5-7 pertain to saving the file. Skip to step 8 if you are not saving the file after import.

5. Update the **File Title** if needed.
6. Enter an optional **File Description**.

7. Confirm or update the **File Category**.
8. Select a **Source** from the dropdown menu provided.

Users can also click on **Add a New Source** if the desired source is not listed in the dropdown menu. If administrators have enabled TLP view settings, users can select a TLP classification light for the new source in the dropdown menu provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.



9. Select a **Status** to be applied to the extracted indicators.
10. Select any optional **Attributes** to be applied.
11. Click on **Next Step**.

If the file contains events that are detected, the Step 2: Review Events page opens. Indicators may be new or pre-existing. Pre-existing indicators are identified by a badge within the table. You can isolate new and pre-existing indicators by using the tabs at the top of the right hand panel.

12. Locate and select one or more indicators using one of the following options:

- From within the contents (on the left)
- From the table (on the right)
- By using the Select dropdown menu

13. Once you have selected one or more indicators, you can perform these functions:
    1. **Add Info** – Click the Add Info button to open the Add Info dialog box where you can perform the following functions:
        - Add Attributes to the indicator: add one or more attributes to the selected indicator(s). Once completed, click Add Attributes.
        - Link to Another Object: Link the selected indicator(s) to another object (indicator, event, adversary, file) and click Link Object.
        - Set Status: Select a status and click Set Status.
    2. **Edit** the type or status of an indicator by clicking its type or status in the table and selecting an option from the dropdown menu.
    3. **Add Indicator** - If you notice an indicator on the left that was not extracted, you can add it by clicking Add Indicator and completing the process.
    4. If you want to search within the table, use the fields at the top of the columns.

If at any point, you wish to abandon the import, click **x ABANDON THIS IMPORT**.

15. Click on **Finish Import**.

CSV File Format - Parsing

When importing a .csv file to parse for indicators using the ThreatQ CSV File Parser, the .csv file **must** meet the following criteria:

- The file must be comma-delimited.
- The file must include **at least** the following columns:
  - Indicator
  - Type: This column cannot contain types that are not already established in ThreatQ. You cannot add custom indicator types and indicator types are case sensitive. Choose from the following:
    - CIDR Block
    - CVE
    - Email Address
    - Email Attachment
    - Email Subject
    - File Path
    - Filename
    - FQDN
    - Fuzzy Hash
    - GOST Hash
    - IP Address
    - MD5
    - Mutex
    - Password
    - Registry Key
    - SHA-1
    - SHA-256
    - SHA-384
    - SHA-512

- String
- URL
- URL Path
- User-agent
- Username
- X-Mailer

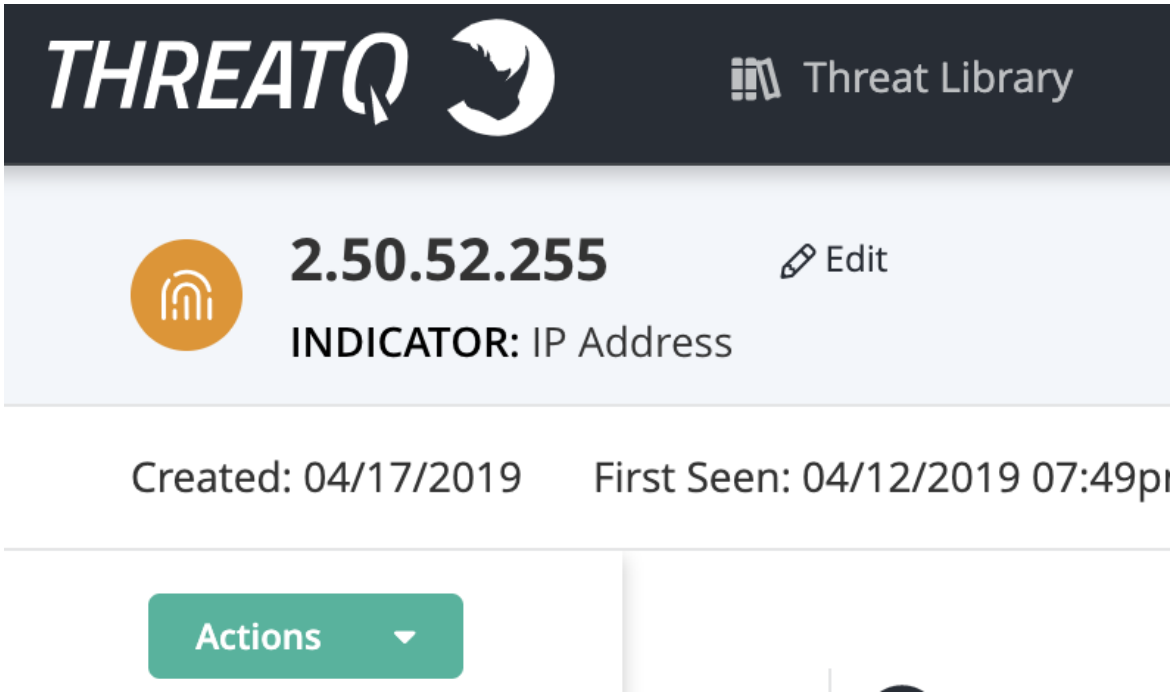
◦ Status

If the file is not properly delimited, missing a required column, or containing a valid type, it will fail upon upload.

Editing Indicators

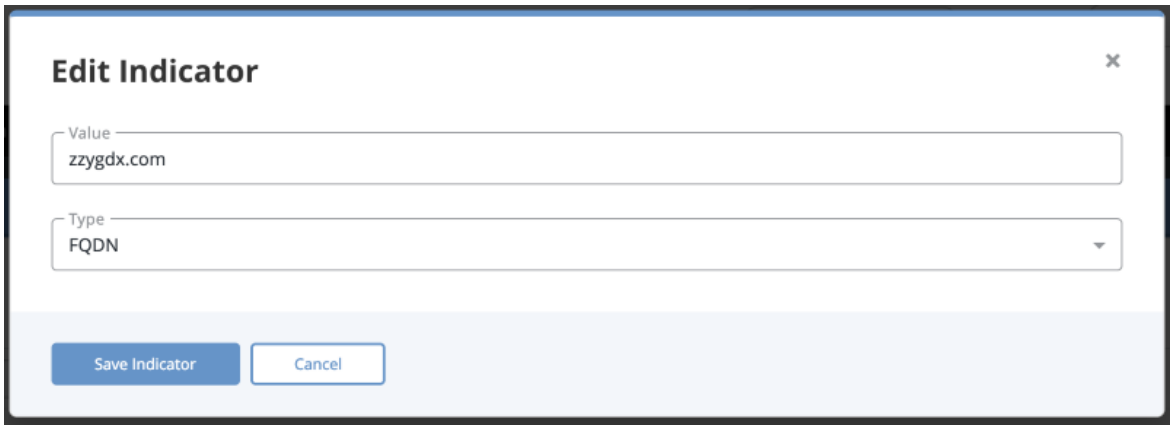
To edit an Indicator:

1. Locate and click on the indicator.
   The Indicator Details page opens.



2. Click on **Edit** next to the Indicator name.

   The Edit Indicator dialog box opens.



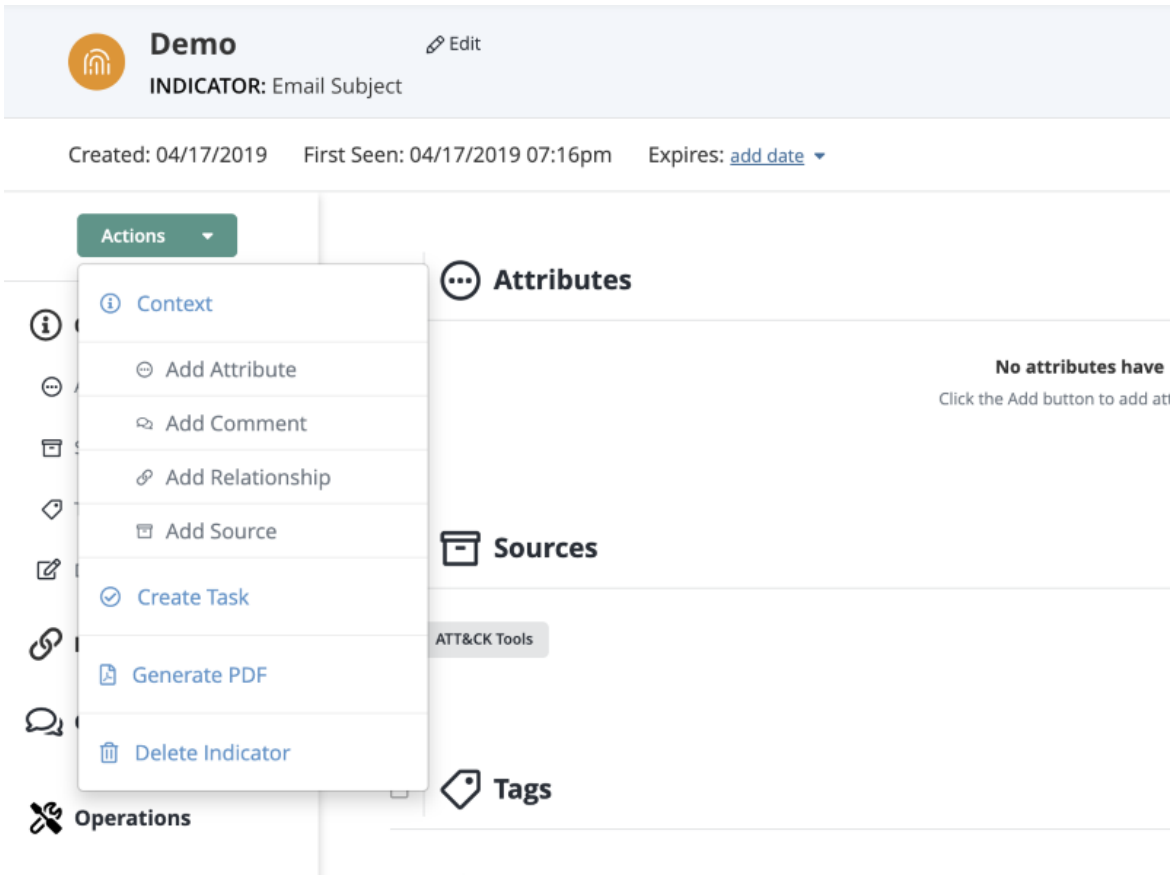
3. Make the desired change to the indicator **Value** and **Type**.
4. Click on **Save Indicator**.

Deleting Indicators

To delete an Indicator:

1. Locate and click on the Indicator.

   The Indicator Details page opens.



2. Click on **Delete this Indicator** located to the top right of the page.

   A confirmation dialog box appears.

3. Click on **Delete Indicator**.

Indicator Search

The Indicator Search will be deprecated in near the future. See the Legacy Indicator Search Deprecation topic for further details.

Indicator Search allows you to search indicators based on a wide range of modifiers and search criteria. For example, when searching for an event, the results will include all indicators related to that event.

Using indicator search will provide the total number of indicators matching the criteria of your search, however, the page will only load 1,000 indicators within the results table.

With respect to searching for IP Address or CIDR Block indicators, your results will be as follows:

- If searching for an IP Address, CIDR blocks will be returned if they fall within the range.
- If searching for CIDR blocks, IP addresses will be returned if they fall within the range.

This will search indicator values as well as Attribute of type “IP Address” (for instance, if an IP address is associated to another IP address through a passive DNS relationship).

Legacy Indicator Search Deprecation

This notice is to communicate the planned deprecation of the legacy indicator search feature within ThreatQ.

Background

Over the past several months, we have been investing in significant enhancements to the newer Threat Library search. This newer search provides improved performance and

functionality over the legacy Indicator Search and is the foundational search tool we will be building on top of moving forward. Among other capabilities, it allows users to search across any object type, apply bulk actions to results sets greater than one thousand records, and select many more output columns.

Additionally, removal of the Indicator Search and consolidation of backend components will enable further significant performance and functionality improvements to the Threat Library and other ThreatQ components.

Timeline

ThreatQuotient plans to remove Indicator Search from ThreatQ by End of Summer 2020.

Requested Actions

If you are currently using the Indicator Search for User Interface workflows or Integrations **OR if you are unsure** please take the following steps:

- Review the impacted components section below for more details about the scope of the changes
- Transition any known workflows or integrations that use indicator search to utilize the Threat Library search instead - see the Indicator Search to Threat Library Advance Search Migration Examples section and accompanying video below.

Run the following commands in the ThreatQ CLI if you are unsure if the custom integrations that you are running use Indicator Search. This does not apply to customers using a **ThreatQuotient Hosted instance**. ThreatQuotient hosted customers should contact support.

1. Run the following commands in the ThreatQ CLI:

```
/opt/threatq/python/bin/pip freeze
pip freeze
grep -r "/api/search/advanced"
```

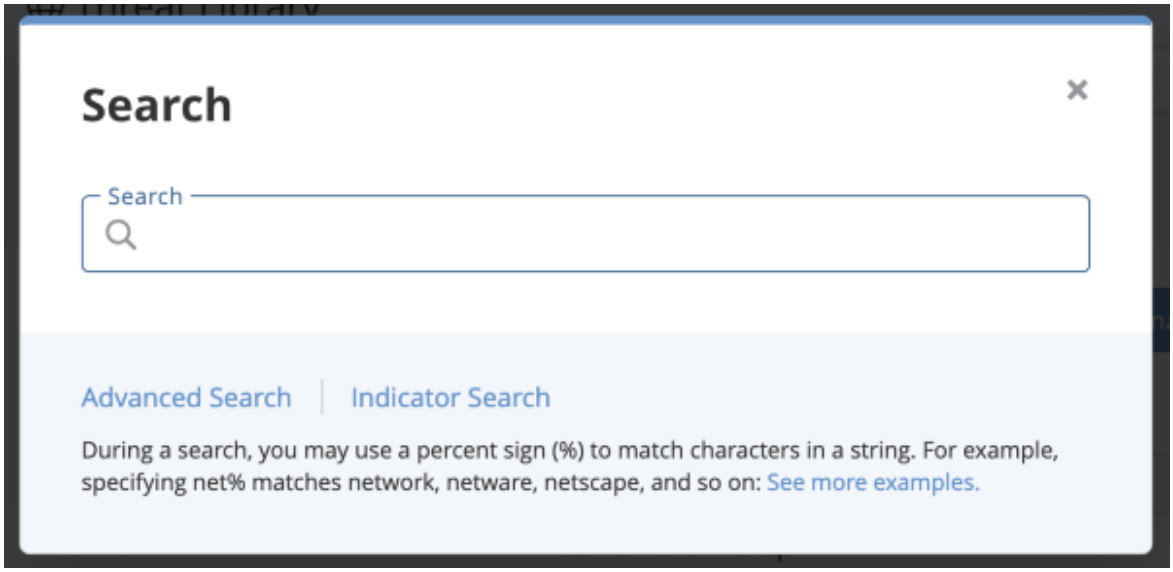
```
/var/log/httpd/access_log* | grep -v
'Chrome\|Mozilla' | wc -l
```

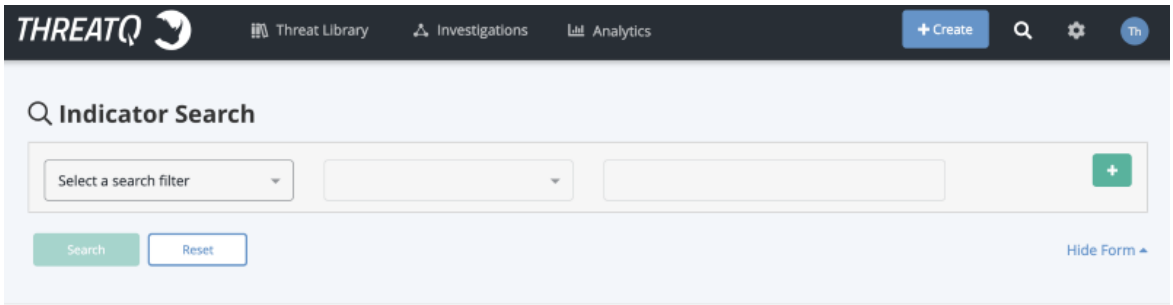
2. Email the results to support@threatq.com using the following subject: **Indicator Search Migration**.

> Contact support@threatq.com if you have any questions or require assistance with these actions.

Impacted Components

Legacy Indicator Search Page (UI)





- The Indicator Search page (UI) is accessed by selecting the magnifying glass in the top navigation bar in ThreatQ and then selecting the Indicator Search link at the bottom left of the Search dialog box.
- Following deprecation, the Indicator Search page and any backend components will be removed from the ThreatQ platform.
- Any Saved Searches that are being used in the Indicator search will no longer be available when the page is removed. ThreatQuotient recommends migrating those saved searches to the Threat Library saved search feature to avoid impact when Indicator Search is removed from the product.

All functionality available in Indicator Search is or will soon be available in the Threat Library search.

Platform links to the Indicator Search Page (UI)

- Previously there were several pages within ThreatQ that linked directly to search results in the Indicator search. For example, selecting an attribute key from a details page or selecting a total indicator count in the Indicator Status configuration page. All of these links have been or will shortly be updated to direct to equivalent results in the newer Threat Library. There should be no impact to associated workflows.

Integrations using Indicator Search Saved Searches

Indicator search contains a feature that allows for saving search parameters. These saved searches can be used in custom integrations developed by ThreatQ or your team. These integrations could be custom connectors or operations.

- For integrations developed and maintained by ThreatQuotient we have migrated those integrations to use the newer Threat Library and therefore they will not be impacted by removal of the Indicator Search.

- For integrations that your team has built and/or maintains, they must be updated to utilize Threat Library saved searches. Integrations that use Indicator Search saved searches will no longer function when the Indicator Search is removed.

FAQs

What is Impacted

Legacy Indicator Search and integrations that utilize saved searches created on that page. See the Impacted Components Section for more details.

Is the Indicator Search being removed in the next release?

No, the Indicator search will remain available and function as normal. We will provide additional follow-on notification with the confirmed release date and version associated with these changes.

Can I recreated the saved searches I have in the Indicator Search using saved searches in the Threat Library?

Yes. For any saved searches in the Indicator Search that you use regularly, we highly recommend migrating them and the associated workflows to the Threat Library as soon as possible. See the Advanced Search section for more details on filtering the Threat Library and saving searches.

Who should I contact if I have questions about impact to my current workflows and/or integrations?

Contact support@threatq.com if you have any questions or require assistance with your integrations or workflows.

What should I do if I am unable to migrate my integrations to use the Threat Library in time?

Please contact support@threatq.com and we will discuss migration options.

The Indicator Search functionality and related integrations will continue to function until you upgrade to the affected ThreatQ version (the actual date and release version will be communicated at a later date in a follow-on notification).

Does the Threat Library support all of the same search filter capabilities that are available in the Indicator Search?

Yes. The Threat Library has parity with Indicator Search filters as well as additional enhancements.

Does the Threat Library support all of the Bulk Actions available in the Indicator Search?

Yes. The Threat Library includes all bulk actions available in Indicator Search and also includes Bulk Add/Remove Tags, Bulk Add/Remove Attributes, bulk remove relationships. The Threat Library bulk action capability allows for updates to more than one thousand records, whereas the Indicator Search does not. Additionally, Threat Library bulk actions are tied to in-app status notifications and the Job Management page.

What do the commands in the Request Actions section of this topic do and how will ThreatQ support use the results?

This does not apply to customers using a **ThreatQuotient Hosted instance**. ThreatQuotient hosted customers should contact support.

The commands will provide us with a list of installed packages with their versions, on your ThreatQ system. We can then reference this list against the expected list of packages and identify those that might be utilizing indicator search. From there, we can follow up with you to determine if any further actions are required.

```
/opt/threatq/python/bin/pip freeze
```

Used for operation integrations

```
pip freeze
```

Used for custom connector integrations

```
grep -r "/api/search/advanced" /var/-
log/httpd/access_log* | grep -v 'Chrome\|Mozilla' |
wc -l
```

Used to pull logs for ID'ing any additional unknown integrations utilizing Indicator search

Indicator Search to Threat Library Advance Search Migration Examples

Source is AlienVault OTX and Date Created within 30 Days

Indicator Search Field Breakdown:

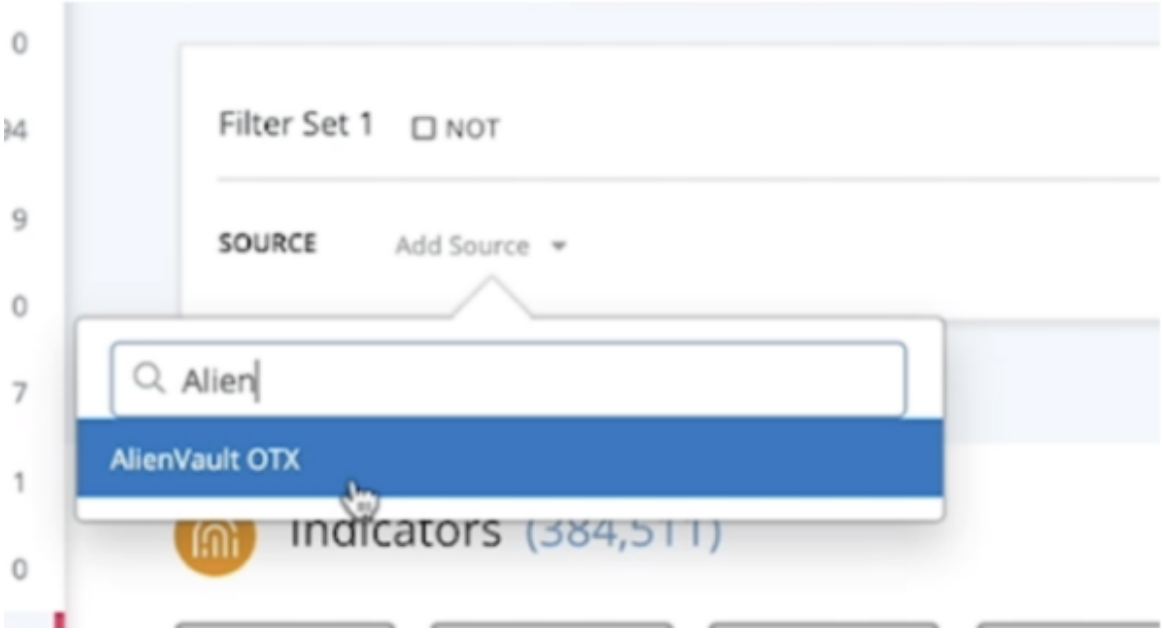
Filter	Operator	Entry
Source	Is	AlienVault OTX
Logical Operator	N/A	AND
Date Created	Is within the last	30 Days

In the Threat Library:

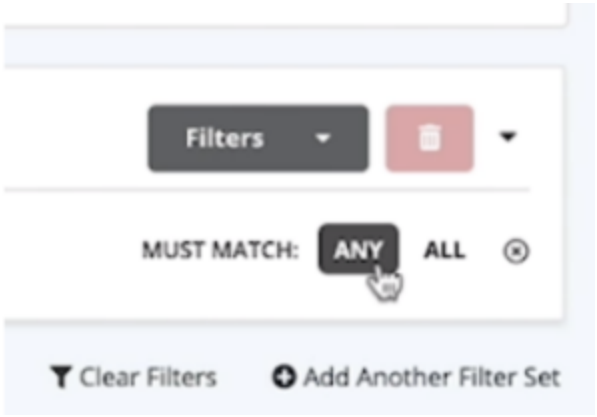
1. Click on the **Filters** dropdown for **Filter Set 1** and select **Source**.

   The Source filter appears in the filter set.

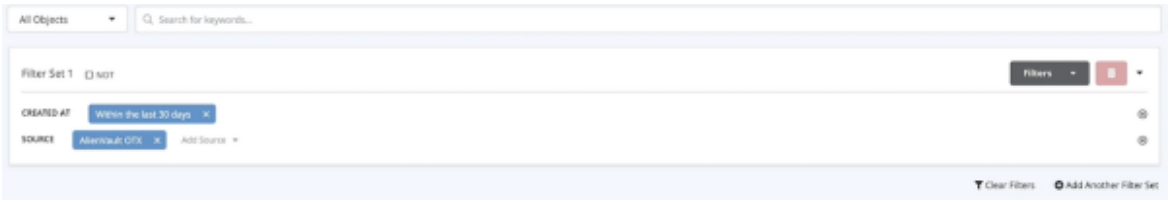
2. Click on **Add Source** and select **AlienVault OTX**.



3. Repeat Step 2 to add **DomainTools** and **VirusTotal**.
4. Confirm that the **Must Match** option, located to the right of the sources, is set to **Any**. This will cause to return results that have at least one of the Sources in the filter set.

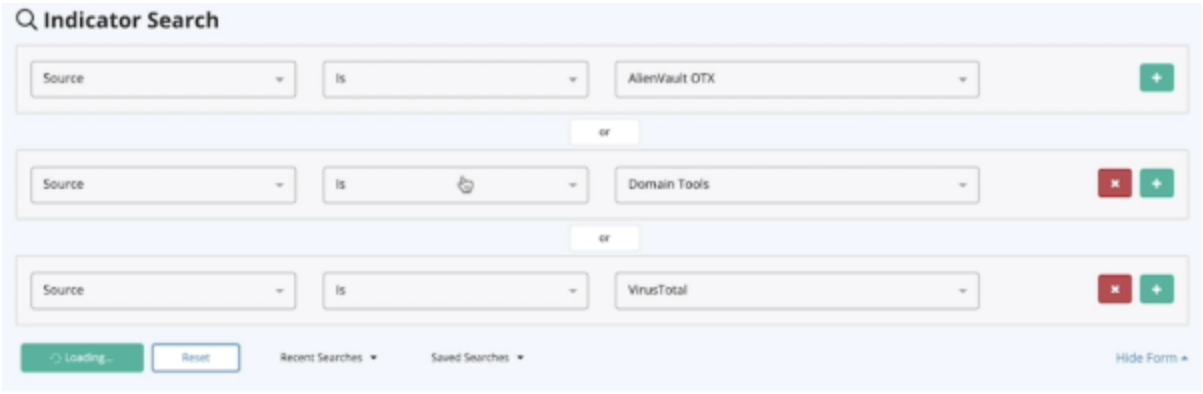


5. Save the search.



Source is AlienVault OTX or DomainTools or VirusTotal

Indicator Search Field Breakdown:



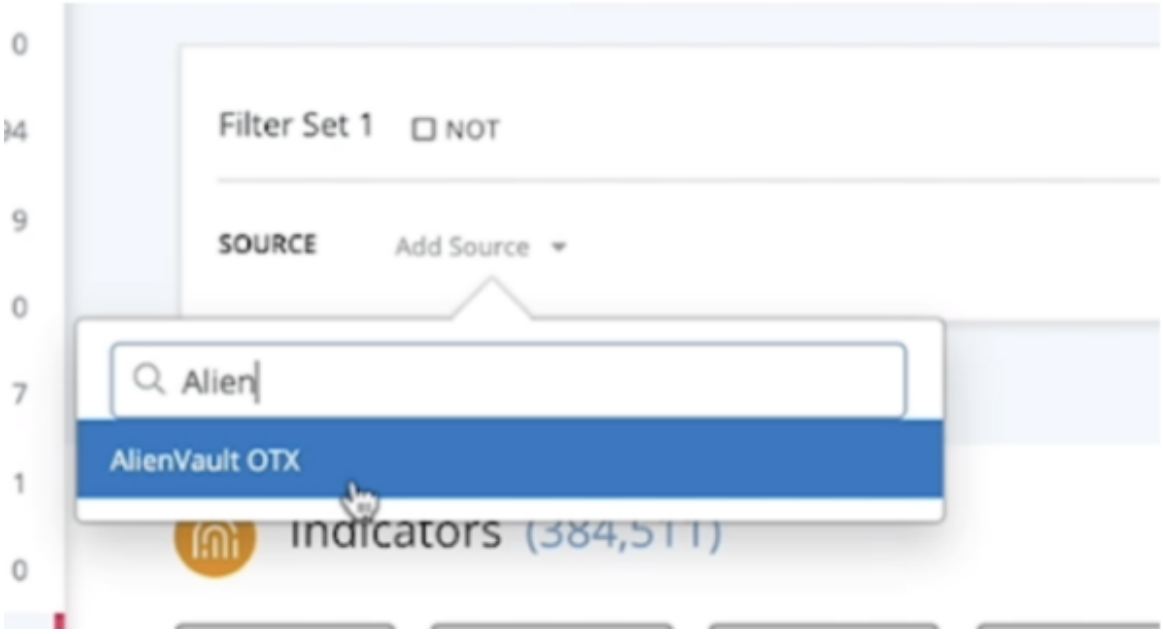
Filter	Operator	Entry
Source	Is	AlienVault OTX
Logical Operator	N/A	OR
Source	Is	DomainTools
Logical Operator	N/A	OR
Source	Is	VirusTotal

In the Threat Library:

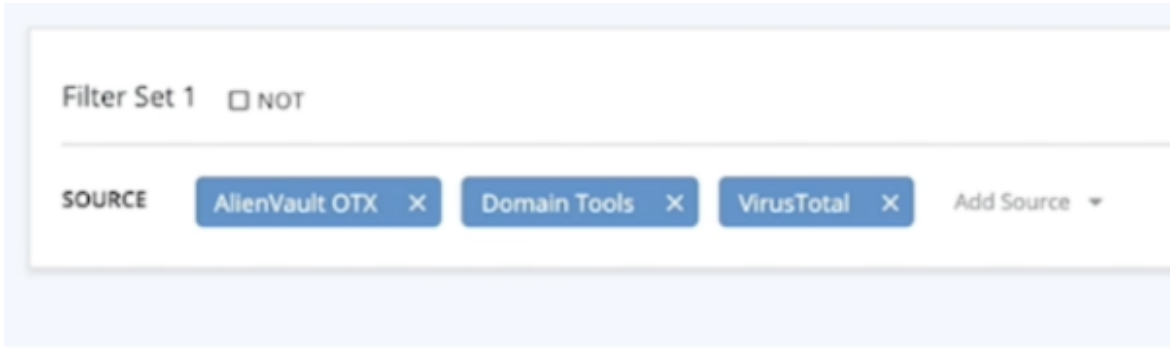
1. Click on the **Filters** dropdown for **Filter Set 1** and select **Source**.

   The Source filter appears in the filter set.

2. Click on **Add Source** and select **AlienVault OTX**.

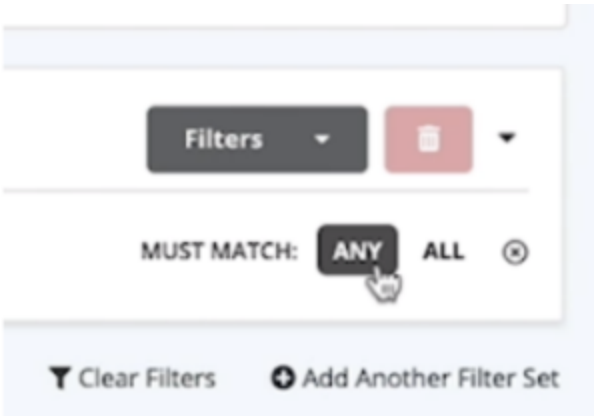


3. Repeat Step 2 to add **DomainTools** and **VirusTotal**.



4. Confirm that the **Must Match** option, located to the right of the sources, is set to **Any**. This will cause to return results that have at least one of the Sources in the fil-

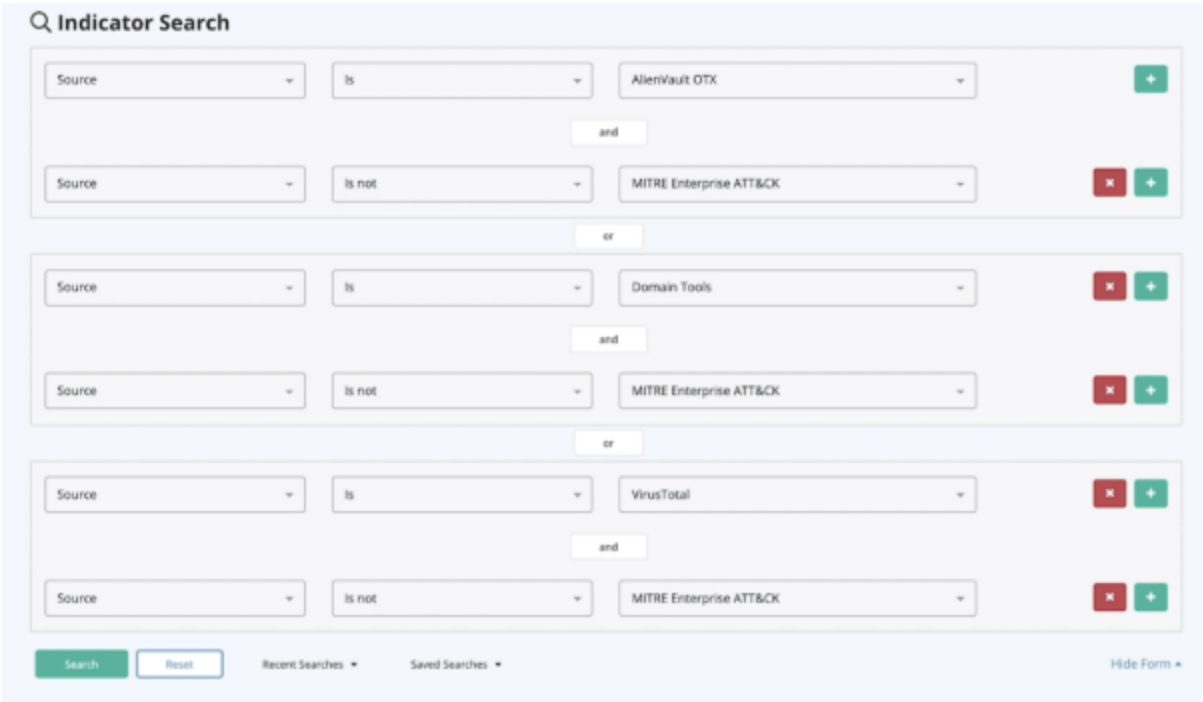
ter set.



5. Save the search.

Source is AlienVault OTX or DomainTools or VirusTotal but not MITRE Enterprise ATT@CK

Indicator Search Field Breakdown:



Filter	Operator	Entry
Source	Is	AlienVault OTX

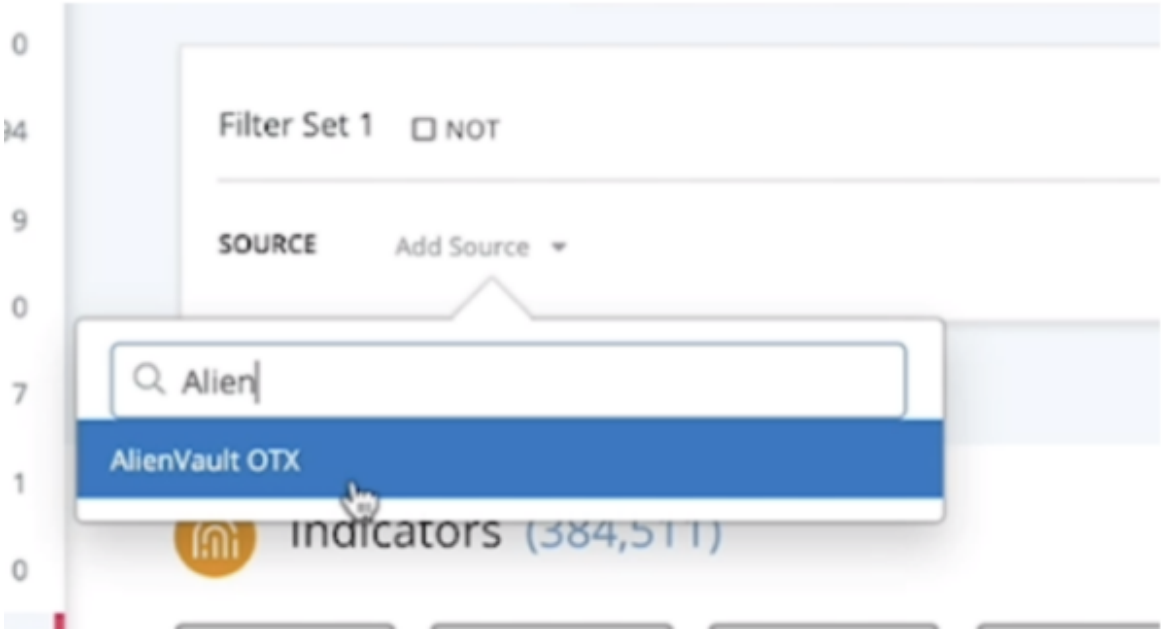
Filter	Operator	Entry
Logical Operator	N/A	AND
Source	Is not	MITRE Enterprise ATT@CK
Logical Operator	N/A	OR
Source	Is	DomainTools
Logical Operator	N/A	AND
Source	Is not	MITRE Enterprise ATT@CK
Logical Operator	N/A	OR
Source	Is	VirusTotal
Logical Operator	N/A	AND
Source	Is not	MITRE Enterprise ATT@CK

In the Threat Library:

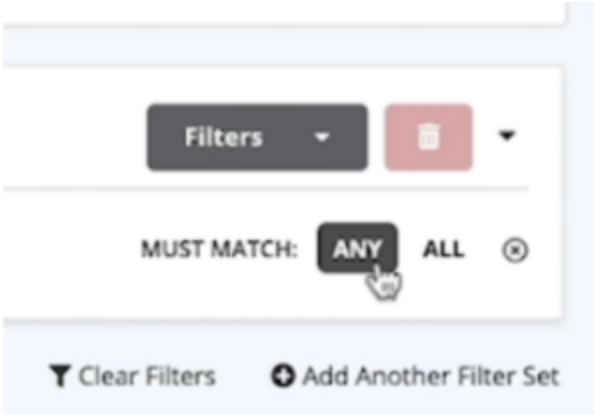
1. Click on the **Filters** dropdown for **Filter Set 1** and select **Source**.

   The Source filter appears in the filter set.

2. Click on **Add Source** and select **AlienVault OTX**.



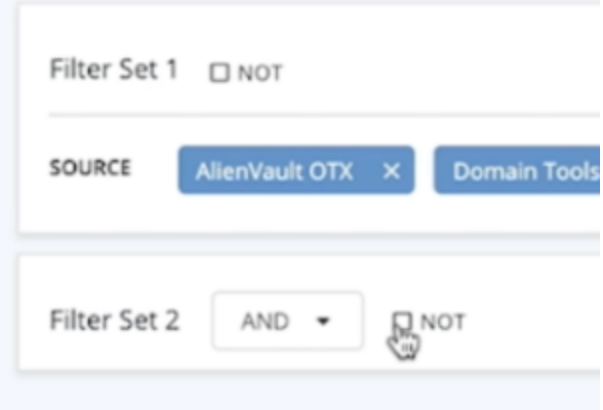
3. Repeat Step 2 to add **DomainTools** and **VirusTotal**.
4. Confirm that the **Must Match** option, located to the right of the sources, is set to **Any**. This will cause to return results that have at least one of the Sources in the filter set.



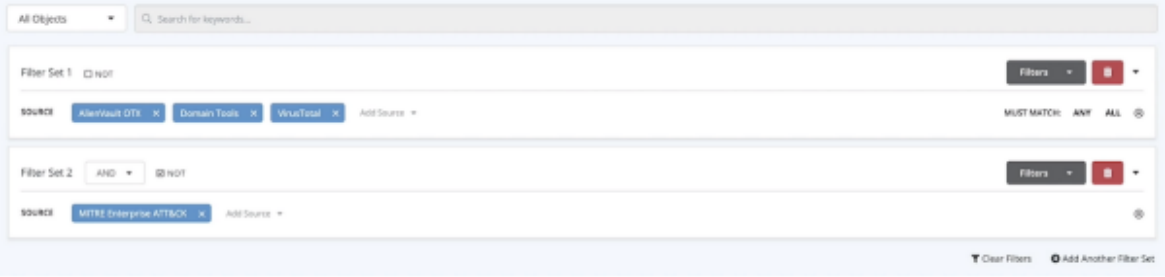
5. Click on **Add Another Filter Set** to create **Filter Set 2**.

6. Select **AND** as the filter set's logical operator.

7. Check the **Not** checkbox.



8. Click on the **Filters** dropdown for **Filter Set 2** and select **Source**.
9. Click on **Add Source** and select **MITRE Enterprise ATT@CK**.
10. Save the search.



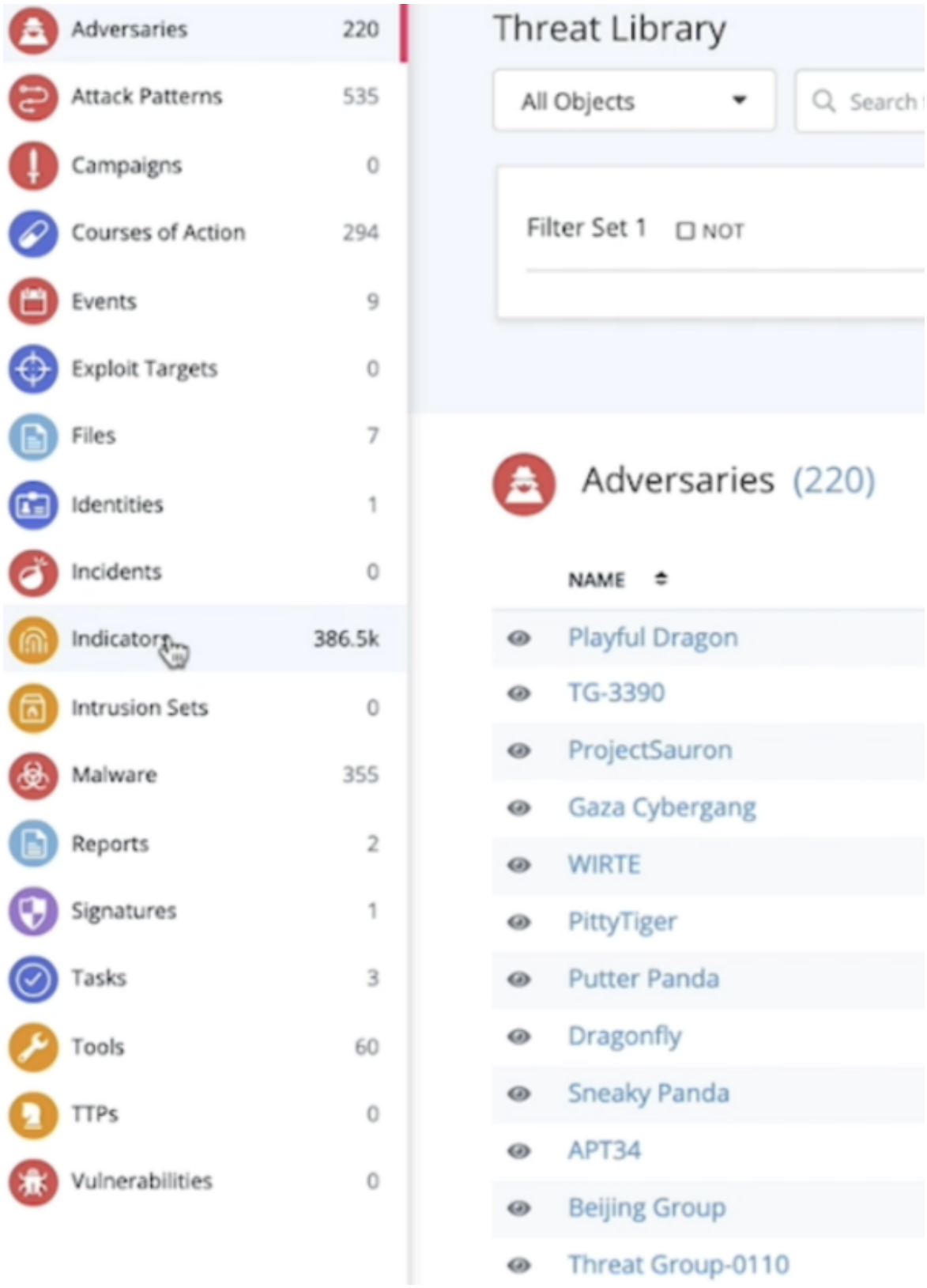
Indicator Type is FQDN and Score is 3 - 10

Indicator Search Field Breakdown:

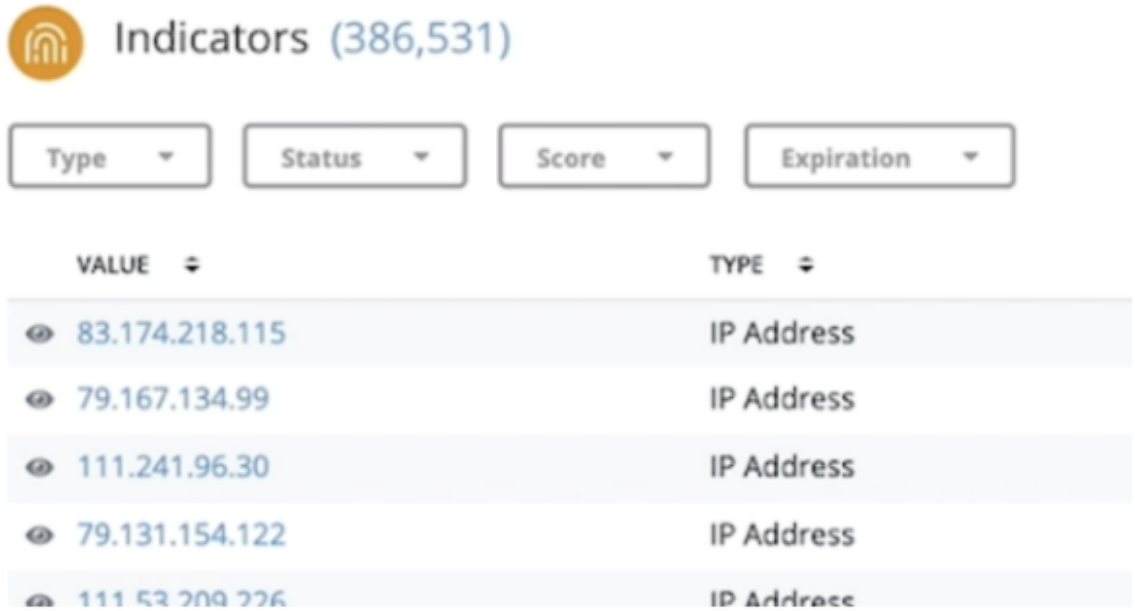
Filter	Operator	Entry
Type	Is	FQDN
Logical Operator	N/A	AND
Score	Is greater than or equal to	3

In the Threat Library:

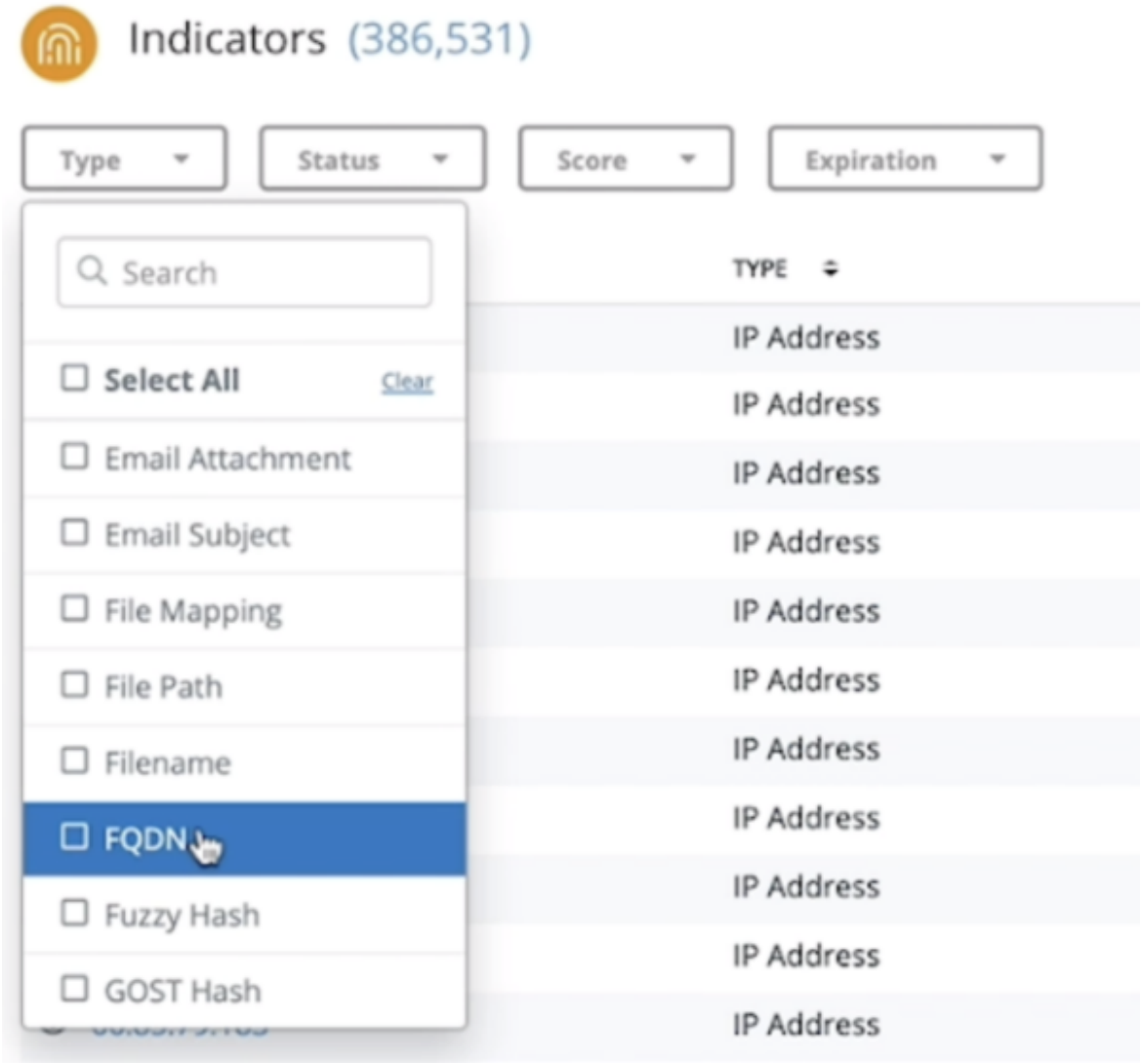
1. Click on the **Indicators** heading in the Threat Library's side menu. This will load the Indicators-only view on your page.


Adversaries 220
Attack Patterns 535
Campaigns 0
Courses of Action 294
Events 9
Exploit Targets 0
Files 7
Identities 1
Incidents 0
Indicators 386.5k
Intrusion Sets 0
Malware 355
Reports 2
Signatures 1
Tasks 3
Tools 60
TTPs 0
Vulnerabilities 0
Threat Library
All Objects
Search
Filter Set 1
NOT
Adversaries (220)
NAME
Playful Dragon
TG-3390
ProjectSauron
Gaza Cybergang
WIRTE
PittyTiger
Putter Panda
Dragonfly
Sneaky Panda
APT34
Beijing Group
Threat Group-0110

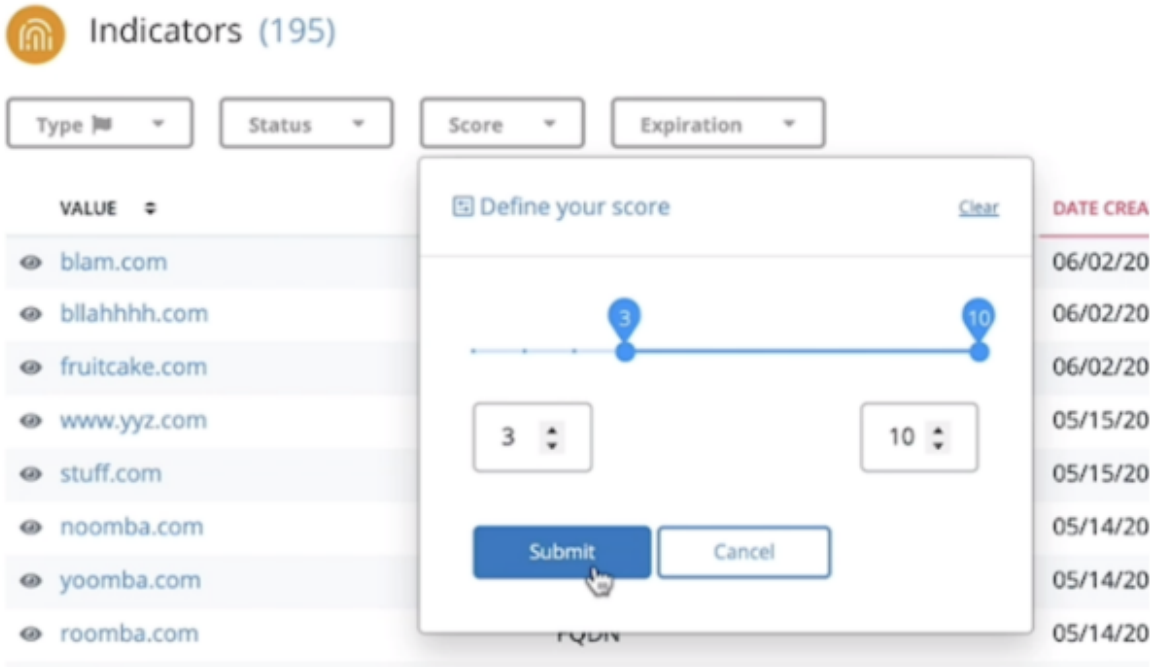
A set of dropdown filters will appear above the library results that are specific to indicators.



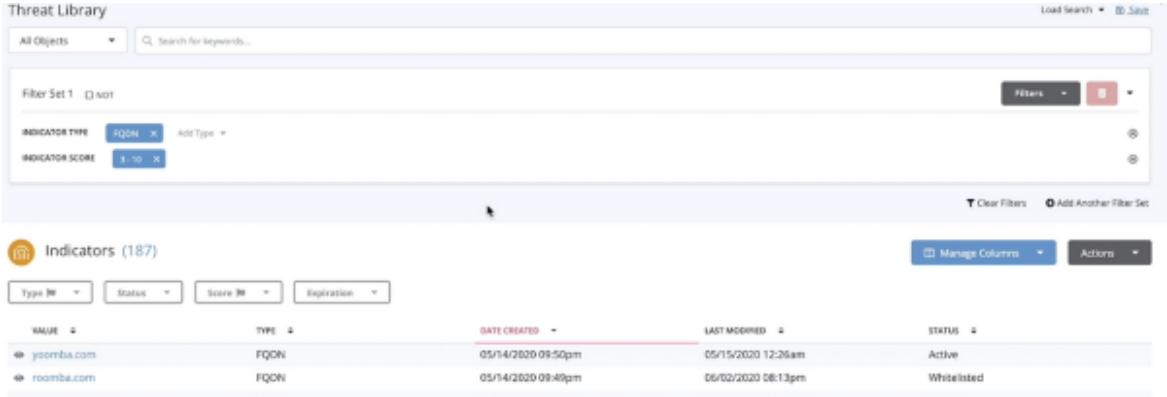
2. Click on the **Type** dropdown and select **FQDN**.



3. Click on the **Score** dropdown and use the slide to select **3 - 10**.

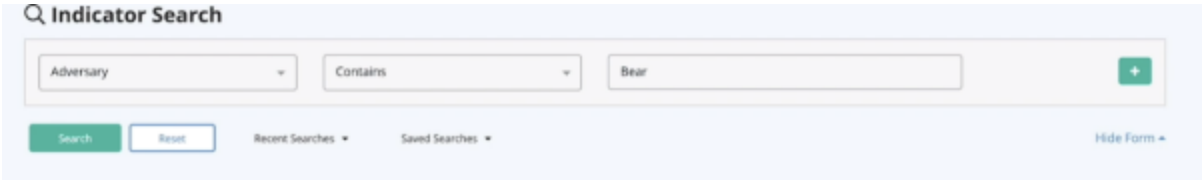


4. Save the search.



Adversary Contains Bear

Indicator Search Field Breakdown:



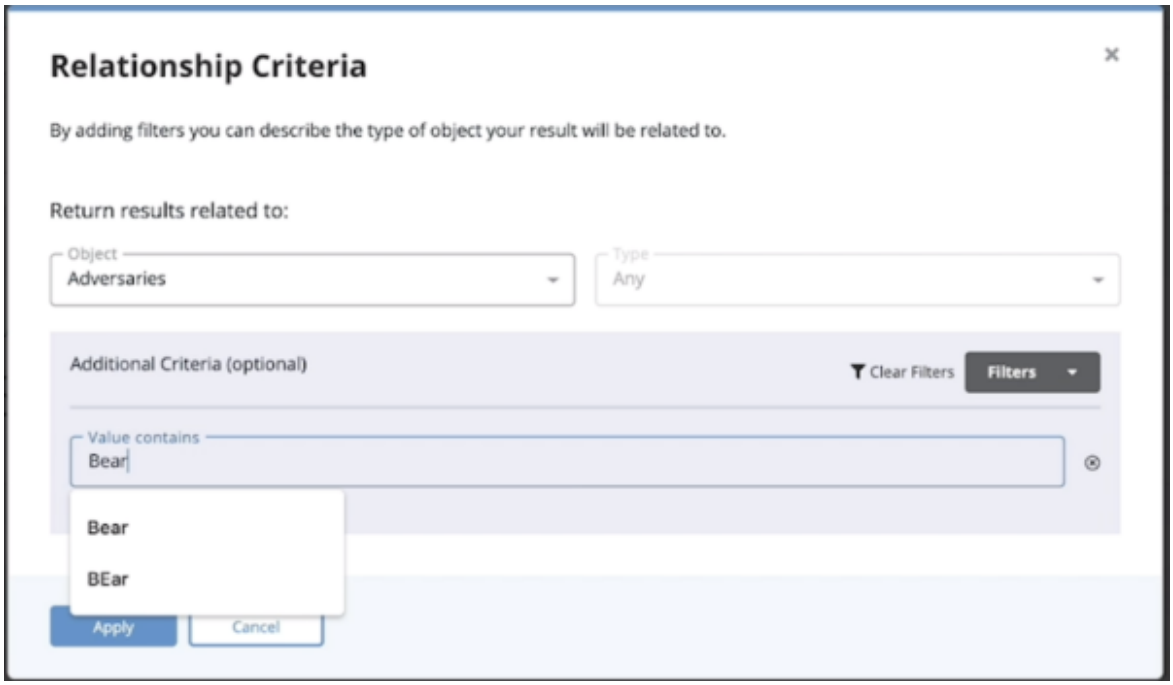
Filter	Operator	Entry
Adversary	Contains	Bear

In the Threat Library:

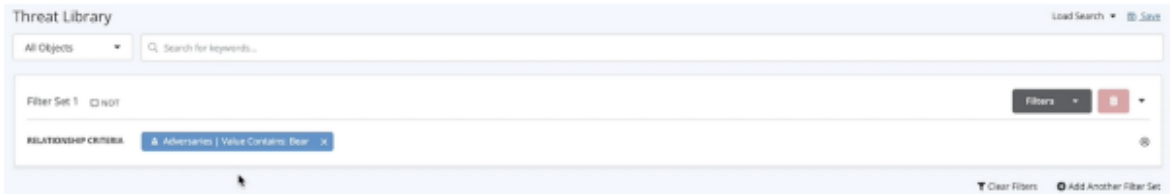
1. Click on the **Filters** dropdown for **Filter Set 1** and select **Relationship Criteria**.

   The Relationship Criteria dialog box opens.

2. Select **Adversaries** from the **Object** dropdown, select **Bear** from the **Value Contains** field, and click on **Apply**.



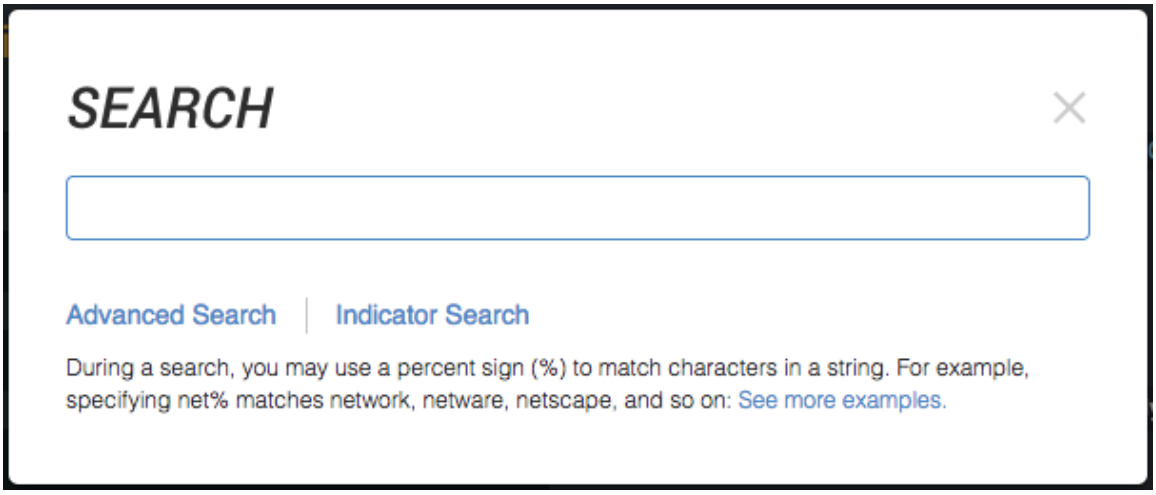
3. Save the search.



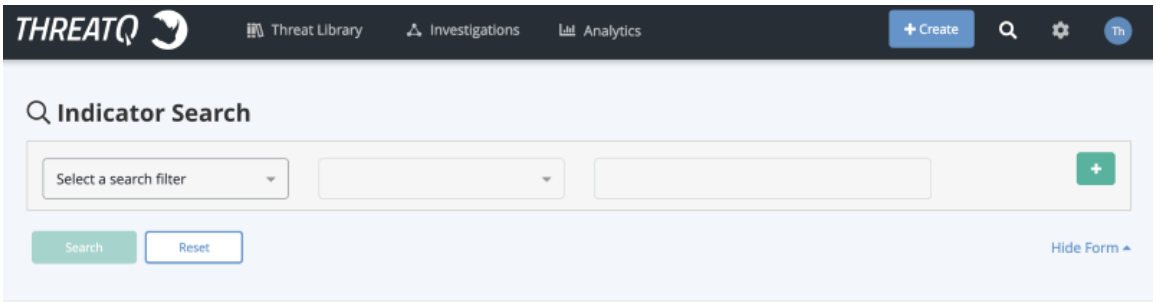
Performing an Indicator Search

To perform an Indicator Search:

1. From the main menu, click the **Search** icon.
   The Search dialog box appears.



2. Click **Indicator Search.**
   The Indicator Search page appears.



3. Select the desired search parameters and operators using the dropdowns, and enter the values.

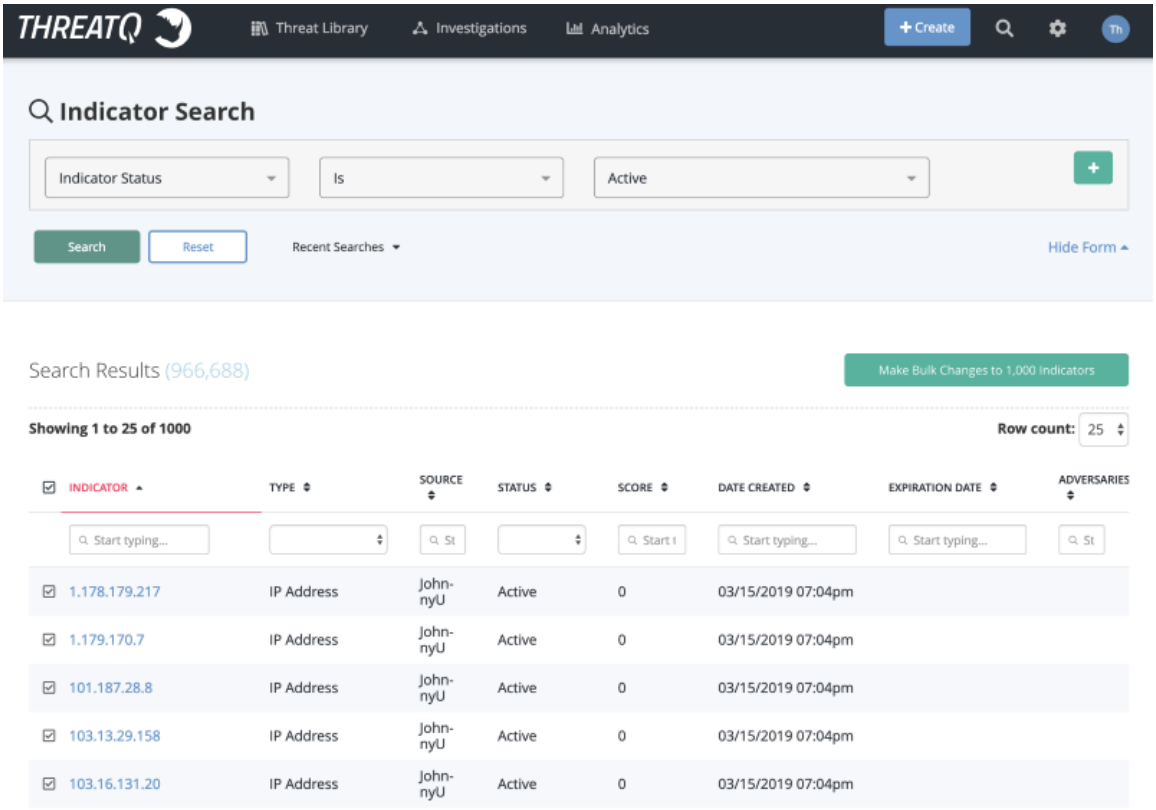
Parameter	Operator
Indicator Class	Is Is not Is Blank

Parameter	Operator
	Is Not Blank
Indicator Value	Contains Does Not Contain Is Is not Is Blank Is Not Blank
List of Indicators	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Indicator Status	Is Is not Is Blank Is Not Blank
Indicator Type	Is Is not Is Blank Is Not Blank
Date Created	Is Is not Is after Is before Is in the range of Is Blank Is Not Blank
Date Last Modified	Is Is not Is after Is before

Parameter	Operator
	Is in the range of Is Blank Is Not Blank
Attachment Title	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Adversary	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Event Title	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Event Type	Is Is not Is Blank Is Not Blank
Attribute	Contains Does Not Contain Is Is not Is Blank Is Not Blank

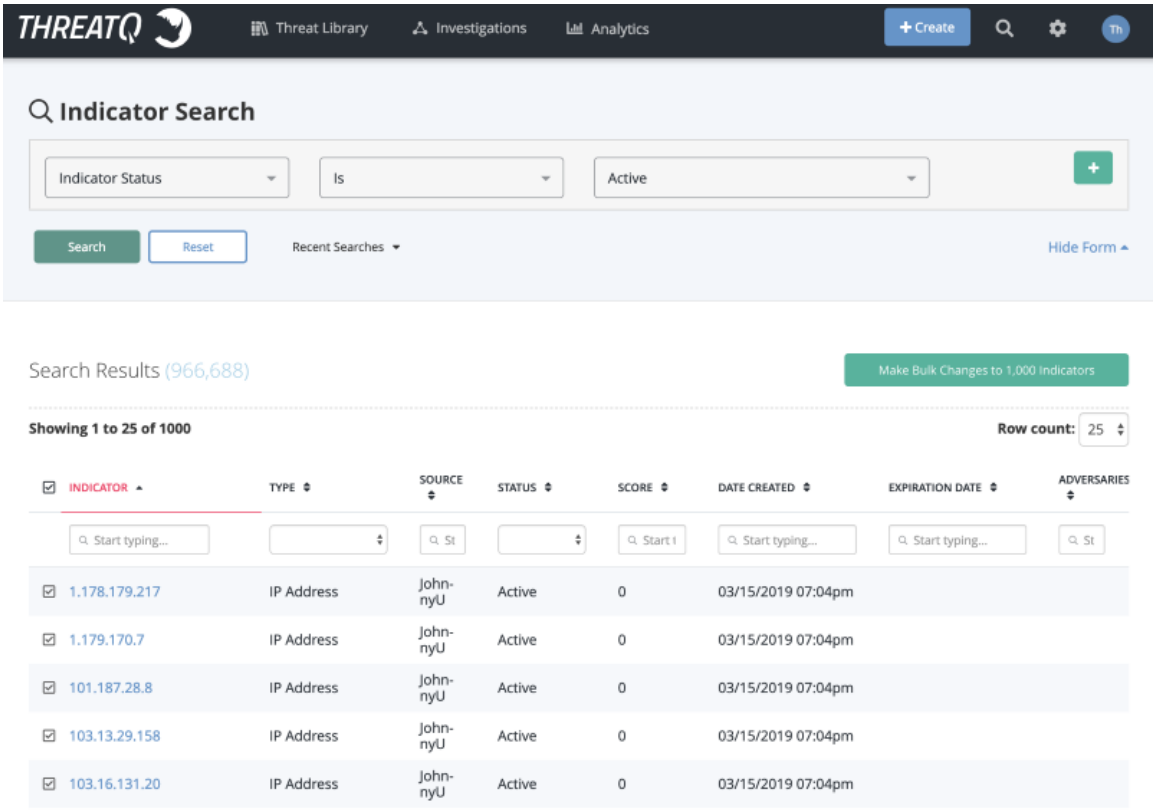
Click **+** to add more parameters. When your search consists of more than one parameter, you can select **and** or **or** using the dropdown between the search parameters.

4. Click **Search**.
   Search results are displayed in a search results table.



5. (Optional) Change the number of entries shown in the search results table by clicking the dropdown menu at the top right and selecting the desired option.
6. (Optional) Click a column header to sort the data by column, and click again to reverse sort order.
7. (Optional) Search within a column by clicking within the search field at the top of the column, entering a search keyword, and pressing Enter.

Results will be shown below the search query.



You can hide the query to view more of the search results.

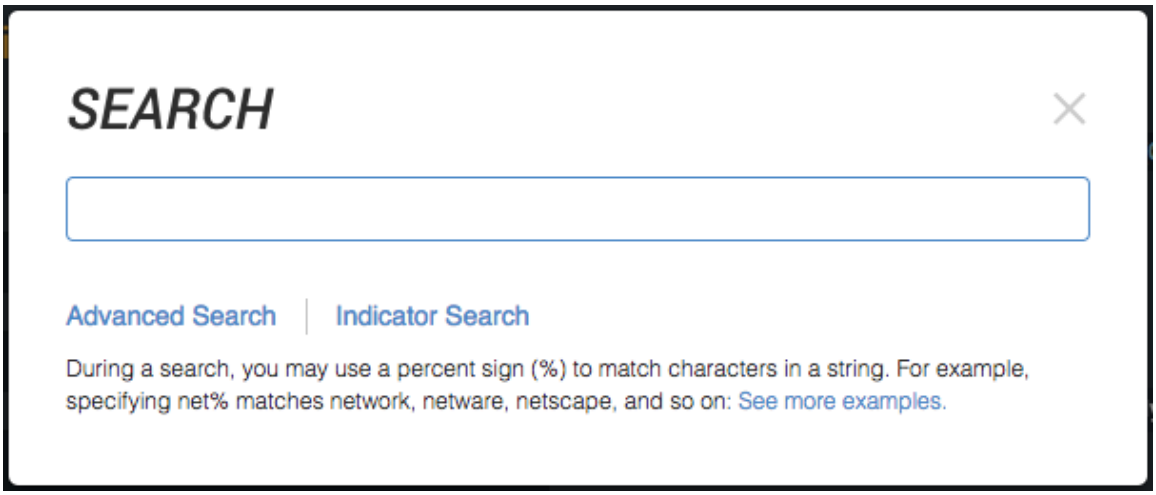
Making Bulk Updates to Search Results

The bulk update tool allows you to make batch changes to the objects in your Search results. The tool is limited to 1000 objects per update.

To make bulk updates to search results:

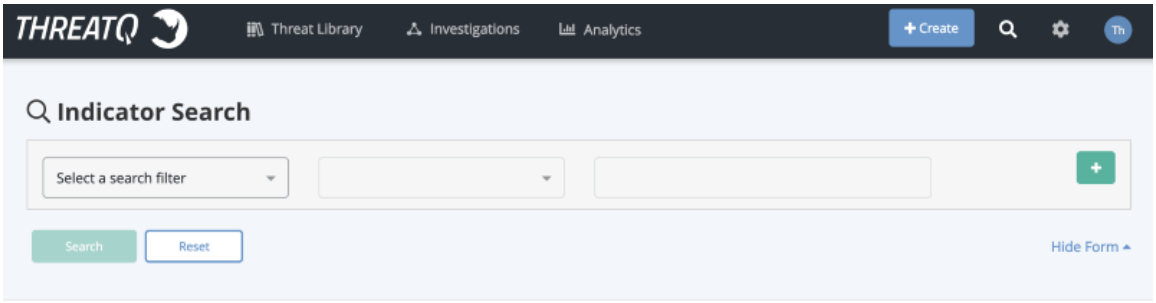
1. From the main menu, click the Search icon.

   The Search dialog box appears.



2. Click **Indicator Search.**

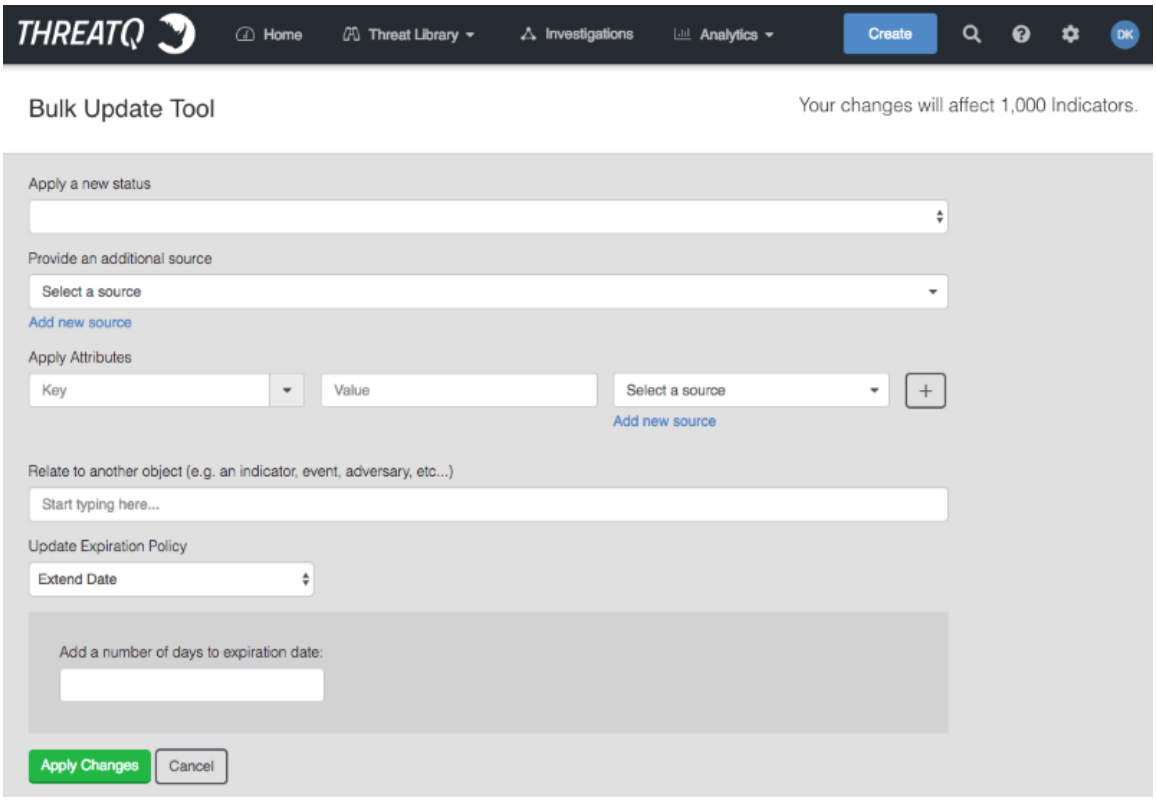
   The Indicator Search page appears.



3. Perform your Indicator Search.

4. At the top of the Search Results, choose **Make Bulk Changes to 1,000 Indicators**.

   The Bulk Update Tool appears.



5. Optionally, apply a new object status by choosing from the dropdown.
6. Optionally, enter an additional source.
7. Optionally, apply one or more attributes:
   a. Choose an Attribute Type from the dropdown.
   b. Enter an Attribute Value.
   c. Enter an Attribute Source.
   d. Optionally, choose the add icon to apply additional attributes.
8. Optionally, relate your search results to another object in the platform. As you enter the related object, ThreatQ offers type-ahead suggestions.

9. Optionally, update the object's expiration policy, by choosing an option from the Update Expiration Policy dropdown.
10. Click **Apply Changes**.

Indicator Status

Every indicator in the system will have a status applied to it.

The default statuses that ship with a standard installation of ThreatQ are as follows:

Status	Description
Active	Poses a threat and is being exported to detection tools.
Indirect	Associated to an active indicator or event (i.e. pDNS).
Review	Requires further analysis.
Whitelisted	Poses NO risk and should never be deployed.
Expired	Indicator has reached its expiration and has been is deemed by an analyst to pose less of a threat to their infrastructure than other indicators.

You cannot delete a default status but you can add new custom statuses to be used. See Adding an Indicator Status and the Related Topics section below for more details.

Most exports in ThreatQ are configured to use the Active status to signal deployment to external devices. However this can be modified and each status can be used however your organization sees fit.

Related Topics:

- Changing the Status of an Indicator
- Bulk Status Change
- Indicator Statuses

- Indicator Expiration
- Automatic Expiration and Policies

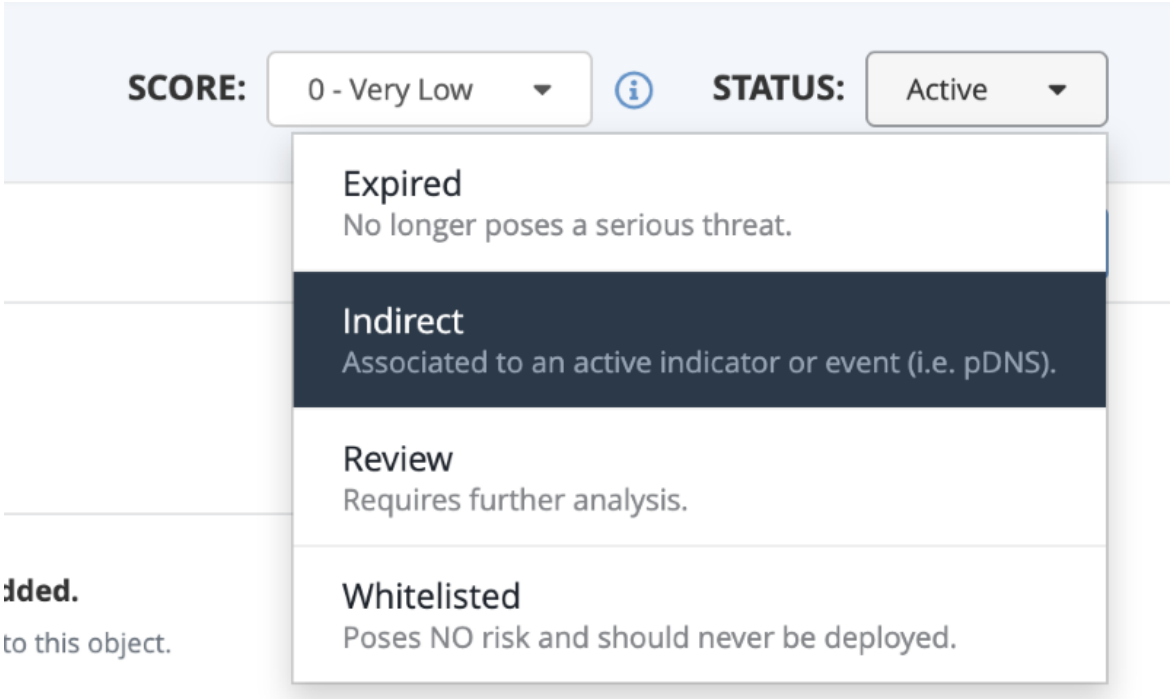
Changing the Status of an Indicator

Changing an indicator's status is straightforward, except in the case of whitelisting CIDR Block indicators. When whitelisting a CIDR Block indicator, this process generates a whitelisting rule. See Whitelisted Indicators for more information.

> See the Bulk Status Change topic for information on changing the status for multiple indicators.

Changing the status of an indicator:

1. Locate and click the indicator to open its details page.
2. Click the status dropdown menu, and select the desired status.



The status will be updated.

If an Administrator or the Primary Contributor are whitelisting a CIDR BLOCK indicator, there is a different process, as this actually generates a whitelisting rule. For more information, see the Creating a Whitelist Rule topic.

Indicator Expiration

Expiration ("Expired") is a status that can be assigned to an indicator. The expired status should be used when an indicator is deemed by an analyst to pose less of a threat to their infrastructure than other indicators.

Related Topics:

- Ways an Indicator can Expire
- Expiration Date Displays
- Changing an Individual Indicator's Date
- Automatic Expiration and Policies

Ways an Indicator can Expire

- **An analyst manually changes an indicator(s) status to "Expired"**

  This can be achieved by visiting an individual indicator's details page, then using the Status dropdown in the top right hand corner of the page to change the status.

  If the analyst wishes to change the status of multiple indicators at the same time, they can use the advanced search tool to find the indicators they'd like to update, then click the Bulk Update button found directly to the right above the search results.

- **An analyst manually sets an expiration date for a specific indicator**

  Each indicator has the option to have an expiration date set, which once past, will toggle the status of that indicator from it's current status to "Expired".

- **An expiration policy has been applied to the source reporting an indicator and therefore an expiration date is automatically set for that indicator during ingestion**

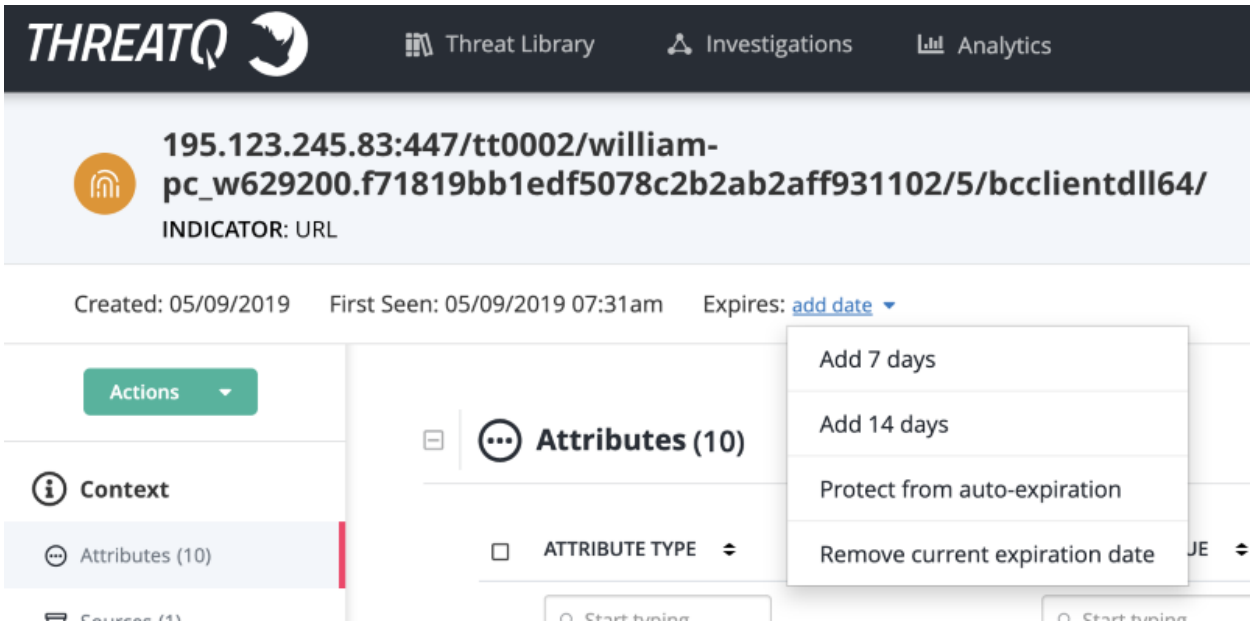
  Using the “Expiration” tab on the Indicator Management page, a ThreatQ admin has the ability to apply expiration policies to all ingested information, both new and existing, coming from a specific intelligence source.

If an indicator is reported by multiple sources that have expiration policies, the date will be set using the greater expiration date. For example, if both Feed A (with a 5 day policy) and Feed B (with a 3 day policy) report the same indicator on the same day, that indicator will automatically expire 5 days from now.

Changing an Individual Indicator's Date

See the Bulk Change Expiration Date topic for steps on updating the expiration date for a group of indicators.

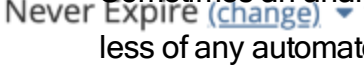
When viewing a specific indicator, its expiration date can be changed by clicking on the link next to the expiration information.



Options include:

Option	Description
Add 7 Days	This will extend the current expiration date by 7 days.
Add 14 Days	This will extend the current expiration date by 14 days.
Protect from Auto-Expiration	This will set the indicator to "Never Expire". Once set, this indicator will be exempt from all automated expiration processes regardless of circumstances. The only way for this indicator to expire moving forward is by analyst choice.
Remove Current Expiration Date	This will remove the currently set expiration date. If this indicator is reported by an intelligence feed (with an expiration policy) in the future, a new expiration date will be added at that point in time.

Expiration Date Displays

Option	Image	Description
No expiration date has been set		In this example, the indicator will not automatically expire because an expiration date has not been specified. This status will be changed if an analyst sets an expiration date or a new source (with an expiration policy applied to it) reports this indicator in the future.
An expiration date is set		In this example, the indicator has an expiration date set of 1/20/2017. This means that this indicator will expire when the calendar day changes from the 19th to the 20th of January (based on ThreatQ's server time, not the user's local time).
		When an expiration date is less than 7 days away, ThreatQ will switch to show a relative version of the date.
Protected from automatic expiration (Never Expire)		Sometimes an analyst will want an indicator to stay "Active" regardless of any automated circumstances. In this case you can set an indicator to be protected from auto-expiration, which will display the words "Never Expire". This can only be "overwritten" by an analyst.

Automatic Expiration and Policies

Automatic expiration allows you to deprecate stale intelligence based on a set of defined criteria. As the data becomes less relevant, ThreatQ sets the status to Expired, which relieves the data burden on your team or infrastructure.

You can configure automatic expiration from the Data Management page.

1. From the navigation menu, click on settings icon and select **Data Management**.

   The Data Management page will open with the Automatic Expiration tab selected by default.

Related Topics:

- How ThreatQ Calculates Expiration Dates
- Selecting an Expiration Policy per Feed
- Applying Expiration Policy Changes to Data
- Adding Exceptions
- Common Expiration Policy Scenarios

How ThreatQ Calculates Expiration Dates

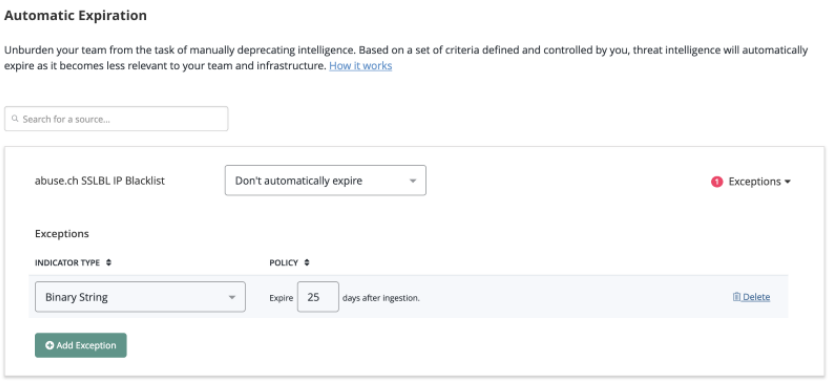
Scenario	Description
Indicator Reported by Source with an Expiration Policy	If an indicator has an expiration date and it's reported by a new source that has an expiration policy, ThreatQ will set the expiration date using the policy with the greater expiration date.
Indicator Report by a Source with an Expiration Policy of Never Expire	If an indicator has an expiration date and it's reported by a new source that has an expiration policy of Never Expire, ThreatQ sets that indicator to Never Expire.
Indicator Reported by a	If an indicator is reported by a source that has an exception for the indicator, the exception expiration date will be used regardless of

Source with an Exception for that Indicator	the greater expiration date. An exception takes precedence over the source's expire policy.
Indicator Reported by Two Different Sources	If an indicator is reported by a source with an Expiration Policy and then reported by a second source with another Expiration Policy, the greatest expiration date is selected to set the expiration date. The expiration date will be set based on the date the second source reported the indicator.
Indicator Reported by Two Different Sources, one with an Exception	If an indicator is reported by a source that has an exception for the indicator and then reported by a second source, the greatest expiration date is selected despite the exception. The expiration date will be set based on the date the second source reported the indicator.

Selecting an Expiration Policy per Feed

You can choose from three options when configuring an expiration policy for a source of intelligence:

Option	Description
Don't automatically expire (No policy set)	ThreatQ sets all feeds to **Don't Automatically Expire** until an analyst decides otherwise. When set, indicators reported from this specific feed do not have an expiration date automatically applied to them. If an indicator is reported by Source A (an intelligence feed without an expiration policy), and is later reported by Source B (an intelligence feed that expires data in 7 days), ThreatQ sets

Option	Description
	the indicators to automatically expire in 7 days.
Automatically Expire Indicators	When setting a specific intelligence feed to **Automatically Expire Indicators**, ThreatQ requires you to provide a specific number of days. After you configure this setting, it applies to all intelligence currently in the system, as well as new intelligence as it is ingested. ThreatQ calculates the appropriate expiration date based on the number of days from ingestion. Once an indicator's expiration date is met, its status changes to **Expired**. 
Never Expire	Using this setting ensures that all intelligence reported by a specific feed is protected from automatic expiration, regardless of scenario.

Applying Expiration Policy Changes to Data

When updating an expiration policy, the system now applies the update to all selected existing data in the platform to honor the new policy. This process can take a while based on system resources and the number of indicators in the system.

Refer to the following table for estimates on the total time required for the system to apply the selected policy to existing data, based on the following criteria:

- Dataset: 6 Million Indicators
- System Specifications: 32GB VM 4 vCPU

Indicators to reset expiration out of 6m total indicators	Reset and Recalculate Expiration	Expire Indicators	Total Time for Reset
50,000	3 hours and 30 minutes	53 seconds	3 hours 31 minutes
100,000	4 hours and 51 minutes	1.8 minutes	4 hours 53 minutes
200,000	10 hours 20 minutes	3.5 minutes	10 hours 24 minutes
1.2 million	2 days 7 hours 4 minutes	35 minutes	2 days 7 hours 40 minutes
3.1 million	3 days 16 hours 42 minutes	3.5 hours	3 days 20 hours
5.3 million	4 days 7 hours 17 minutes	4.7 hours	4 days 12 hours

Adding Exceptions

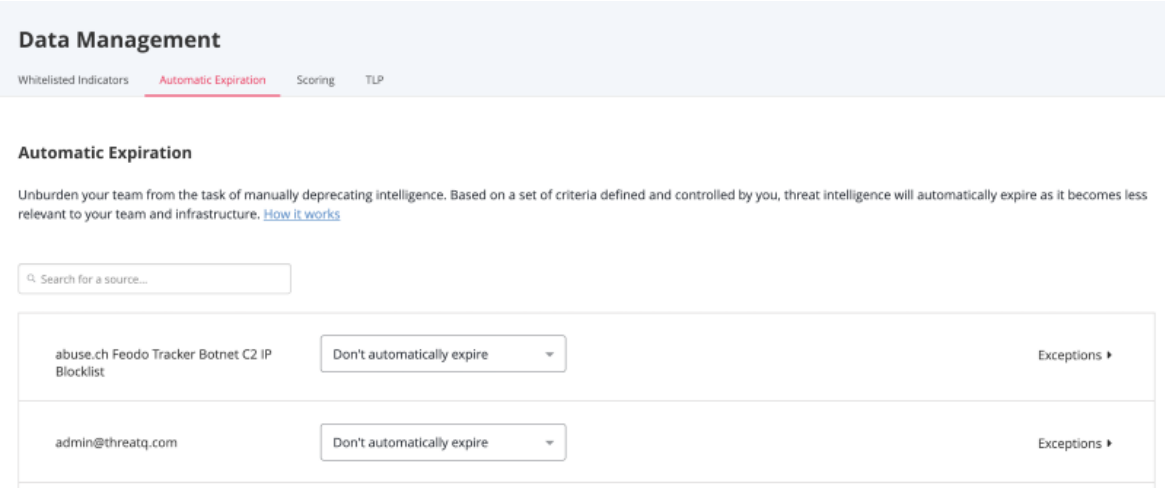
ThreatQ allows you to add exceptions based on specific indicator types within in a feed in addition to setting an expiration policy at a global level for all intelligence ingested by a specific feed.

To Add an Exception:

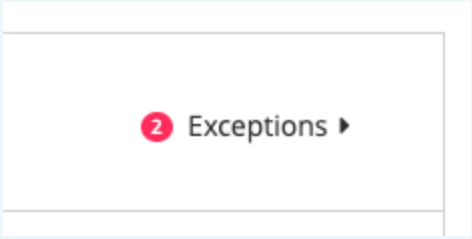
1. Navigate to the **Automatic Expiration** tab under **Data Management**.
2. Locate the source.

3. Click **Exceptions** to expand the option.

   The Exceptions option menu opens.



The number of existing exceptions for a source will be listed next to its Exceptions link.



4. Click **Add Exception**.
5. Select the **Indicator Type** from the dropdown.
6. Enter the number of days after the item has been ingested before expiring.

Repeat steps 4-6 to add multiple

7. Click on **Delete** next to the row to delete an exception.

8. Click on **Save**.

Common Expiration Policy Scenarios

Scenario	Description
An indicator is reported by a single source (with an expiration policy)	1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8. 2. When the date switches from 10/7 to 10/8, this indicator is queued to have its status changed to **Expired**.
An indicator is reported by Source A (with an expiration policy of 7 days) and 3 days later is reported by Source B (with an expiration policy of 10 days).	1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8. 2. Source B reports the same indicator 3 days later (10/4). The indicator's expiration date is set using the greatest expiration date between the two sources. In this example, the new expiration date will be 10/14 (10 days from when it was reported by Source B). 3. When the date switches from 10/14 to 10/15, this indicator is queued to have its status changed to **Expired**.
An indicator is reported by Source A (with an expiration policy of 7 days) and is later reported by Source B (with an expiration policy of Never Expire).	1. On 10/1, Source A reports the indicator and the expiration date is set to 7 days. 2. Source B reports the same indicator 3 days later with a policy of **Never Expire**. The indicator's expiration date is removed and the indicator is now set to **Protect from auto-expiration**.

Scenario	Description
An indicator is currently set to Expired and is reported by Source A (with an expiration policy of 7 days).	1. On 10/1, an indicator is in ThreatQ with a status of **Expired**. 2. On 10/1, Source A reports the indicator. The status of the indicator changes to whatever the default status is for Source A and the expiration date is set to 10/8. 3. When the date switches from 10/7 to 10/8, this indicator is queued to have its status changed to **Expired**.
An indicator is currently set to Expired and is reported by Source A (with an expiration policy of Never Expire).	1. An indicator is in ThreatQ with a status of Expired. 2. Source A, with an expiration policy of Never Expire, reports the indicator. The expiration of that indicator changes to Protect from auto-expiration.
A FQDN indicator is reported by Source A (with an expiration policy of 10 days with an exception for 5 days for FQDN indicators) and is later reported by Source B (with an expiration policy of 15 days).	1. On 10/1, Source A reports the FQDN indicator and the expiration date is set to 10/6.  An exception takes precedence over the source's expire policy. 2. Source B reports the same indicator 1 day later (10/2). The indicator's expiration date is set using the greatest expiration date between the two sources. In this example, the new expiration date will be 10/17 (15 days from when it was reported by Source

Scenario	Description
	B). 3. When the date switches from 10/17 to 10/18, this indicator is queued to have its status changed to **Expired**.

Indicator Scoring

Indicator scoring allows you to apply weighting to indicators and their contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. Indicator scoring allows you to set manual scores or you can rely on ThreatQ's scoring algorithm to calculate scores. After scores are calculated, you can change the score as desired to your custom value or accept the calculated value.

Related Topics:

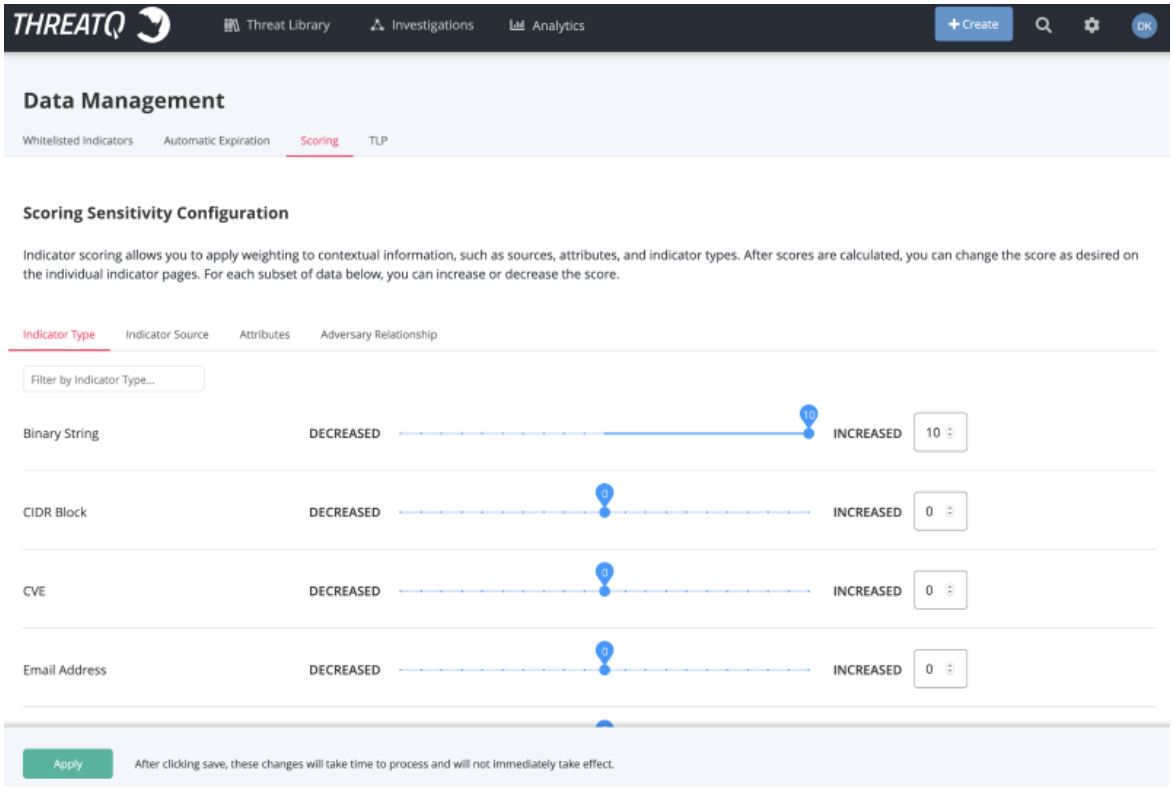
- Configure Indicator Scoring
- Building a Scoring Algorithm
- Overriding the Scoring Algorithm with a Manual Score

Configure Indicator Scoring

1. From the navigation menu, click on settings icon and select **Data Management**.

   The Data Management page will open with the Automatic Expiration tab selected by default.

2. Click on the **Scoring** tab.



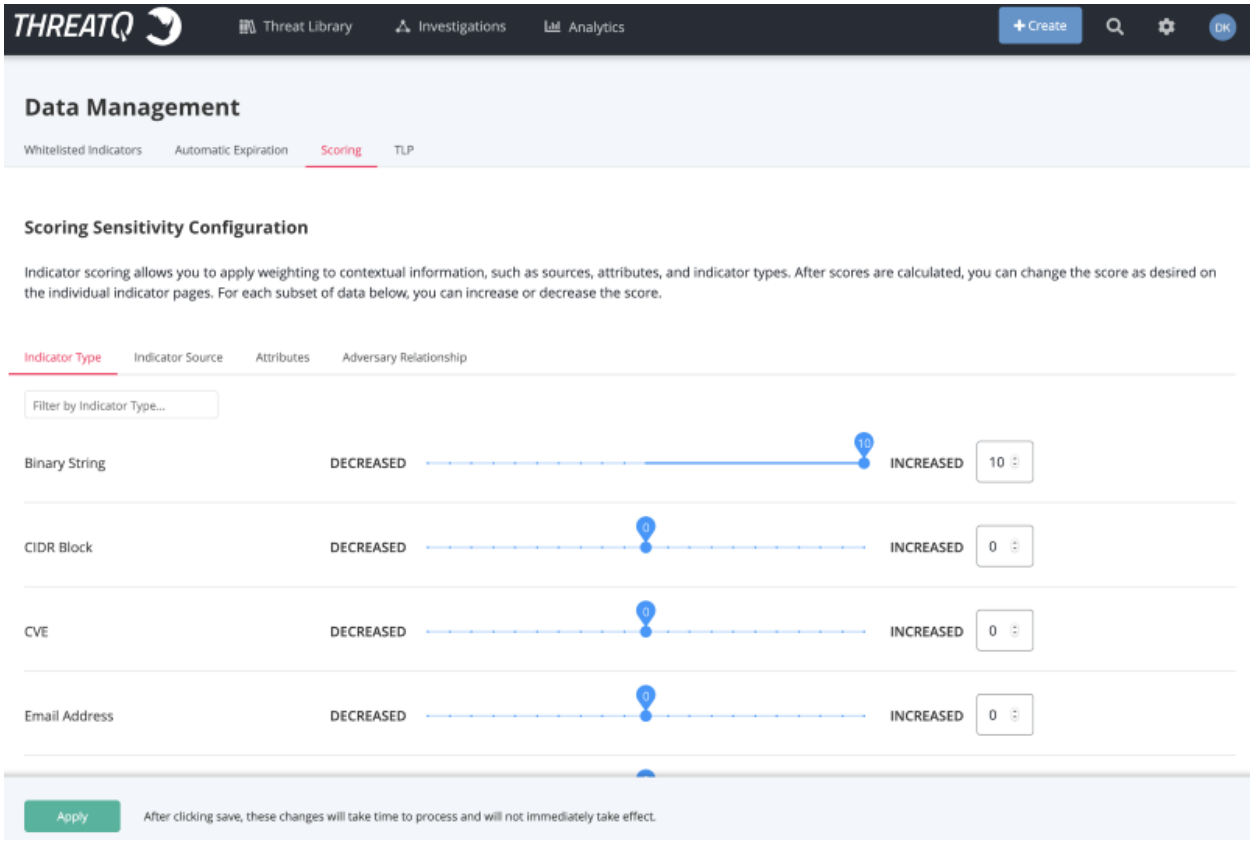
Building a Scoring Algorithm

As you build a scoring algorithm, you influence indicator scores based on the following criteria:

- Indicator Type
- Indicator Source
- Attributes
- Adversary Relationship

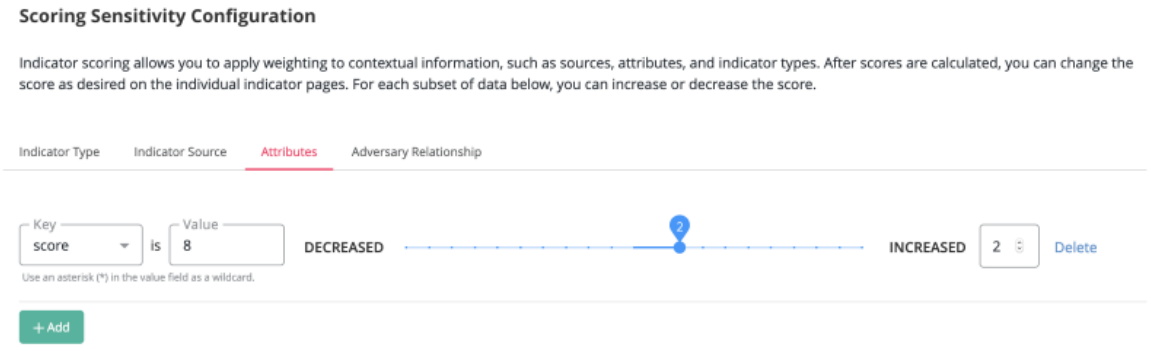
Use the slider to determine the sensitivity of the criterion you select. By default, the slider is positioned in neutral position, which in isolation produces an indicator score of zero. You may increase the score up to 10, which creates a score of **Very High**. You may also

decrease the score, which creates a score of **Very Low**.



Influencing Score Based on Attributes

1. Navigate to the Attributes category under Scoring.

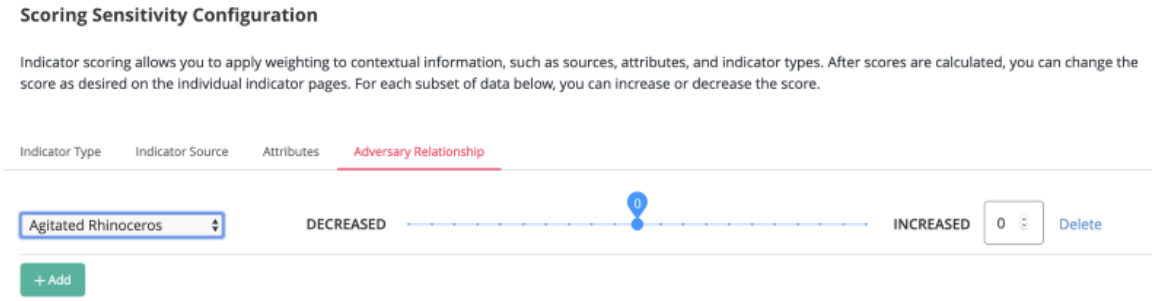


2. Click **Add**
3. Designate an **Attribute Key / Value Pair**

4. Adjust the sensitivity using the slider.
5. Click **Save**.

Influencing Score based on Adversary Relationship

1. Navigate to the Adversary category under Scoring.

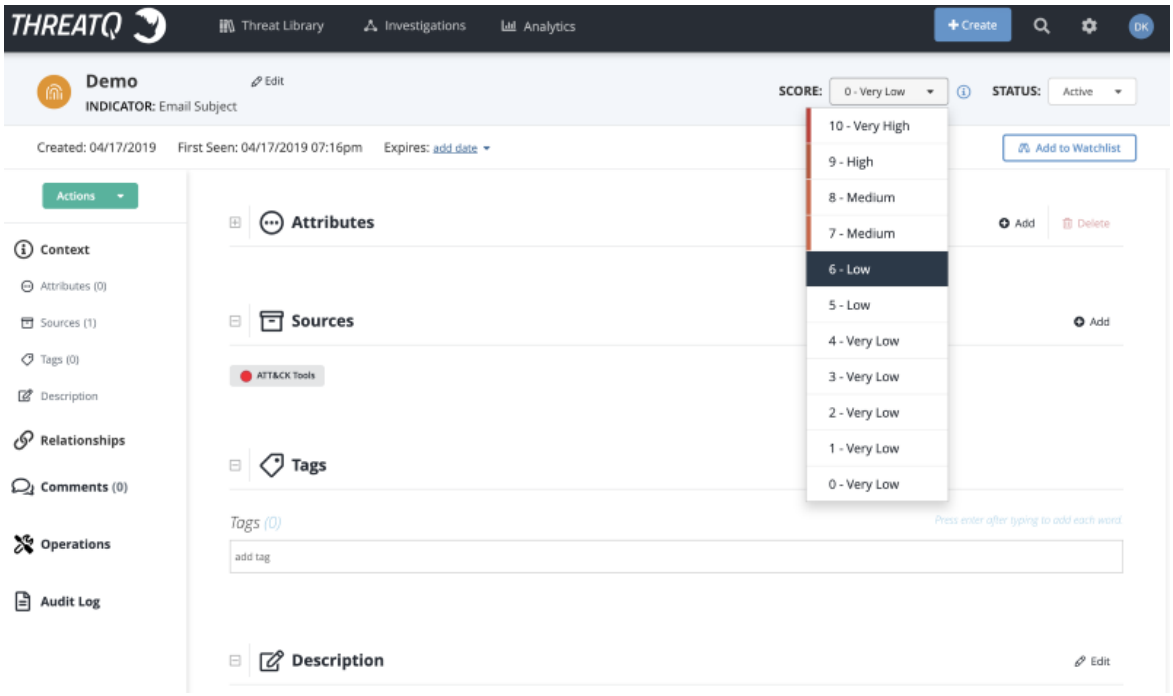


2. Click **Add**
3. Select an **Adversary**.
4. Adjust the sensitivity using the slider.
5. Click **Save**.

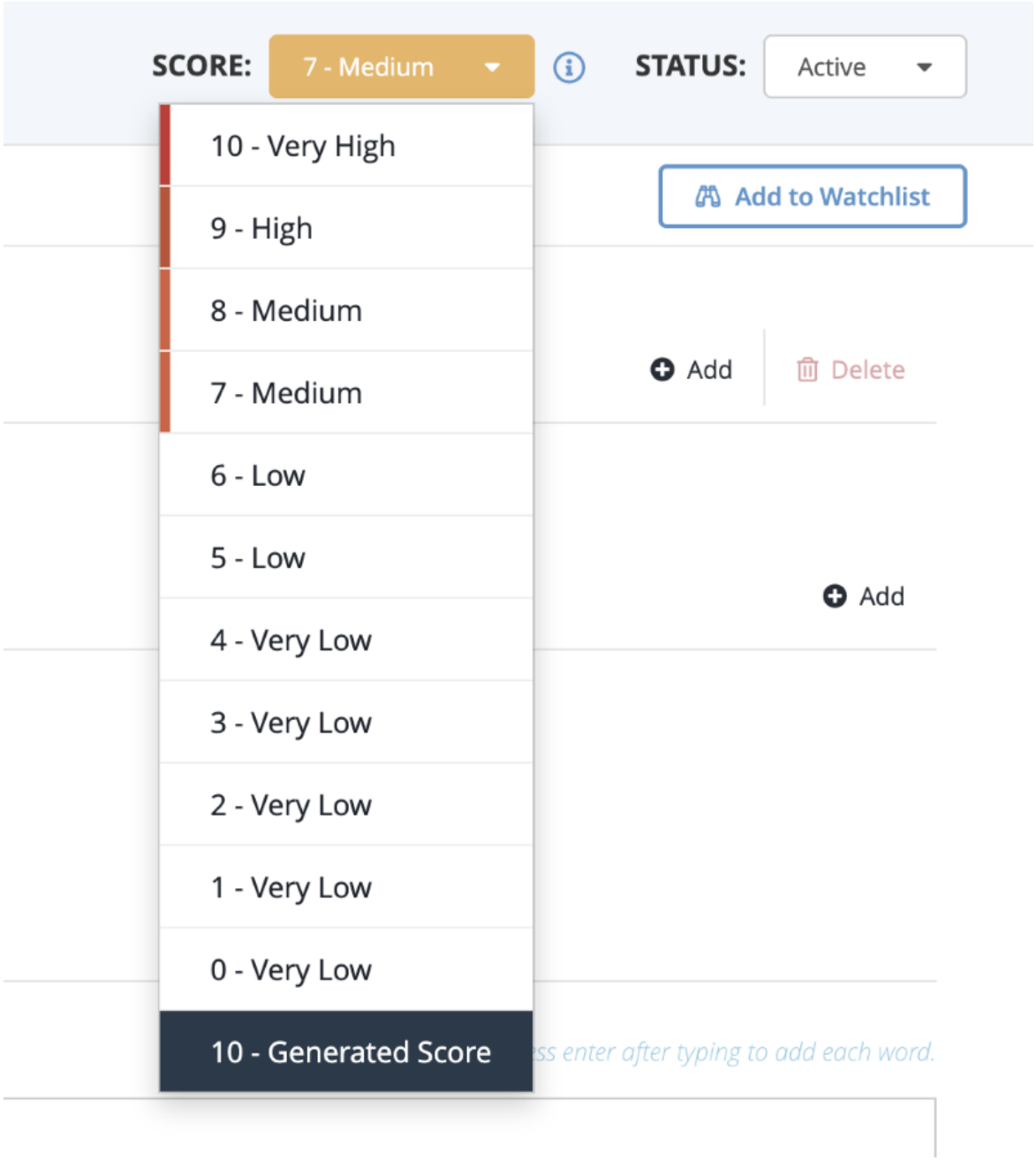
Overriding the Scoring Algorithm with a Manual Score

Setting a manual Indicator Score:

1. Navigate to an Indicator's Details page.
2. Click the **Score** dropdown and select a score.


THREATQ
Threat Library
Investigations
Analytics
+ Create
Demo
Edit
INDICATOR: Email Subject
SCORE: 0 - Very Low
STATUS: Active
Created: 04/17/2019
First Seen: 04/17/2019 07:16pm
Expires: add date
Add to Watchlist
Actions
Context
Attributes (0)
Sources (1)
Tags (0)
Description
Relationships
Comments (0)
Operations
Audit Log
Attributes
Add
Delete
Sources
Add
ATT&CK Tools
Tags
Tags (0)
add tag
Description
Edit
10 - Very High
9 - High
8 - Medium
7 - Medium
6 - Low
5 - Low
4 - Very Low
3 - Very Low
2 - Very Low
1 - Very Low
0 - Very Low

Optionally, you may revert to the calculated score by clicking on the Score dropdown and selecting **Generated Score**.



Whitelisted Indicators

There are some indicators that should be considered to be whitelisted, or non-malicious, and we do not want those indicators going out to other systems. For example, a company's

own domain name would never need to be blocked.

The whitelisting process creates rules that apply to particular indicators, so that when those indicators come in in the future, they will be automatically whitelisted.

Within this section, the following options are available:

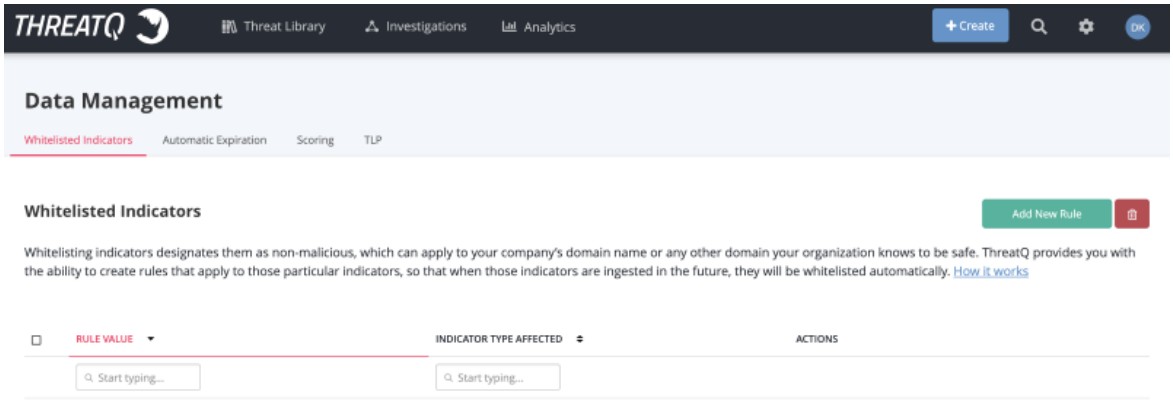
- Viewing Existing Whitelist Rules
- Creating a Whitelist Rule
- Editing a Whitelist Rule
- Removing a Whitelist Rule

Viewing Existing Whitelist Rules

To view existing whitelist rules:

1. Click on the settings icon and select **Data Management**.
2. Select the **Whitelisted Indicators** tab

   The Whitelist Rules page opens. Existing whitelist rules are listed in the Whitelist Rules table.



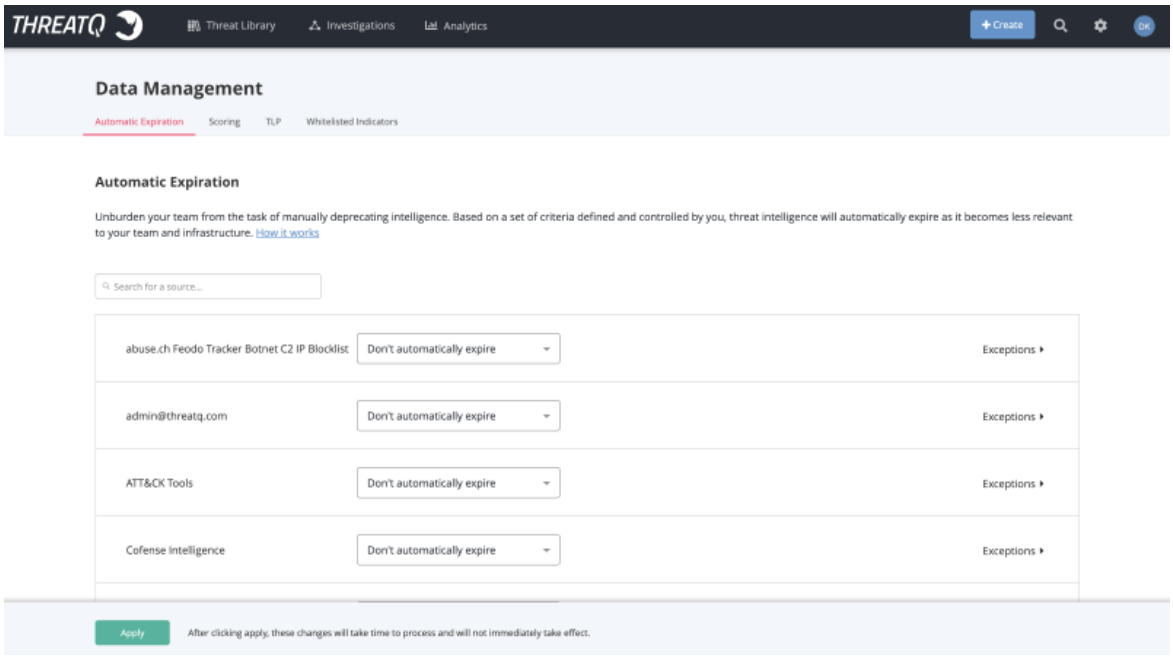
Creating a Whitelist Rule

The process of creating a whitelist rule is almost exclusively available via the Tools menu. However, it is important to note that whitelisting a CIDR Block indicator also creates a whitelist rule.

To create a whitelist rule:

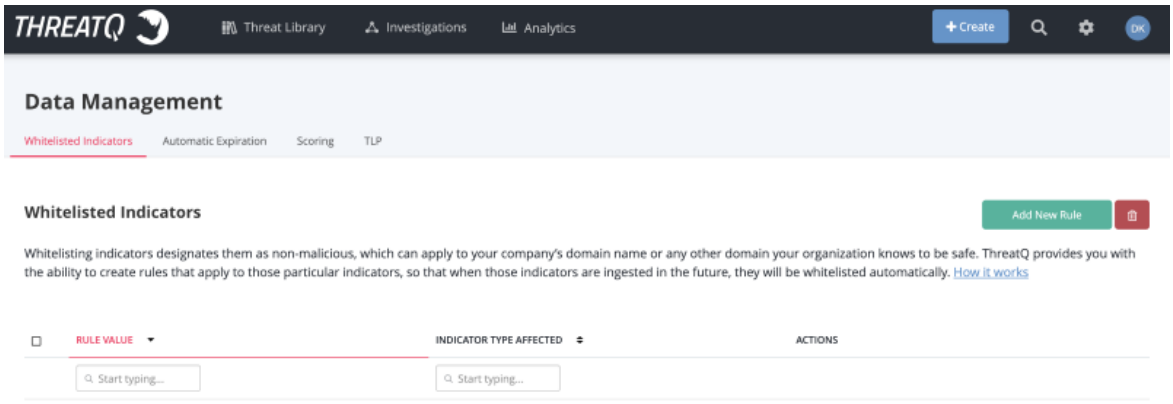
1. Click on the settings icon and select **Data Management**.

   The Data Management page opens.



2. Select the **Whitelisted Indicators** tab.

   The Whitelisted Indicators section loads.



3. Click **Add Rule**.

   The Add Whitelist Rules page opens.

4. Select the Indicator type the rule will apply to.

5. Add a Rule Value.

6. Click **Next**.

Affected indicators are listed in the dialog box.

7. Review the affected indicators to determine if you are satisfied with the rule.

   The rule has not been applied yet, so you still have time to edit it based on whether you are satisfied with how it affects the indicators.

8. Click **Continue Editing this Rule**.

9. If you are satisfied with the rule, click **Add Rule**.

   The rule is applied to existing indicators, and it is entered into the Whitelist Rules table.

   Any new indicators will also have the rule applied to them as they enter the system.

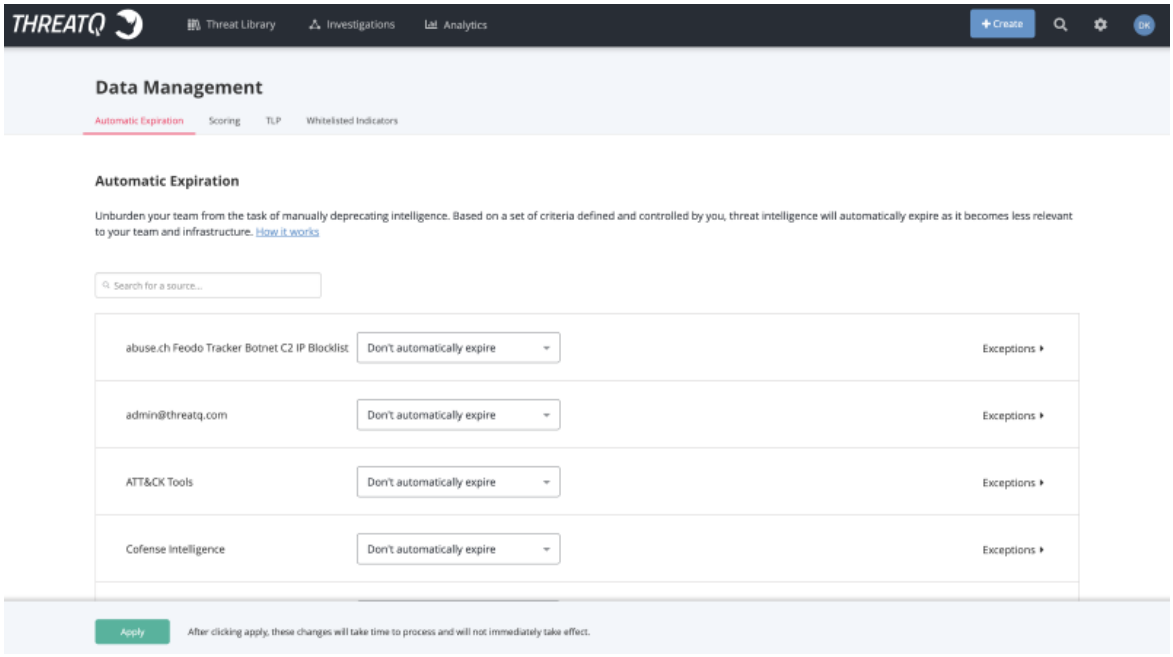
Editing a Whitelist Rule

Important: Editing a whitelist rule will not undo any changes the rule had made prior to being edited.

To edit a whitelist rule:

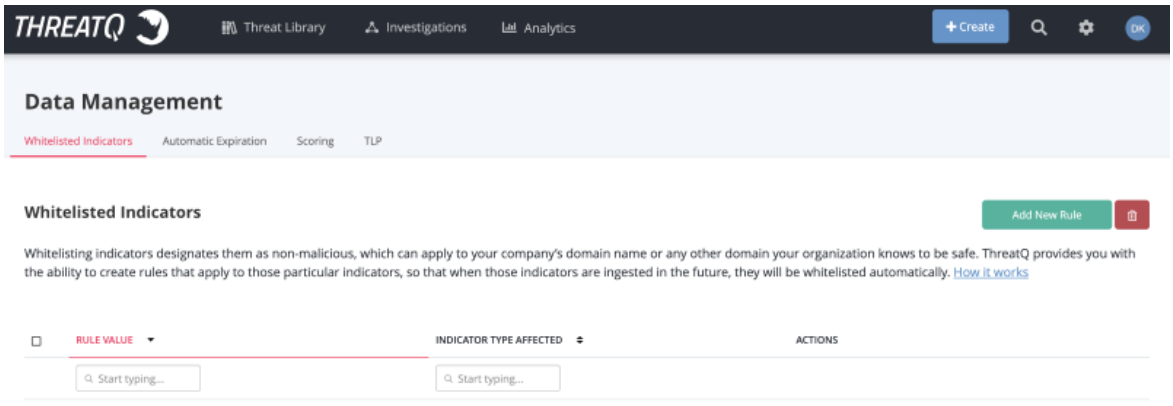
1. Click on the settings icon and select **Data Management**.

   The Data Management page opens.



2. Select the **Whitelisted Indicators** tab.

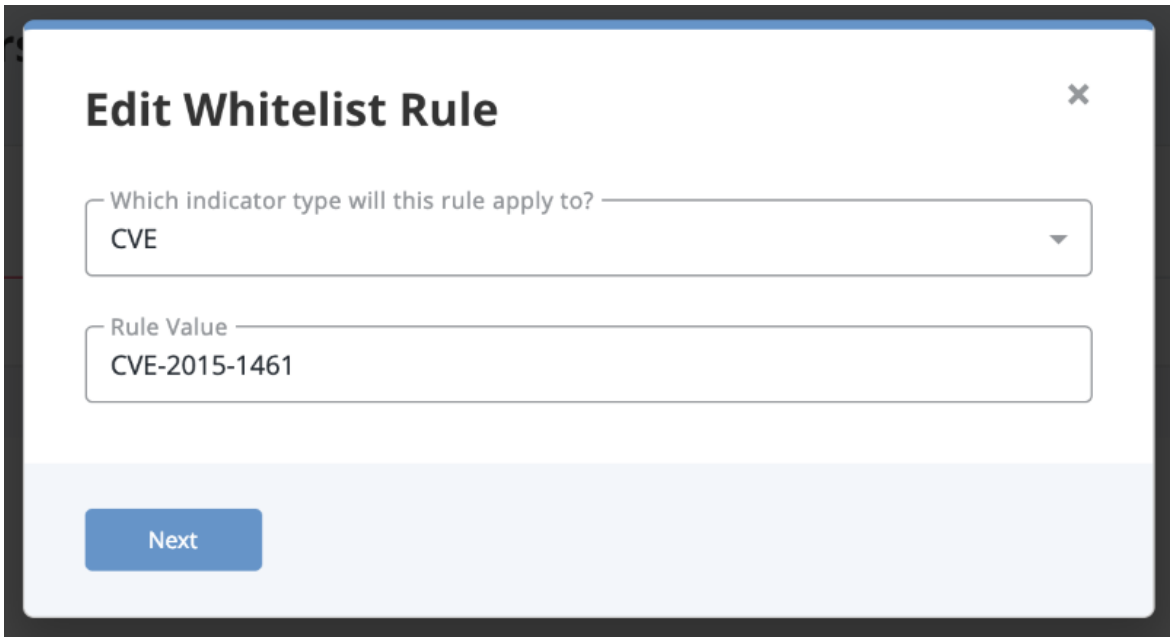
   The Whitelisted Indicators section loads.



3. In the Whitelist Rules table, locate the rule you wish to edit.

4. Click **Edit**.

   The Edit Whitelist Rule dialog box opens.



5. Make the desired edits and click **Next**.

   Affected indicators are listed in the dialog box.

6. Review the affected indicators to determine if you are satisfied with the rule.

   The rule has not been applied yet, so you still have time to edit it based on whether you are satisfied with how it affects the indicators.

7. If you are satisfied, click **Edit Rule**.

   The rule is applied to existing indicators, and it is updated in the Whitelist Rules table.

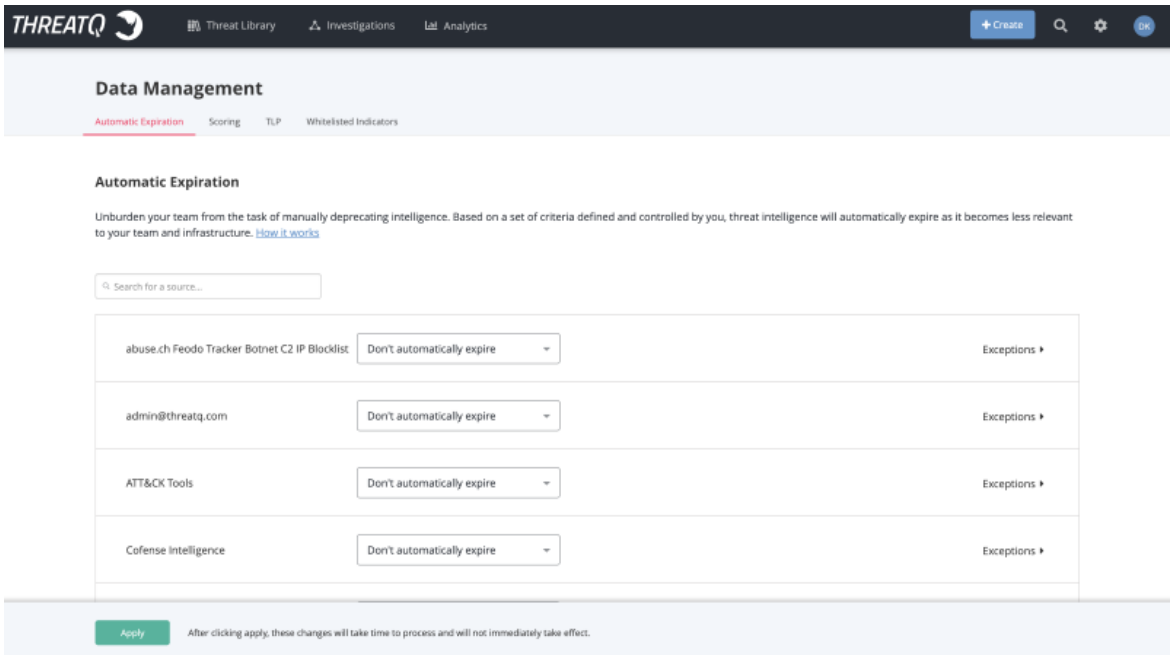
   Any new indicators will also have the rule applied to them as they enter the system.

Removing a Whitelist Rule

To remove a whitelist rule:

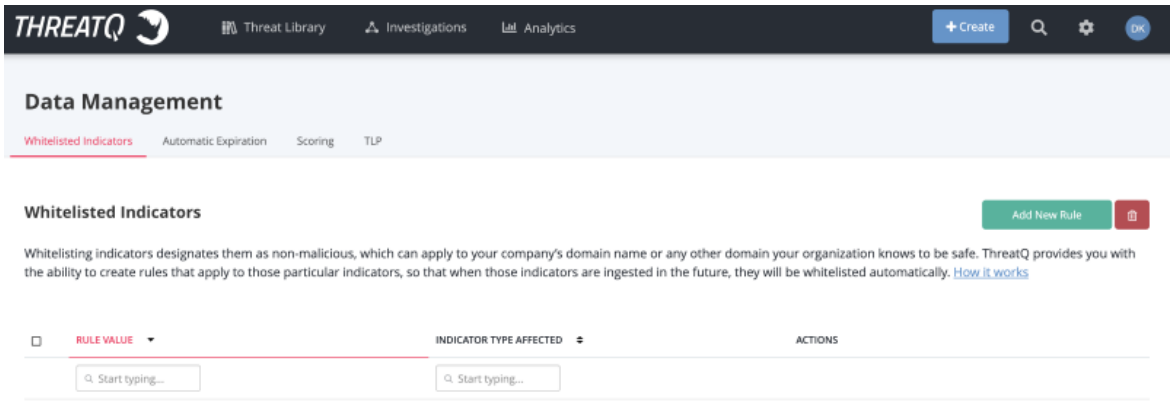
1. Click on the settings icon and select **Data Management**.

   The Data Management page opens.



2. Select the **Whitelisted Indicators** tab.

   The Whitelisted Indicators section loads.



3. Locate and select the rule(s) from the table that you wish to remove.
4. Click on the delete Icon  .

   A confirmation dialog box opens, asking if you are sure.

5. Click **Delete Whitelist Rule**.

   The rule is deleted and a confirmation alert appears in an alert bar at the top of the page.

Indicator URL Normalization

Remove Quotes from the Beginning and/or End of an Indicator

Single and double quote characters are removed if they are the first or last character of an indicator.

Remove Unneeded Spaces found within an Indicator

All spaces irrelevant of their position in the Indicator value are removed (when applicable).

Adjust leading protocol from indicators

Indicators with a leading protocol [http://, https://, ftp://, or ftps://] are extracted and included as an attribute. When applicable, this indicator adjustment could change the indicator type from URL to FQDN.

Example: Original URL indicator of http://evilsubdomain.no-ip.biz/ would convert to a FQDN = evildomain.no-ip.biz.

Adjust the Port from an IP Address

An IP address with a port [ex. 199.7.136.88:8143] will be truncated to the IP address and the port assignment will be added as an attribute.

Using the previous example the following indicator/attribute will be created:

Field	Value
URL	199.7.136.88
Attribute > Port	8143

Adjust Defanged/Neutered Indicators

Indicators that have been defanged/neutered in order to “safely” share them (i.e. www [dot] 3322 [dot] org or badguy [at] gmail.com) need to be adjusted during import in order to ensure the indicators are properly deployed.

Create an IP Address from a URL (when applicable)

Using the previous example the following indicators will be created:

Field	Value
URL	51.255.131.66/civis/viewforum.php
IP Address	51.255.131.66

Create a FQDN from a URL (when applicable)

When a URL contains a domain [ex. bat99-11611.co/gate777.php] a second indicator will be created for the domain [bat99-11611.co].

Using the previous example, the following indicators will be created:

Field	Value
URL	bat99-11611.co/g-ate777.php
FQDN	bat99-11611.co

Extract HTTP Parameters from a URL Indicator

HTTP parameters [chained.j3oil-gasinc.net/civis/viewforum.php?keywords=9obo&fid0=c27] are important but can significantly limit pattern-matching detection capabilities due to the likelihood of parameter deviations, as well as, hamper the volume of URL indicators being deployed. To increase the probability of detection the http parameters are extracted and created as attributes.

In this example:

Field	Value
URL IOC	chained.j3oilgasinc.net/civis/viewforum.php
Attribute = HTTP Parameter = keywords	9obo&fid0=c27

Maintain "WWW" on FQDN Indicators

When parsing or importing a FQDN the "www" will be maintained.

Replace and/or Remove Special Characters

Character	Replacement
ASCII Values < 32 ASCII Values > 127	<space>
Ascii 96	-
Ascii145	'
Ascii146	'
Ascii147	"
Ascii148	"
Ascii151	-
carriage return and line feed	<space>
Control Characters	Remove
Convert to UTF8	
Remove leading and trailing space, tab, newline, carriage return, vertical tabs and null characters.	

Supported Defanging Techniques

The table below lists all supported indicator defanging techniques.

[.]	=>	.
[dot]	=>	.
(dot)	=>	.
[d]	=>	.
-dot-	=>	.
dot	=>	.
hxxp://	=>	http://
hxxx://	=>	http://
hxxps://	=>	https://
hxxxs://	=>	https://
[hxxp]	=>	http
hxtp://	=>	http://
htxp://	=>	http://
hxtps://	=>	https://

htxps://	=>	https://
[http]	=>	http
[http://]	=>	http://
[https]	=>	https
[https://]	=>	https://
[at]	=>	@
-at-	=>	@
_at_	=>	@
-@-	=>	@
_@_	=>	@
[@]	=>	@
[www]	=>	www

Signatures

ThreatQ allows you to ingest and manage Signatures, such as Snort and OpenIOC. While importing, ThreatQ parses the signature file for Indicators to add. Once signatures are included in your deployment, you can add contextual information and correlate them with Indicators, Events, Adversaries, and Files.

Related Topics:

Signatures Management Page

The Signatures Overview page displays all signatures in the platform. For each signature, the table displays the Date Created, Signature Type, and Signature Title.

You can filter the table based on criteria to view specific signatures. For each signature, you can click to view expanded details.

From the Signatures Overview page, you can do the following:

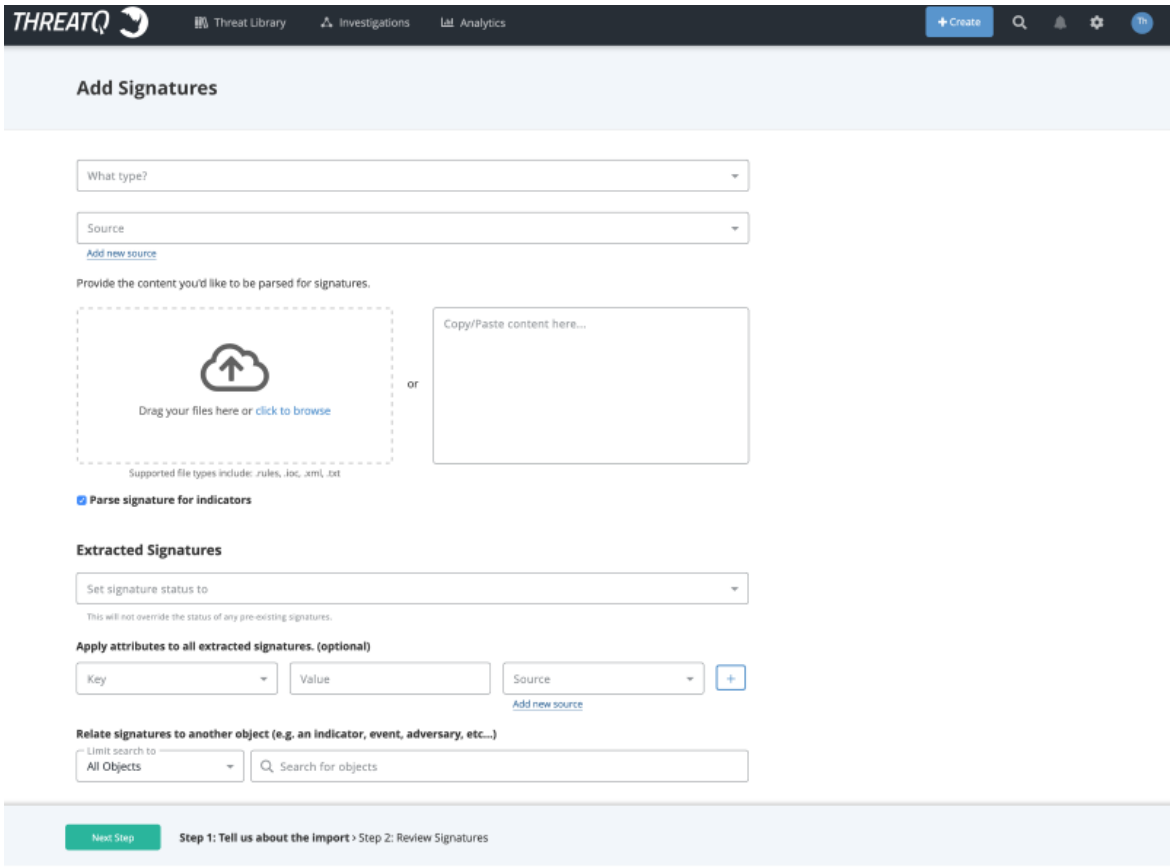
- View all signatures in the platform and details for each signature
- Filter signatures by Date Created, Signature Type, and Signature Title
- Add new signatures

Adding a Signature

To add a Signature:

1. From the main menu, choose **Create > Signature**.

   The Add Signatures dialog box opens.

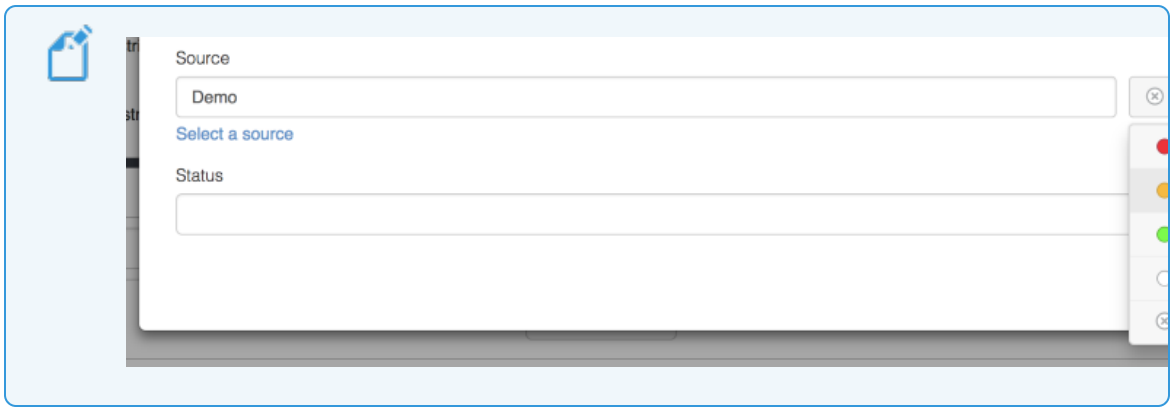


2. Choose the type of signature from the drop-down .

   For Yara, see Adding a Yara Signature.

3. Select a **Source** from the dropdown provided.

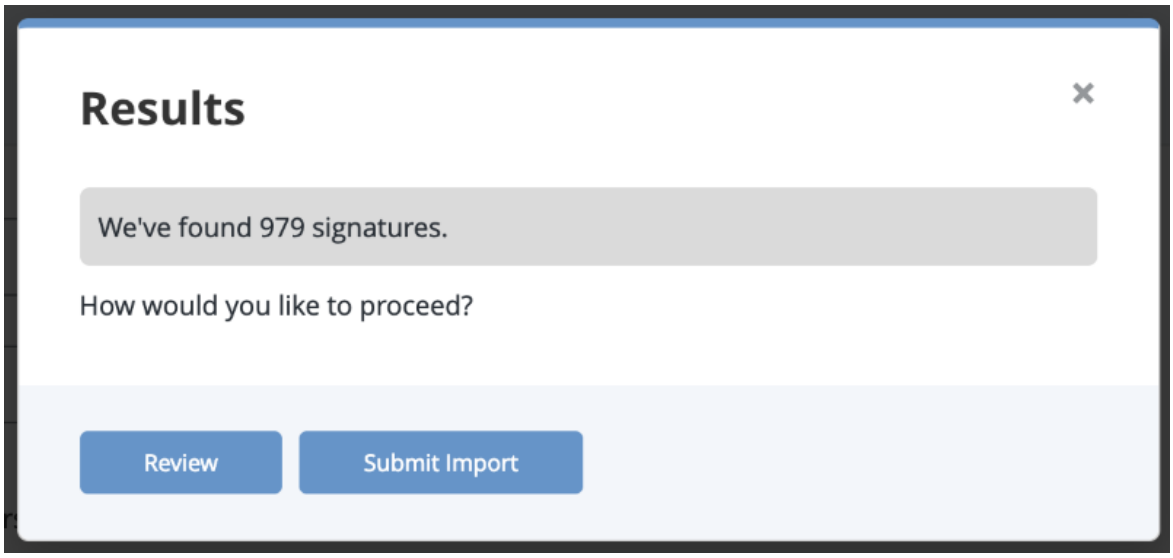
   You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP designation light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



5. Do one of the following:
   - Drag your file(s) into the left pane.
   - Click **click to browse**, and locate the file you wish to upload.
   - Copy/paste content into the right pane.
6. Optionally, select to parse the signature for indicators.
7. Choose a **Signature Status** from the drop-down menu.
8. Optionally, **Apply attributes to all extracted signatures**:
   - Select an **Attribute Type**.
   - Enter an **Attribute Value**.
   - Enter an **Attribute Source**.
   - Optionally, click the Add icon for additional attributes.
9. Optionally, relate the signature to another object by entering the object in the **Relate signatures to another object** field.

10. Click **Next Step**.

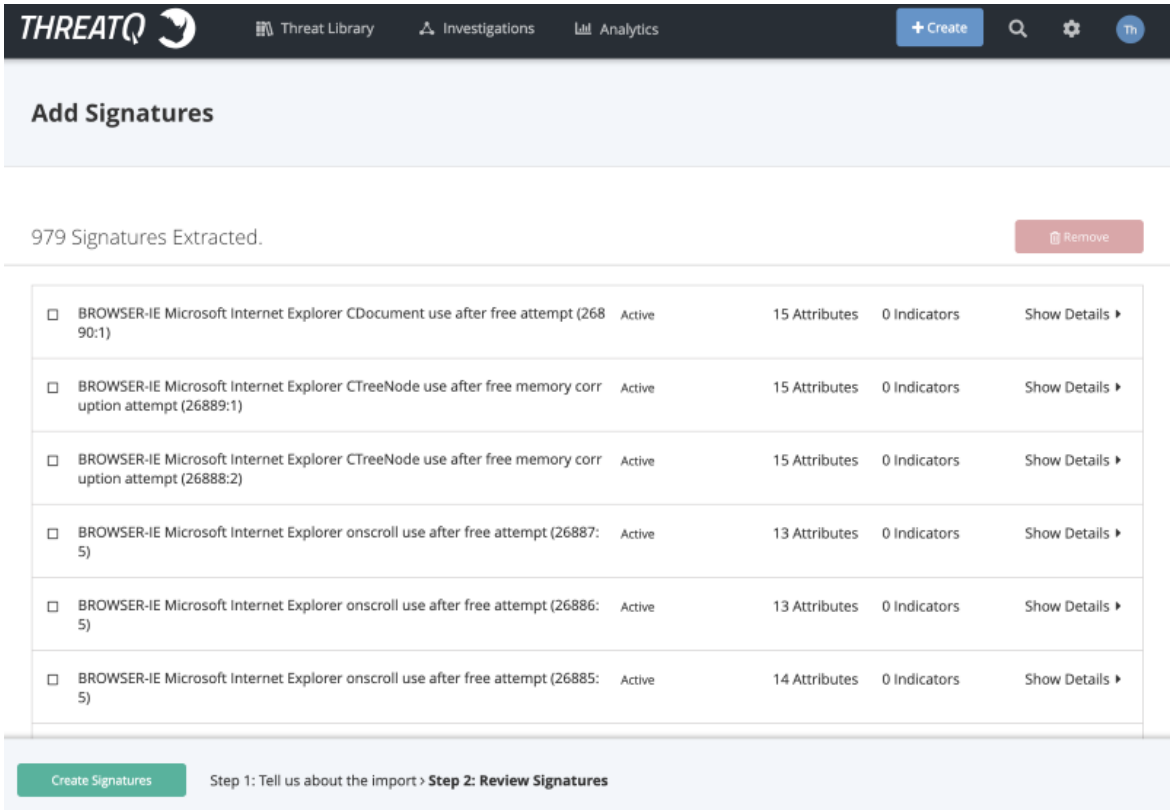
    If signatures are discovered, the Results dialog box appears.



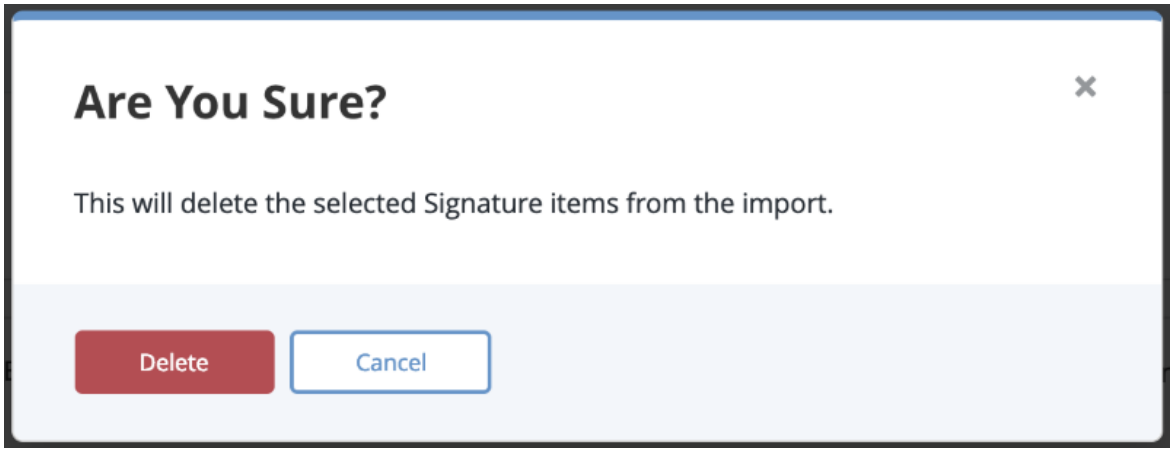
11. You can either select **Submit Import** to finish adding the signatures or **Review** to customize what data is imported.

    If you selected to review signatures, the Add Signatures Step 2: Review page

loads.



12. Select one or more signatures and click **Delete**.
13. Click on **Show Details** for a signature to review individual items in a signature.
    Use the checkboxes to select unwanted signature items and click **Delete**.
    A warning dialog box appears.



14. Click **Delete** to remove the unwanted items.

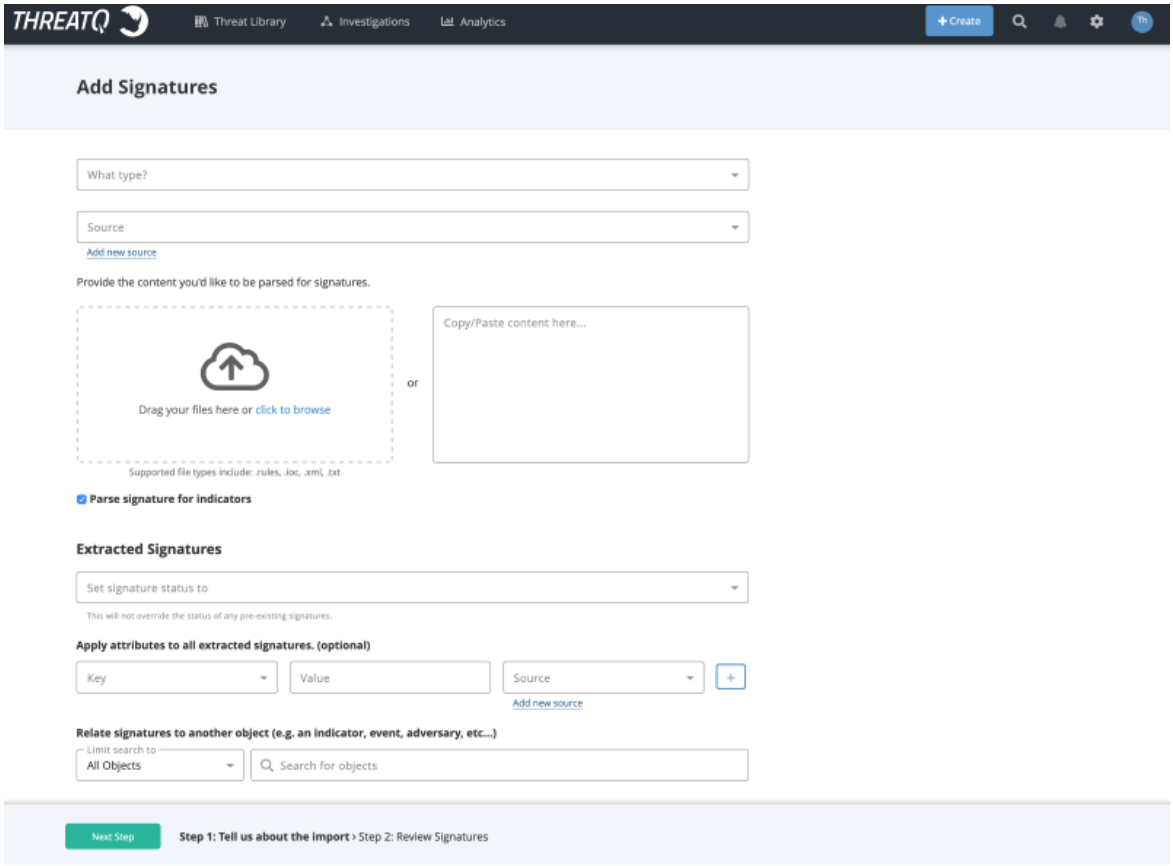
15. Click **Create Signatures** when finished.

Adding a Yara Signature

To add a Signature:

1. From the main menu, choose **Create > Signature**.

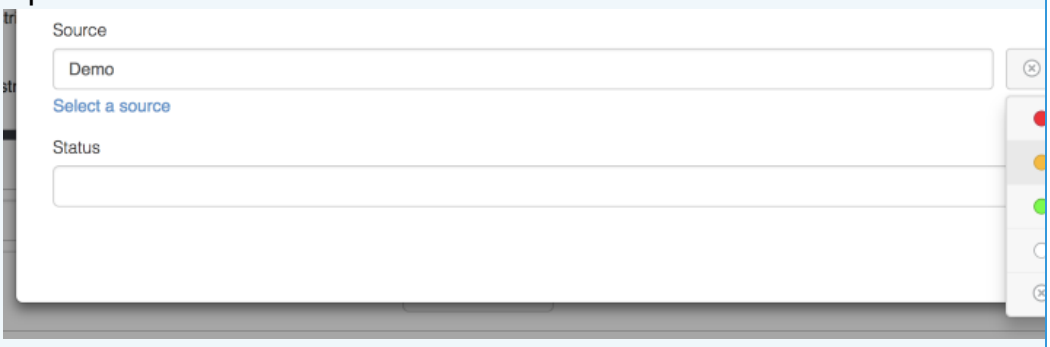
   The Add Signatures dialog box opens.



2. Select **Yara** as the type of signature from the drop-down .
3. Select a **Source** from the dropdown provided.

> You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP designation light for the new source

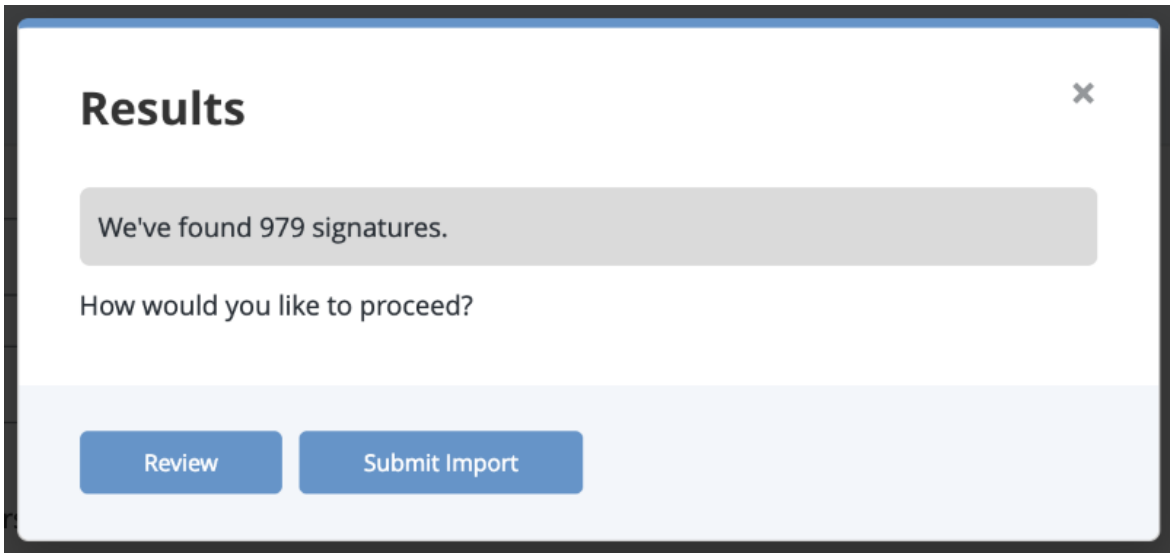
in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



5. Do one of the following:
   - Drag your file(s) into the left pane.
   - Click **click to browse**, and locate the file you wish to upload.
   - Copy/paste content into the right pane.
6. Optionally, select to parse the signature for indicators.
7. Determine the method to use if multiple signatures are discovered:
   - Save independently as unique signatures
   - Save as a single signature
8. Choose a **Signature Status** from the drop-down menu.
9. Optionally, **Apply attributes to all extracted signatures**:
   - Select an **Attribute Type**.
   - Enter an **Attribute Value**.
   - Enter an **Attribute Source**.
   - Optionally, click the Add icon for additional attributes.
10. Optionally, relate the signature to another object by entering the object in the **Relate signatures to another object** field.

11. Click **Next Step**.

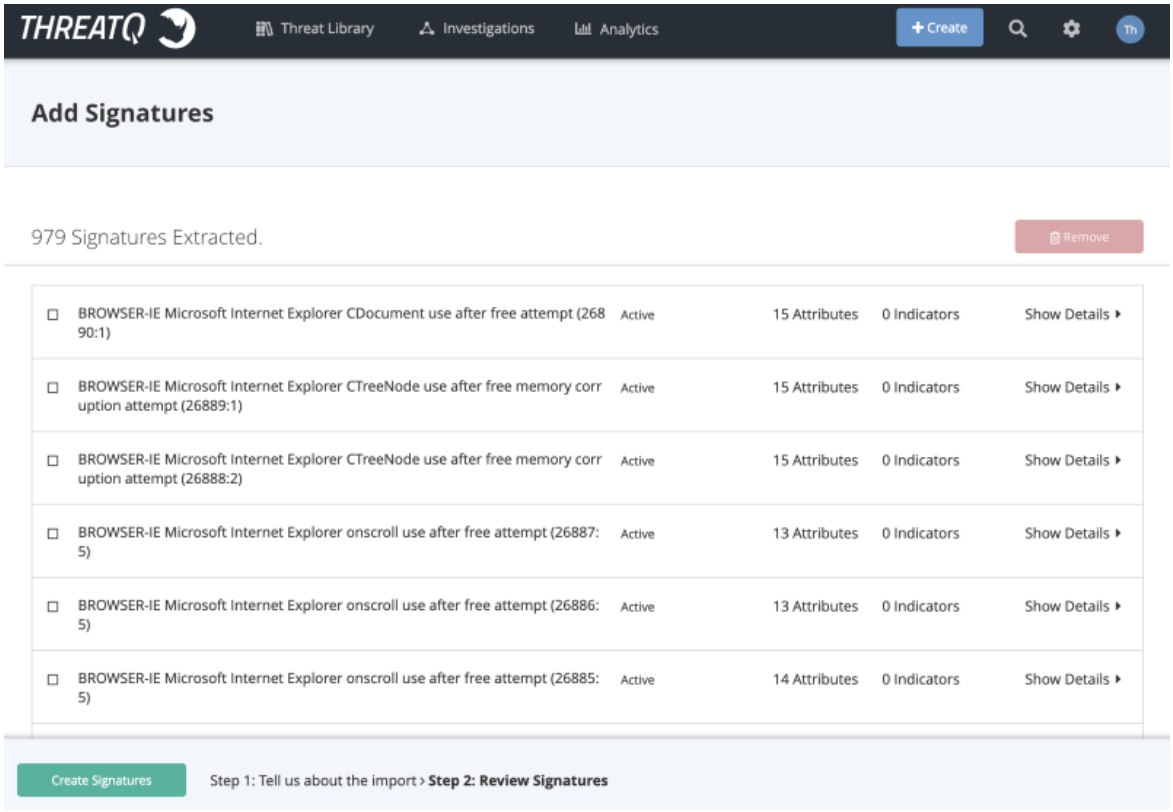
    If signatures are discovered, the Results dialog box appears.



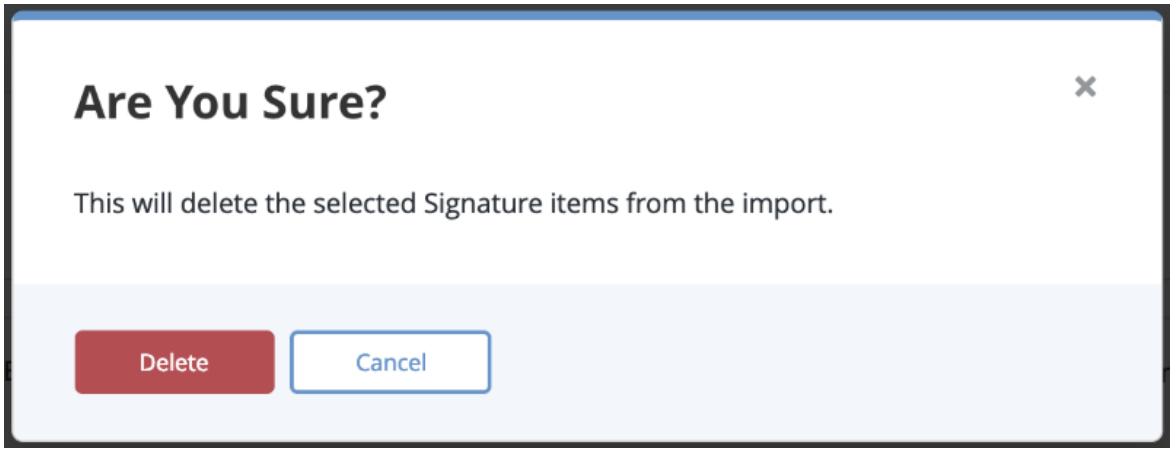
12. You can either select **Submit Import** to finish adding the signatures or **Review** to customize what data is imported.

    If you selected to review signatures, the Add Signatures Step 2: Review page

loads.



13. Select one or more signatures and click **Delete**.
14. Click on **Show Details** for a signature to review individual items in a signature.
    Use the checkboxes to select unwanted signature items and click **Delete**.
    A warning dialog box appears.



15. Click **Delete** to remove the unwanted items.

16. Click **Create Signatures** when finished..

STIX

The following describes how to use STIX in ThreatQ:

- STIX Overview
- ThreatQ STIX Object Types
- STIX Data Mapping
- Parsing a STIX File for Indicators

STIX Overview

ThreatQ allows you to ingest and manage STIX files. You can ingest STIX data in two ways:

- You can set up a STIX/TAXII Feed, as described in STIX/Taxii Feeds.
- You can upload a STIX file or insert STIX data to parse for indicators, as described in Parsing a STIX File for Indicators.

ThreatQ supports STIX 1.1.1, STIX 1.2 and STIX 2.0.

Related Topics

- STIX Data Mapping
- ThreatQ STIX Object Types

ThreatQ STIX Object Types

STIX integration provides ThreatQ with the following additional object types.

- Campaigns
- Courses of Action
- Exploit Targets
- Incidents

- TTP objects
- Identities (STIX 2.0)
- Reports (STIX 2.0)
- Vulnerabilities (STIX 2.0)

These objects enable better understanding and communication of STIX data. STIX data will be mapped to these objects and existing objects in the system.

STIX Data Mapping

The following sections display how STIX data becomes mapped to indicator objects and attributes in ThreatQ.

- STIX 1.1.1, 1.2 Data Mappings
- STIX 2.0 Data Mappings

STIX 1.1.1, 1.2 Data Mappings

You can click on the icon located to top-right of this topic to expand and collapse all mapping tables below.

Threat Actors Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Identity	Adversary.value	
ID	Adversary.attribute	STIX Reference ID
Title	Adversary.value	
Type	Adversary.attribute	Type
Timestamp	Adversary.published_at	

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Description	Adversary.attribute	Description
Motivation	Adversary.attribute	Motivation
Sophistication	Adversary.attribute	Sophistication
Intended_Effect	Adversary.attribute	Intended Effect
Role	Adversary.attribute	Role
Confidence	Adversary.attribute	Confidence
Handling	Adversary.tlp	
Observed_TTPs	TTP	
Associated_Actors	Adversary	
Associated_Campaigns	Campaign	

Indicators Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Indicator.attribute	Indicator Title
ID	Indicator.attribute	STIX Reference ID
Timestamp	Indicator.published_at	
Type	Indicator.attribute	Indicator Type
Description	Indicator.attribute	Description
Short Description	Indicator.attribute	Short Description
Producer	Indicator.source	

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Observable	Indicator	
Indicated_TTP	TTP	
Kill_Chain_Phases	Indicator.attribute	Kill Chain Phase
Likely_Impact	Indicator.attribute	Likely Impact
Suggested_COAs	Course of Action	
Handling	Indicator.tlp	
Confidence	Indicator.attribute	Confidence
	Indicator.attribute.source	
Related_Observables		
Related_Indicators	Indicator	
Related_Campaigns	Campaign	
	Signature	
	Signature.type = "Snort"	
	Signature.value	
	Indicator.source	
	Course of Action	
	Indicator.attribute	Start Time
	Indicator.attribute	End Time
	Indicator.published_at	

Exploit Targets Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Exploit Target.value	
ID	Exploit Target.attribute	STIX Reference ID
Description	Exploit Target.attribute	Description
Short Description	Exploit Target.attribute	Short Description
Weakness	Exploit Target.attribute	CWE ID
Weakness	Exploit Target.attribute	Weakness Description
Configuration	Exploit Target.attribute	CCE ID
Configuration	Exploit Target.attribute	Configuration Description
Configuration	Exploit Target.attribute	Configuration Short Description
Vulnerability	Exploit Target.attribute	CVE ID
Potential_COAs	Course of Action	
Related_Exploit_Targets	Exploit Target	

Observables Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
ID	Indicator.attribute	STIX Reference ID
	Indicator.attribute	Description
	Indicator.type	IP Address
	Indicator.value	
	Indicator.type	Filename

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator.value	
	Indicator.type	File Path
	Indicator.value	
	Indicator.attribute	File Size
	Indicator.attribute	File Format
	Indicator.attribute	Packer
	Indicator.type	MD5
	Indicator.type	SHA-256
	Indicator.type	SHA-1
	Indicator.type	SHA-512
	Indicator.value	
	Indicator.type	SSDEEP
	Indicator.value	
	Indicator.type	FQDN
	Indicator.value	
	Indicator.type	URL
	Indicator.value	
	Indicator.type	Email Subject
	Indicator.value	
	Indicator.type	Email Address

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator.value	
	Indicator.type	IP Address
	Indicator.value	
	Indicator.type	User-agent
	Indicator.value	
	Indicator.type	Filename
	Indicator.value	
	Indicator.type	Mutex
	Indicator.value	
	Indicator.attribute	Port
	Indicator.attribute	Protocol
	Object.Description	
	Spearphish.value	
	Indicator.type	Registry Key
	Indicator.value	
	Indicator.attribute	Hive

Campaigns Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Campaign.value	

STIX Field	ThreatQ Field Mapping	ThreatQ Name
ID	Campaign.attribute	STIX Reference ID
Description	Campaign.attribute	Description
Short Description	Campaign.attribute	Short Description
Timestamp	Campaign.started_at	
Names	Campaign.attribute	Alias
Status	Campaign.attribute	Status
Intended_Effect	Campaign.attribute	Intended Effect
Confidence	Campaign.attribute	Confidence
Activity	Campaign.attribute	Activity
Related TTPs	TTP	
Related Incidents	Incident	
Attribution	Adversary	
Associated_Campaigns	Campaign	

Courses of Action Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Course of Action.value	
ID	Course of Action.attribute	STIX Reference ID
Description	Course of Action.attribute	Description
Stage	Course of Action.attribute	Stage

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Objective	Course of Action.attribute	Objective
Objective Confidence	Course of Action.attribute	Objective Confidence
Type	Course of Action.attribute	Type
Short Description	Course of Action.attribute	Short Description
Parameter_Observables	Indicator	
Impact	Course of Action.attribute	Impact
Cost	Course of Action.attribute	Cost
Efficacy	Course of Action.attribute	Efficacy
Related_COAs	Course of Action	

Incidents Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Incident.value	
ID	Incident.attribute	STIX Reference ID
Timestamp	Incident.published_at	
Description	Incident.attribute	Description
Categories	Incident.attribute	Category
First Malicious Action	Incident.attribute	First Malicious Action
Initial_Compromise	Incident.attribute	Initial Compromise
First_Data_Exfiltration	Incident.attribute	First Data Exfiltration

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Incident_Discovery	Incident.attribute	Incident Discovery
Incident_Opened	Incident.attribute	Incident Opened
Incident_Opened	Incident.started_at	
Containment_Achieved	Incident.attribute	Containment Achieved
Restoration_Achieved	Incident.attribute	Restoration Achieved
Incident_Reported	Incident.attribute	Incident Reported
Incident_Closed	Incident.attribute	Incident Closed
Incident_Closed		
Coordinator	Incident.attribute	Coordinator
	Incident.attribute	Coordinator
Reporter	Incident.attribute	Reporter
	Incident.attribute	Reporter
Responder	Incident.attribute	Responder
	Incident.attribute	Responder
Victim	Incident.attribute	Victim
	Incident.attribute	Victim
Related Indicators	Indicator	
Related Observables	Indicator	
Leveraged_TTPs	TTP	
Intended_Effect	Incident.attribute	Intended Effect

STIX Field	ThreatQ Field Mapping	ThreatQ Name
COA_Requested	Course of Action	
COA_Taken	Course of Action	
Confidence	Incident.attribute	Confidence
Attributed_Threat_Actors	Adversary	
Discovery_Method	Incident.attribute	Discovery Method
Related_Incidents	Incident	

TTP Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	TTP.value	
ID	TTP.attribute	STIX Reference ID
Description	TTP.attribute	Description
Handling	TTP.tlp	
Kill_Chain_Phases	TTP.attribute	Kill Chain Phase
Intended_Effect	TTP.attribute	Intended Effect
	TTP.attribute	CAPEC ID
Behavior	TTP.attribute	Attack Pattern
	TTP.attribute	Attack Pattern Description
	TTP.attribute	Attack Pattern Short Description
	TTP.attribute	Malware Type

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	TTP.attribute	Malware Name
	TTP.attribute	Malware Description
	TTP.attribute	Malware Short Description
	TTP.attribute	Malware Detection Vendor
	TTP.attribute	Malware Family
	TTP.attribute	Exploit
	TTP.attribute	Exploit Description
	TTP.attribute	Exploit Short Description
Exploit_Targets	Exploit Target	
Related_TTPs	TTP	
Resources	TTP.attribute	Tool
	TTP.attribute	Tool
	TTP.attribute	Tool Type
	TTP.attribute	Tool Description
	TTP.attribute	Tool Short Description
	TTP.attribute	Infrastructure Type
	TTP.attribute	Infrastructure
	TTP.attribute	Infrastructure Short Description
	TTP.attribute	Infrastructure Description
	Indicator	

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	TTP.attribute	Persona
Victim Targeting	TTP.attribute	Victim Name
	TTP.attribute	Victim <CIQ Identity Name>
	TTP.attribute	Targeted Systems
	TTP.attribute	Targeted Information
	Indicator	

CIQ Identity Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Party Name	Object.attribute	Name
Organization Name	Object.attribute	Organization
Industry Sector	Object.attribute	Industry
Nationality	Object.attribute	Nationality
Languages	Object.attribute	Language
Address	Object.attribute	Country
Email Address	Object.attribute	E-Mail Address
Chat Handle	Object.attribute	Chat Handle
Phone	Object.attribute	Phone

STIX 2.0 Data Mappings

You can click on the icon located to top-right of this topic to expand and collapse all mapping tables below.

Attack Patterns Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Attack Pattern.Published_at	
description	Attack Pattern.Attribute	Description
external_references[]	See External References	
kill_chain_phases.[]e	See Kill Chain Table	
modified	Attack Pattern.Attribute	Modified At
name	Attack Pattern.Value	
revoked (if revoked == true)	Attack Pattern.Attribute	Revoked
labels	Attack Pattern.Attribute	Label

Threat Actors Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
aliases	Adversary	* The Adversary created will have all the same attributes and published_at as the base Attribute. All alias Adversaries will be inter-related

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Adversary.Published_At	
goals	Adversary.Attribute	Goal
labels	Adversary.Attribute	Label
modified	Adversary.Attribute	Modified At
name	Adversary.Value	
primary_motivation	Adversary.Attribute	Primary Motivation
resource_level	Adversary.Attribute	Resource Level
roles	Adversary.Attribute	Role
secondary_motivation	Adversary.Attribute	Secondary Motiv-ation
sophistication	Adversary.Attribute	Sophistication
revoked (if revoked == true)	Adversary.Attribute	Revoked
external_references[]	See External References	
personal_motivations	Adversary.Attribute	Personal Motivation

Indicators Mappings

STIX 2.0 Field	ThreatQ Field Map-ping	ThreatQ Name
created	Signature.Published_at	
description	Signature.Description	

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
external_references[]	See External References	
labels	Signature.Attribute	Label
modified	Signature.Attribute	Modified At
name	Signature.Name	ThreatQ will default to using Indicator Pattern as the signature name if a `name` is not provided.
pattern	Signature.Value	
	Signature.Type	Indicator Pattern
valid.from	Signature.Attribute	Valid From
valid.until	Signature.Attribute	Valid Until
revoked (if revoked == true)	Signature.Attribute	Revoked
kill_chain_phases.[]	See Kill Chain Table	

ThreatQ Indicator and / or Event objects based on the Observables Mapping may be derived from the `pattern` field and related back to the resulting Signature.

Identities Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
contact_information	Identity.Contact_Information	

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Identity.Published_at	
description	Identity.Description	
external_references[]	See External References	
identity_class	Identity.Attribute	Identity Class
modified	Identity.Attribute	Modified At
name	Identity.Value	
sectors	Identity.Attribute	Sector
labels	Identity.Attribute	Label
revoked (if revoked == true)	Identity.Attribute	Revoked

Observables Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Observable.Published_at	
modified	Observable.Attribute	Modified At
revoked (if revoked == true)	Observable.Attribute	Revoked
external_references	Observable.Attribute	External Reference See External References.
number_	Observable.Attribute	Number Observed

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
observed		
objects[]		Specifies Cyber Observable Objects representing this observation. See the tables below for parsing details.

Artifact Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: artifact	Indicator.Type	URL
mime_type	Indicator.Attribute	MIME Type
url	Indicator.Value	
hashes{}	Indicator.relationship	
hashes {}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
hashes {}.value	Indicator.Value	

Autonomous System Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: autonomous-system	Indicator.Type	ASN
number	Indicator.Value	

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
name	Indicator.Attribute	Name
rir	Indicator.Attribute	Regional Internet Registry

Directory Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: directory	Indicator.Type	File Path
path	Indicator.Value	
path_enc	Indicator.Attribute	Path Encoding
created	Indicator.Attribute	Created At
accessed	Indicator.Attribute	Last Accessed
contains_refs	Indicator.relationship	

Domain-Name Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: domain-name	Indicator.Type	FQDN
value	Indicator.Value	
resolves_to_refs[]	Indicator.relationship	

Email Addr Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: email-addr	Indicator.Type	Email Address

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
display_name	Indicator.Attribute	Display Name
value	Indicator.Value	
belongs_to_ref[]	Indicator.relationship	

Email Message Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: email-message	Event.Type Indicator.Type	Spearphish Email Subject
subject**	Event.Title Indicator.Value	
is_multipart	Indicator.Attribute	Is Multipart
date (if parsing as an event)* sent date (if parsing as an indicator)	Event.happened_at Indicator.Attribute	
content_type	Indicator.Attribute	Content Type
from_ref	Event.Relationship Indicator.Relationship	From
sender_ref	Event.Relationship Indicator.Relationship	Sender
to_refs	Event.Relationship Indicator.Relationship	To
cc_refs	Event.Relationship	CC

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
bcc_refs	Event.Relationship Indicator.Relationship	BCC
received_lines	Event.Attribute Indicator.Attribute	Received Lines
additional_header_fields	Event.Attribute Indicator.Attribute	Additional Header - {key}  An attribute is created for each key-value pair of the additional_header_fields object.
body	Event.Attribute Indicator.Attribute	Body
body_multipart[].body_raw_ref***	Indicator	Filename
raw_email_ref	Event.Relationship Indicator.Relationship	

* To parse an event from an email message, the email must have a **date**and **subject** field.

** To parse an indicator from an email message, the email must contain a **subject** field.

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
*** If an object in body_multipart has a body field (body_multipart[].body), an attribute is created. The attribute's name is "Body Multipart" and the attribute's value is in the format "Content Type: {body_multipart[].content_type}, Content Disposition: {body_multipart[].content_disposition}, Body: {body_multipart[].body}". Note: Parsing both an indicator and event from an email message will relate the two objects .		

File Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: file	Indicator.Type	Filename
size	Indicator.Attribute	File Size
hashes{}		
hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
hashes{}.value	Indicator.Value	
name	Indicator.Value	
name_enc	Indicator.Attribute	File Name Encoding
magic_number_hex	Indicator.Attribute	Magic Number Hex
mime_type	Indicator.Attribute	MIME Type
created	Indicator.Attribute	Created At

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
accessed	Indicator.Attribute	Last Accessed
parent_directory_ref	Indicator.Relationship	
is_encrypted	Indicator.Attribute	Encrypted
encryption_algorithm	Indicator.Attribute	Encryption Algorithm
decryption_key	Indicator.Attribute	Decryption Key
contains_refs[]	Indicator.Relationship	
content_ref	Indicator.Relationship	
extensions.archive-ext.contains_refs[]	Indicator.Relationship	
extensions.archive-ext.version	Indicator.Attribute	Archive Version
extensions.archive-ext.comment	Indicator.Attribute	Archive File Comment
extensions.ntfs-ext.sid	Indicator.Attribute	Security ID
extensions.ntfs-ext.alternate_data_streams[].hashes{}		
extensions.ntfs-ext.alternate_data_streams[].hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
extensions.ntfs-ext.alternate_data_streams[].hashes{}.value	Indicator.Value	

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
extensions.ntfs-ext.alternate_data_streams[].name	Indicator.Attribute	Alternate Data Stream Name
extensions.ntfs-ext.alternate_data_streams[].size	Indicator.Attribute	Alternate Data Stream Size
extensions.pdf-ext.version	Indicator.Attribute	PDF Specification Version
extensions.pdf-ext.is_optimized	Indicator.Attribute	PDF Is Optimized
extensions.pdf-ext.document_info_dict{}.key/value	Indicator.Attribute	Formatted as: 'PDF {key.title()}'
extensions.pdf-ext.pdfid0	Indicator.Attribute	PDF First File Identifier
extensions.pdf-ext.pdfid1	Indicator.Attribute	PDF Second File Identifier
extensions.raster-image-ext.image_height	Indicator.Attribute	Image Height
extensions.raster-image-ext.image_width	Indicator.Attribute	Image Width
extensions.raster-image-ext.bits_per_pixel	Indicator.Attribute	Image Bits Per Pixel
extensions.raster-image-ext.image_compression_algorithm	Indicator.Attribute	Image Compression Algorithm
extensions.raster-image-ext.exif_tags{}.key/value	Indicator.Attribute	Formatted as: 'Image EXIF {key.title()}'

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
extensions.windows-pebinary-ext.pe_type	Indicator.Attribute	Executable Extension Type
extensions.windows-pebinary-ext.imphash	Indicator.Attribute	Executable Imphash
extensions.windows-pebinary-ext.machine_hex	Indicator.Attribute	Target Machine Hex
extensions.windows-pebinary-ext.number_of_sections	Indicator.Attribute	PE Binary Section Count
extensions.windows-pebinary-ext.time_date_stamp	Indicator.Attribute	PE Binary Created Date
extensions.windows-pebinary-ext.pointer_to_symbol_table_hex	Indicator.Attribute	Symbol Table Hex Offset
extensions.windows-pebinary-ext.number_of_symbols	Indicator.Attribute	PE Binary Symbol Table Size
extensions.windows-pebinary-ext.size_of_optional_header	Indicator.Attribute	PE Binary Optional Header Size
extensions.windows-pebinary-ext.characteristics_hex	Indicator.Attribute	PE Binary Characteristics Hex
extensions.windows-pebinary-ext.file_header_hashes{}		
extensions.windows-pebinary-ext.file_header_hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
		Hash
extensions.windows-pebinary-ext.file_header_hashes{}.value	Indicator.Value	
extensions.windows-pebinary-ext.optional_header.magic_hex	Indicator.Attribute	PE Binary Magic Hex
extensions.windows-pebinary-ext.optional_header.major_linker_version	Indicator.Attribute	PE Binary Major Linker Version
extensions.windows-pebinary-ext.optional_header.minor_linker_version	Indicator.Attribute	PE Binary Minor Linker Version
extensions.windows-pebinary-ext.optional_header.size_of_code	Indicator.Attribute	PE Binary Code Size
extensions.windows-pebinary-ext.optional_header.size_of_initialized_data	Indicator.Attribute	PE Binary Initialized Data Size
extensions.windows-pebinary-ext.optional_header.size_of_uninitialized_data	Indicator.Attribute	PE Binary Uninitialized Data Size
extensions.windows-pebinary-ext.optional_header.address_of_entry_point	Indicator.Attribute	PE Binary Memory Address Entry Point

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
extensions.windows-pebinary-ext.optional_header.base_of_code	Indicator.Attribute	PE Binary Base Code Memory Address
extensions.windows-pebinary-ext.optional_header.base_of_data	Indicator.Attribute	PE Binary Base Data Memory Address
extensions.windows-pebinary-ext.optional_header.image_base	Indicator.Attribute	PE Binary Base Image Memory Address
extensions.windows-pebinary-ext.optional_header.section_alignment	Indicator.Attribute	PE Binary Section Alignment Bytes
extensions.windows-pebinary-ext.optional_header.file_alignment	Indicator.Attribute	PE Binary Image File Alignment Bytes
extensions.windows-pebinary-ext.optional_header.major_os_version	Indicator.Attribute	Windows OS Major Version
extensions.windows-pebinary-ext.optional_header.minor_os_version	Indicator.Attribute	Windows OS Minor Version
extensions.windows-pebinary-ext.optional_header.major_image_version	Indicator.Attribute	Image Major Version

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
extensions.windows-pebinary-ext.optional_header.minor_image_version	Indicator.Attribute	Image Minor Version
extensions.windows-pebinary-ext.optional_header.major_subsystem_version	Indicator.Attribute	Subsystem Major Version
extensions.windows-pebinary-ext.optional_header.minor_subsystem_version	Indicator.Attribute	Subsystem Minor Version
extensions.windows-pebinary-ext.optional_header.win32_version_value_hex	Indicator.Attribute	Win32 Version Hex
extensions.windows-pebinary-ext.optional_header.size_of_image	Indicator.Attribute	Image Byte Size
extensions.windows-pebinary-ext.optional_header.size_of_headers	Indicator.Attribute	PE Binary Combined Header Size
extensions.windows-pebinary-ext.optional_header.checksum_hex	Indicator.Attribute	PE Binary Checksum Hex
extensions.windows-pebinary-ext.optional_header.subsystem_hex	Indicator.Attribute	PE Binary Required Subsystem Hex

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
extensions.windows-pebinary-ext.optional_header.dll_characteristics_hex	Indicator.Attribute	DLL Characteristics Hex
extensions.windows-pebinary-ext.optional_header.size_of_stack_reserve	Indicator.Attribute	Reserved Stack Size
extensions.windows-pebinary-ext.optional_header.size_of_stack_commit	Indicator.Attribute	Stack Commit Size
extensions.windows-pebinary-ext.optional_header.size_of_heap_reserve	Indicator.Attribute	Heap Space Reserve Size
extensions.windows-pebinary-ext.optional_header.size_of_heap_commit	Indicator.Attribute	Heap Space Commit Size
extensions.windows-pebinary-ext.optional_header.loader_flags_hex	Indicator.Attribute	Loader Flags Hex
extensions.windows-pebinary-ext.optional_header.number_of_rva_and_sizes	Indicator.Attribute	Number of RVA and Sizes
extensions.windows-pebinary-ext.optional_header.hashes{}		
extensions.windows-pebinary-	Indicator.Type	MD5 / SHA-1 / SHA-

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
ext.optional_header.hashes{}.key		256 / SHA-384 / SHA-512 / Fuzzy Hash
extensions.windows-pebinary-ext.optional_header.hashes{}.value	Indicator.Value	
extensions.windows-pebinary-ext.sections[].hashes{}		
extensions.windows-pebinary-ext.sections[].hashes{}.key	Indicator.Type	MD5 / SHA-1 / SHA-256 / SHA-384 / SHA-512 / Fuzzy Hash
extensions.windows-pebinary-ext.sections[].hashes{}.value	Indicator.Value	
extensions.windows-pebinary-ext.sections[].name	Indicator.Attribute	PE Binary Section Name
extensions.windows-pebinary-ext.sections[].size	Indicator.Attribute	PE Binary Section Size
extensions.windows-pebinary-ext.sections[].entropy	Indicator.Attribute	PE Binary Section Entropy

IPv4 Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: ipv4-addr	Indicator.Type	CIDR Block (if value contains a / and does not end with /32) IP Address (if the value ends with /32, the /32 is omitted and reported as an IP Address)
value	Indicator.Value	
resolves_to_refs[]	Indicator.Relationship	
belongs_to_refs[]	Indicator.Relationship	

IPv6 Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: ipv6-addr	Indicator.Type	IPv6 Address
value	Indicator.Value	
resolves_to_refs[]	Indicator.Relationship	
belongs_to_refs[]	Indicator.Relationship	

MAC Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: mac-addr	Indicator.Type	MAC Address
value	Indicator.Value	

Mutex Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: mutex	Indicator.Type	Mutex
name	Indicator.Value	

URL Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: url	Indicator.Type	URL
value	Indicator.Value	

User Account Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: user-account	Indicator.Type	Username
user_id	Indicator.Attribute	User ID
account_login	Indicator.Value	
account_type	Indicator.Attribute	Account Type
display_name	Indicator.Attribute	Display Name
is_service_account	Indicator.Attribute	Is Service Account
is_privileged	Indicator.Attribute	Is Privileged Account
can_escalate_privs	Indicator.Attribute	Can Escalate Privileges
is_disabled	Indicator.Attribute	Is Disabled

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
account_created	Indicator.Attribute	Account Created
account_expires	Indicator.Attribute	Account Expires
password_last_changed	Indicator.Attribute	Password Last Changed
account_first_login	Indicator.Attribute	Account First Login
account_last_login	Indicator.Attribute	Account Last Login
extensions.unix-account-ext.gid	Indicator.Attribute	Account Group ID
extensions.unix-account-ext.-groups[]	Indicator.Attribute	Account Group
extensions.unix-account-ext.home_dir	Indicator.Attribute	Account Home Directory
extensions.unix-account-ext.shell	Indicator.Attribute	Account Command Shell

Windows Registry Key Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
type: windows-registry-key	Indicator.Type	Registry Key
key	Indicator.Value	
values[].name	Indicator.Attribute	Registry Name
modified	Indicator.Attribute	Registry Modified At
creator_user_ref	Indicator.Relationship	

Campaigns Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
aliases	Campaign	
created	Campaign.Published_at	
description	Campaign.Description	
first_seen	Campaign.Started_at	
last_seen	Campaign.Ended_at	
modified	Campaign.Attribute	Modified At
name	Campaign.Value	
objective	Campaign.Objective	
revoked (if revoked == true)	Campaign.Attribute	Revoked
external_references[]	See External References	
labels	Campaign.Attribute	Label

Courses of Action Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Course of Action.Published_at	
modified	Course of Action.Attribute	Modified At
name	Course of Action.Value	
description	Course of Action.Description	
action		

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
revoked (if revoked == true)	Course of Action.Attribute	Revoked
external_references[]	See External References	
labels	Course of Action.Attribute	Label

Intrusion Sets Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
aliases	Intrusion Set	
created	Intrusion Set.Published_at	
description	Intrusion Set.Description	
first_seen		
goals	Intrusion Set.Attribute	Goal
modified	Intrusion Set.Attribute	Modified At
name	Intrusion Set.Value	
primary_motivation	Intrusion Set.Attribute	Primary Motivation
resource_level	Intrusion Set.Attribute	Resource Level
secondary_motivations	Intrusion Set.Attribute	Secondary Motivation
external_references[]	See External References	
revoked (if revoked == true)	Intrusion Set.Attribute	Revoked

Malware Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Malware.Published_at	
description	Malware.Description	
kill_chain_phases.[]	See Kill Chain Table	
labels	Malware.Attribute	Label
modified	Malware.Attribute	Modified At
name	Malware.Value	
external_references[]	See External References	
revoked (if revoked == true)	Malware.Attribute	Revoked

Tools Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Tool.Published_at	
modified	Tool.Attribute	Modified At
labels	Tool.Attribute	Label
name	Tool.Value	
revoked (if revoked == true)	Tool.Attribute	Revoked
external_references[]	See External References	
description	Tool.Description	
kill_chain_phases.[]	See Kill Chain Table	
tool_version	Tool.Attribute	Tool Version

Reports Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
created	Report.Published_at	
modified	Report.Attribute	Modified At
name	Report.Value	
description	Report.Description	
labels	Report.Attribute	Label
object_refs	Report.Relationship.Link	
external_references[]	See External References	
revoked (if revoked == true)	Report.Attribute	Revoked

Sightings Mapping

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
count	Event.Attribute	Count
created	Event.published_at	
first_seen	Event.happened_at	
last_seen	Event.Attribute	Last Seen
observed_data_refs	Event.relationship.link	
sighting_of_ref	Event.relationship.link	
where_sighted_refs	Event.relationship.link	
revoked (if revoked == true)	Object.attribute	Revoked
	Event.name	STIX Sighting

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
	Event.type	Sighting
external_references[]	See External References	
modified	Event.Attribute	Modified

External References

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
Object.external_references[].source_name	Object.Attribute	External Reference*
Object.external_references[].external_id	Object.Attribute	External Reference*
Object.external_references[].description	Object.Attribute	External Reference*
Object.external_references[].url	Object.Attribute	External Reference*
* Formatted as: {source_name} ({external_id}): {description} - {url}		

Kill Chain Phrases

STIX 2.0 Field	ThreatQ Field Mapping	ThreatQ Name
kill_chain_phases[].kill_chain_name	Object.Attribute	Kill Chain Name
kill_chain_phases[].phase_name	Object.Attribute	Kill Chain Phrase

Parsing a STIX File for Indicators

ThreatQ allows you to upload a STIX file or insert STIX data to parse. for indicators.

To parse a STIX file for indicators:

1. Click on the **Create** button, located at the top of the dashboard and select **STIX Parser** under the *Import* heading.

   The Parse For Intelligence dialog box will load.

2. Do one of the following:

   - Drag your file(s) into the left pane.
   - Click on **Click to Browse**, and locate the file you wish to upload.
   - Copy/paste the content in the right pane.

3. Select or clear the **Normalize URL Indicators** check box. See Indicator URL Normalization for more information.
4. Click **Next Step**.
5. Enter an optional **Name**.
6. Select a **Source** from the dropdown menu provided.

   You can also click on **Add a New Source** if the desired source is not listed in the dropdown menu

7. Select any optional **Attributes** to be applied.
8. Optionally, enter a comment.
9. Optionally, use the **Add relationships** search field to add object relationships.
10. Optionally, add any desired **Tags**.

If at any point, you wish to abandon the import, click **Cancel**.

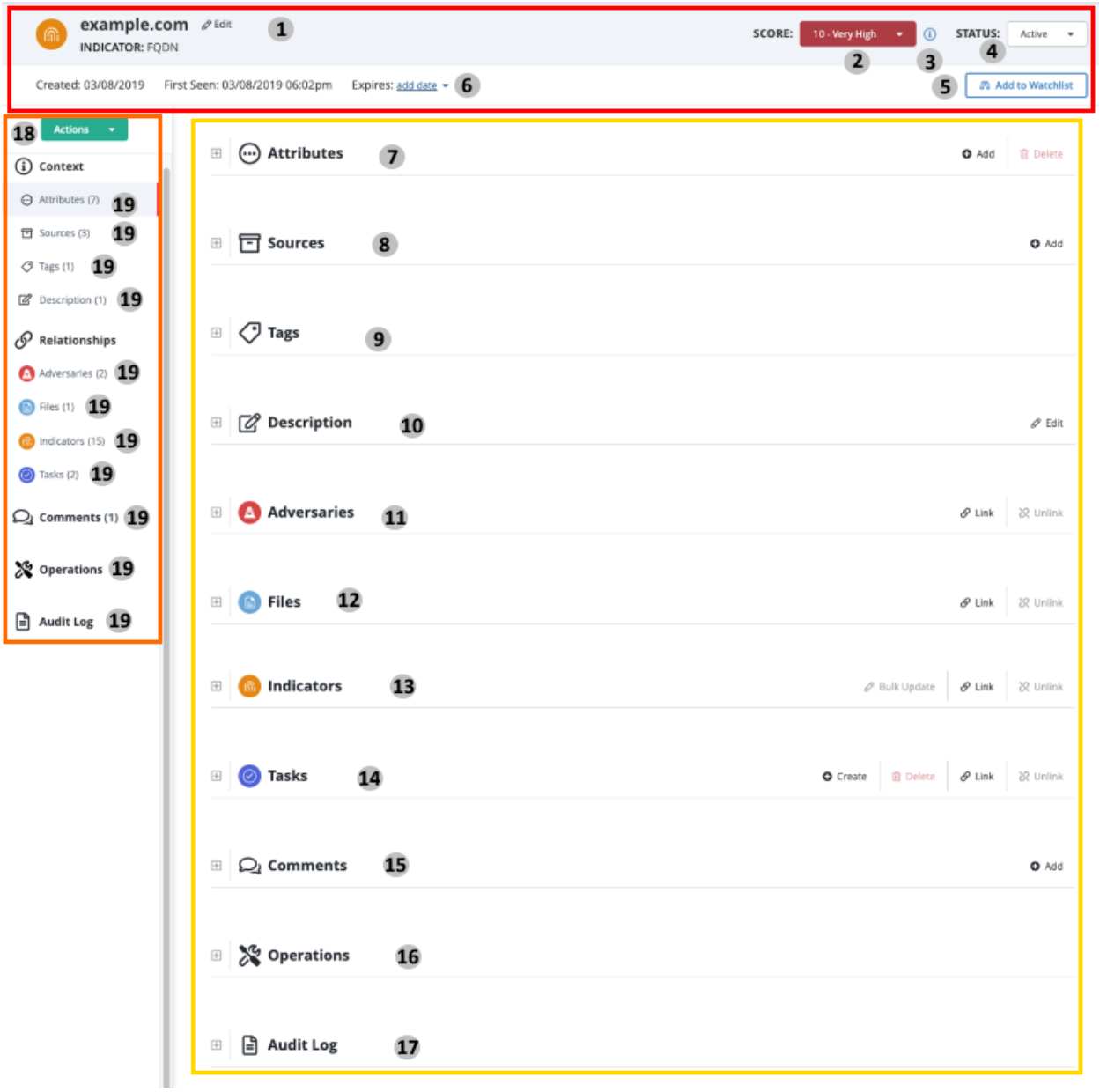
11. Click **Apply**.

    New objects will become available in the Threat Library.

Object Details Page

You can click on an object within the ThreatQ application to access its details page. The Object Details page provides you with an in-depth look at an individual object. You can enter comments for others to view, link related objects, and view an audit log of all activity associated with the object.

Specific objects, such as Indicators, will display additional information such as the indicator's status, score, and expiration data.



Items marked with an * in the Object Details Legend indicate an option only available to specific object types.

Object Details Page Legend			
Header Section			
Number	**Field**	**Description**	**Reference**

Object Details Page Legend			
1	Edit Object Link	The Edit link allows you to edit specific details about an object. Edit fields will differ based on the type of object.	• Editing Adversaries • Editing Events • Editing Files • Editing Indicators
2	Score Selection* *Applies to Indicator Object Types Only*	The Score Selection dropdown allows you to override an indicator's score set by the scoring algorithm.	• Overriding the Scoring Algorithm with a Manual Score
3	Scoring Influence* *Applies to Indicator Object Types Only*	You can click on the icon to review the criteria utilized by the application's scoring algorithm to generate the Indicator's score.	• Configure Indicator Scoring • Building a Scoring Algorithm
4	Status* *Applies to Indicator Object Types Only*	The Status dropdown menu allows you to manually set the status of an indicator. Default statuses include: Active, Expired, Indirect, Review, and Whitelisted.	• Indicator Status
5	Add to Watchlist	The Watchlist toggle button allows you to add and remove the object from the Watchlist widget.	• Configuring the Watchlist
6	Expiration* *Applies to Indicator Object Types Only*	The Expire link allows you to set an expiration date for the indicator, protect from auto-expiration policies, and remove an existing set expiration date.	• Indicator Expiration • Automatic Expiration and Policies
Details Section			
Number	**Pane**	**Description**	**Reference**
7	Attributes	The Attributes pane displays	• Attributes Pane

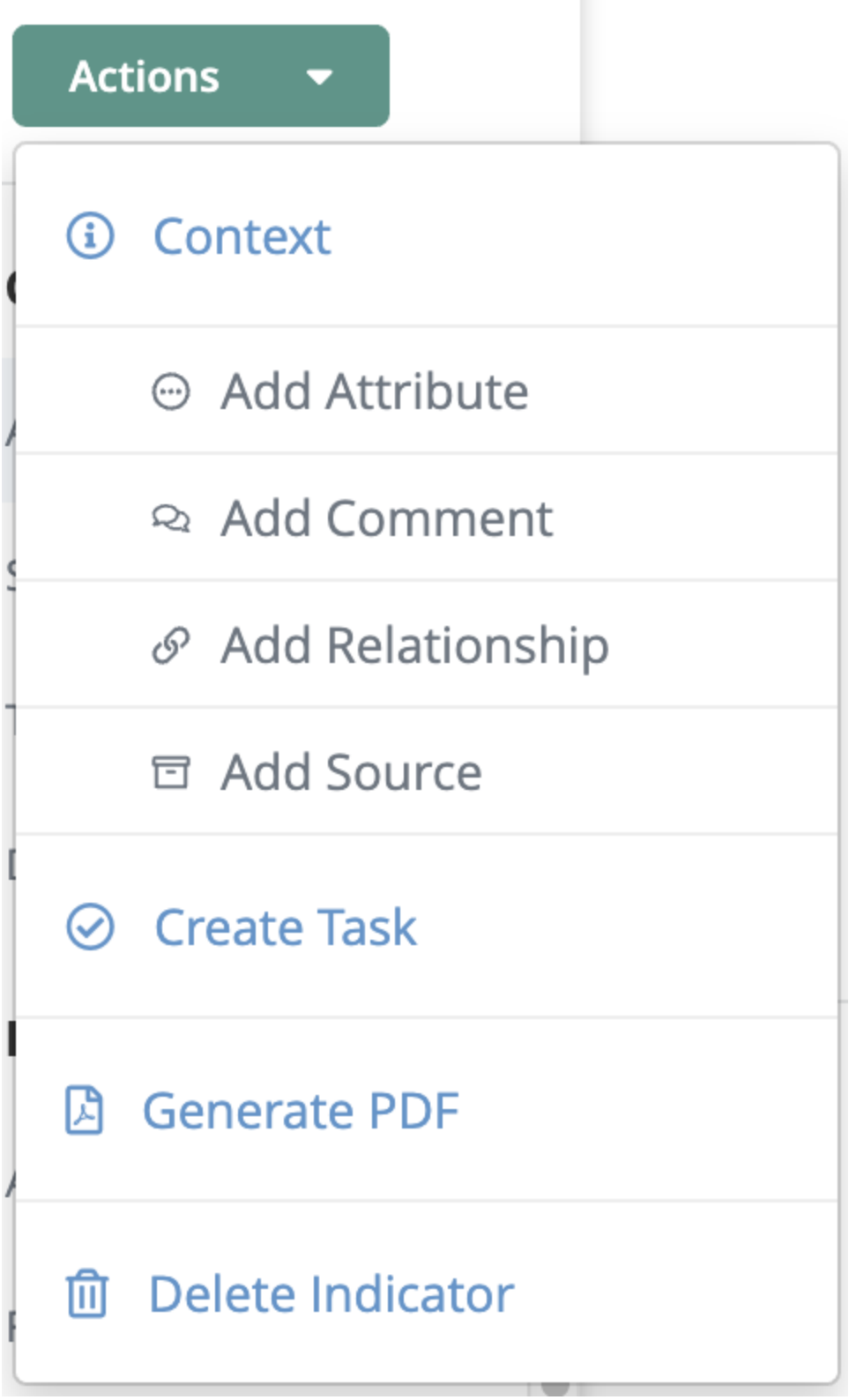
Object Details Page Legend			
		attributes associated with the object. You can Add, Edit, and Delete attributes found in this section.	
8	Sources	The Sources pane displays sources associated with the object. You can Add additional sources to an object.	• Adding a Source to an Object
9	Tags	The Tags pane displays tags associated with the object. You can Add and Delete tags found in this section.	• Managing Tags
10	Description	The Description pane allows you to add general information about the object.	• Description Pane
11	Adversaries	The Adversaries pane displays adversaries associated with the object.	• Adversaries Pane
12	Files	The Files pane displays files associated with the object.	• Files Pane
13	Indicators	The Indicators pane displays indicators associated with the object.	• Indicators Pane
14	Tasks	The Tasks pane displays tasks associated with the object.	• Tasks Pane
10	Related Objects	There are several different related panes depending on the types of objects linked to the object. You can use these panes to view and add/remove linked indicators,	• Relationships Panes

Object Details Page Legend			
		files, signatures, events, adversaries, tasks, and investigations.	
15	Comments	The Comments pane allows you to record comments about the object for other users to read and reference.	• Comments Pane
16	Operations	The Operations pane allows you to associate third-party attributes and related indicators to the indicator. **Note:** This options requires the installation of Operations. See the Operations Overview topic for more details.	• Operations Overview • ThreatQ Operations Development Guide
17	Audit Log	The Audit Log panel displays all actions and changes made to an Object.	• Common Enrichment and Audit Log Questions
Left-Hand Navigation			
Number	**Field**	**Description**	**Reference**
18	Action Menu	The Actions menu allows you to execute the following actions for an object: • Add a New Attribute • Add a New Comment • Create a Task • Generate a Report • Add a Relationship • Add a Source • Delete Object	• Actions Menu
19	Details Navigation	This allows you to jump to a par-	N/A

Object Details Page Legend			
	Tabs	ticular pane on the Object Details page.	

Actions Menu

The Action Menu, located on the left-hand of the Object Details page, allows users to quickly execute system object processes.



Actions Include:

Action	Function	Reference
Add Attribute	Brings up the Add Details dialog box to add an attribute to the object.	• Adding an Attribute to an Object
Add Comment	Creates a new text box entry in the comment pane.	• Adding Comments
Add Relationship	Brings up the Add Relationships dialog box to link other system objects to the object.	• Linking Adversaries • Linking Events • Linking Files • Linking Indicators • Linking Signatures • Linking Tasks
Add Source	Brings up the Add Details dialog box to add a source to the object.	• Adding a Source to an Object
Create Task	Opens up the Add Task dialog box.	• Assigning a Task
Generate Report	Generates a PDF report of the object.	• Generating Reports
Delete Object	Delete the system object.	N/A

Context Panes

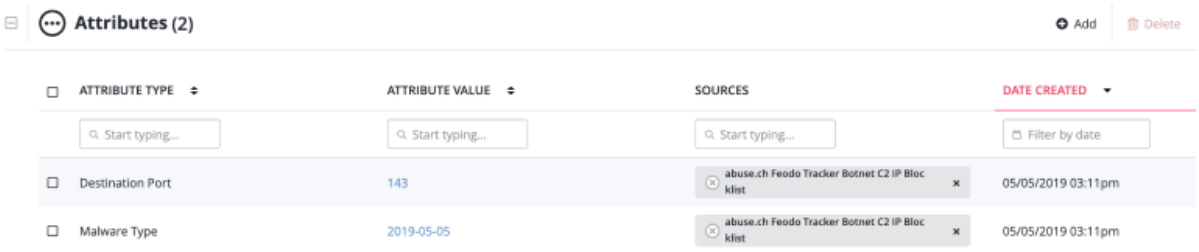
The Context section of the object details page displays attributes, sources, and tags associated with the system object.

Related Topics:

- Attributes Pane
- Adding a Source to an Object
- Managing Tags
- Description Pane

Attributes Pane

The Attributes Pane displays any attributes associated with the system object. You can review attribute details as well as add and remove attributes from this pane.



Related Topics:

- Adding an Attribute to an Object
- Deleting an Attribute
- Deleting an Attribute Source

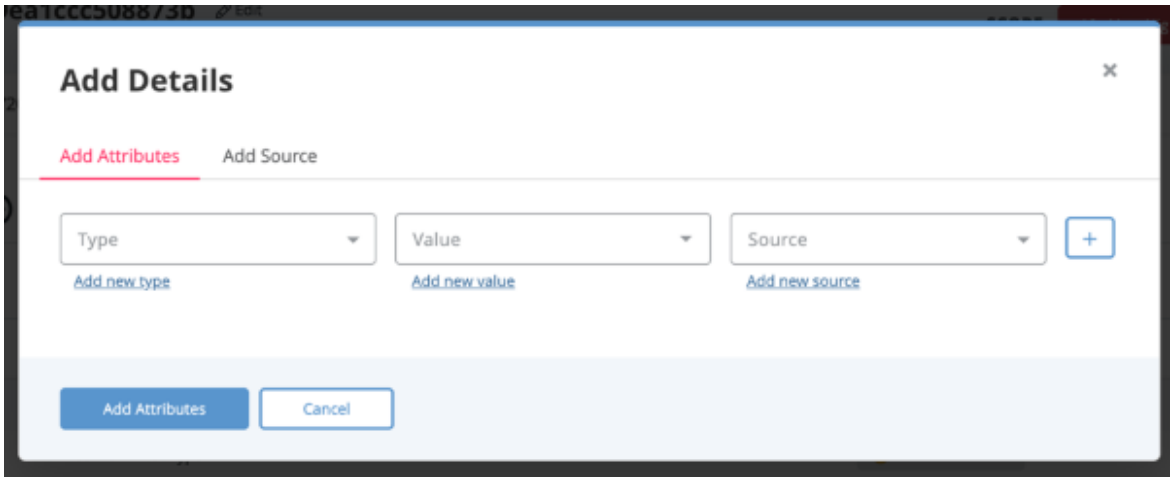
Adding an Attribute to an Object

You can link adversaries to a system object.

To add an attribute:

1. Locate the Attributes pane on the object details page.
2. Click on the **+ Add Details** link located to the top-right.

   The Add Details dialog box opens with the Add Attributes tab selected by default.



3. Select an **Attribute Type** from the Attributes dropdown or enter a new type.
4. Select an existing **Attribute Value** from the dropdown or enter a new value.
5. Select a **Source** from the dropdown or enter a new source.

   You can select the **+** icon to add additional attributes.

6. Select **Add Attributes**.

Deleting an Attribute

You can delete an attribute from the object details page.

To delete an attribute:

1. Locate the Attributes pane on the object details page.
2. Select the checkbox next to the attribute to delete.

   You can select more than one attribute to delete

3. Select **Delete**.

   The confirmation dialog box opens.

4. Select **Delete Attributes**.

Deleting an Attribute Source

You can delete an attribute's source from the object details page.

To delete an attribute source:

1. Locate the Attributes pane on the object details page.

2. Select the **X** next to the attribute's source.

   The confirmation dialog box opens.

3. Select **Delete Attribute Source**.

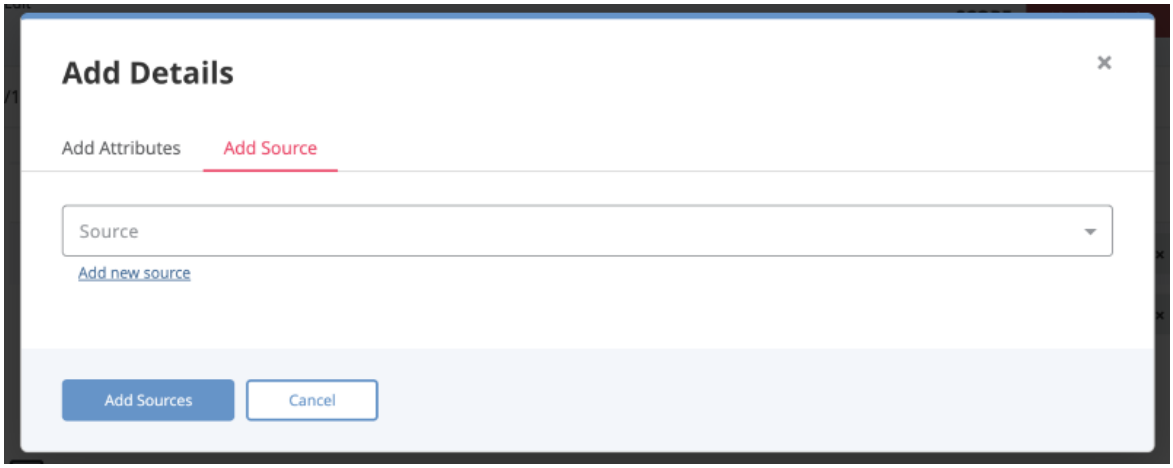
Adding a Source to an Object

You can add sources to a system object in its details pane.

To add a source:

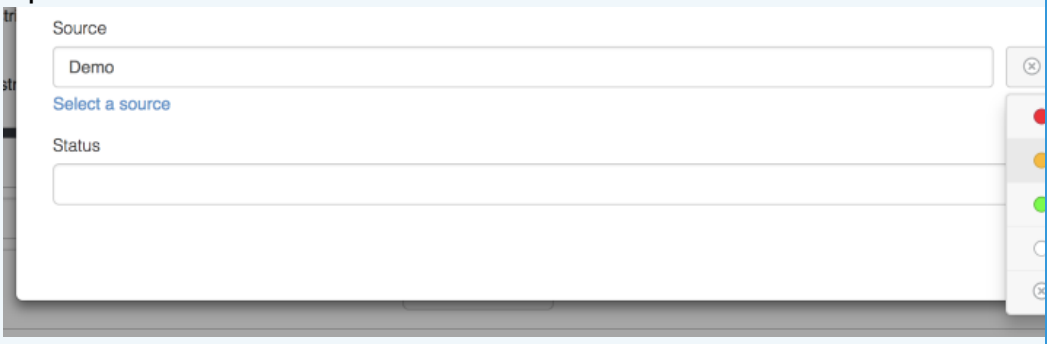
1. Locate the Sources pane on the object details page.
2. Click on the **+ Add** link located to the top-right.

   The Add Details dialog box opens with the Add Source tab selected by default.



3. Select a **Source** from the dropdown provided. If TLP is enabled, you can override the source-default TLP designation.

You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP designation light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP schema.



4. Select **Add Sources**.

Managing Tags

You can add and remove tags in the Tags pane on the object details page.

To add a tag:

1. Locate the Tags pane on the object details page.
2. Select the Tags text field and enter the tag.
3. Press **[Enter]** or **[Return]**.

Repeat steps 2-3 to add additional tags.

To delete a tag:

1. Locate the Details pane on the object details page.
2. Select the **X** next to the tag to delete.

Description Pane

The Description Pane section of the object details page allows you to add a description for the system object.

To update the Description pane:

1. Locate the Description pane on the object details page.
2. Select **Edit**.
3. Make the required changes and select **Save**.

Relationships Panes

The Relationship section of the object details page displays other system objects that have been related to the current object.

You can link/unlink system objects from relationship panes and perform bulk updates (related indicators pane only). You can click on a related object to navigate to its object details page.

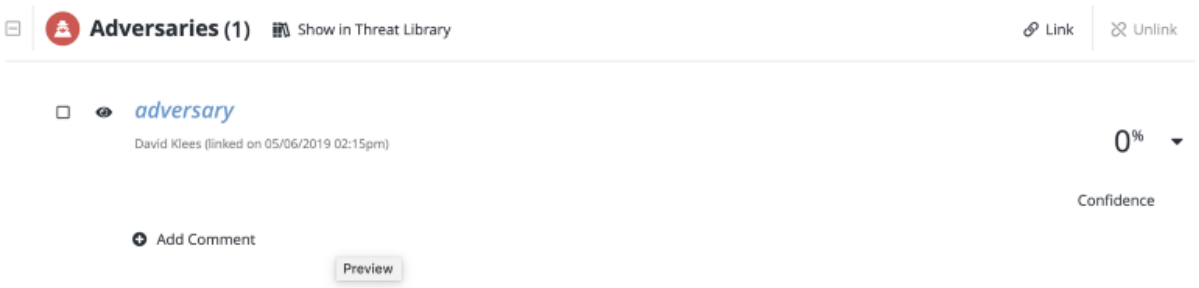
Relationships panes will only appear if a system object is already related to the object. Use the **Actions** button to relate the initial object: **Actions > Add Relationship**.

Related Topics:

- Indicators Pane
- Adversaries Pane
- Files Pane
- Investigations Pane
- Signatures Pane
- Events Pane

Adversaries Pane

The Adversaries Pane allows you to link and unlink adversary to an object. You can also add comments and adjust the adversary's confidence level. You can click on the Show in Threat Library link to view the related adversaries in the Threat Library or on a specific adversary name to open its object details page.



The Adversary pane will only load if there is an existing adversary linked to the object. Click on the **Action Menu** and select **Add Relationship** to add the first adversary.

Related Topics:

- Linking Adversaries
- Configuring Confidence Level
- Commenting on Related Adversaries
- Unlinking Related Adversaries

Linking Adversaries

You can link adversaries to a system object.

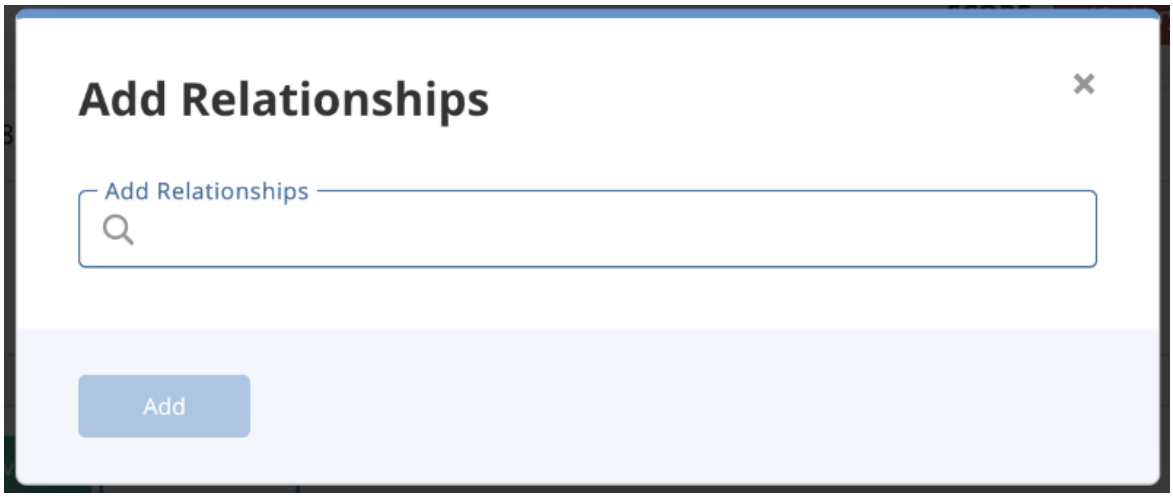
To link an adversary:

1. Locate the Adversaries pane on the object details page.

   The Adversary pane will only load if there is an existing adversary linked to the object. Click on the **Action Menu** and select **Add Relationship** to add the first adversary.

2. Select the Link icon.

   The Add Relationships dialog box opens.



3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple adversaries.

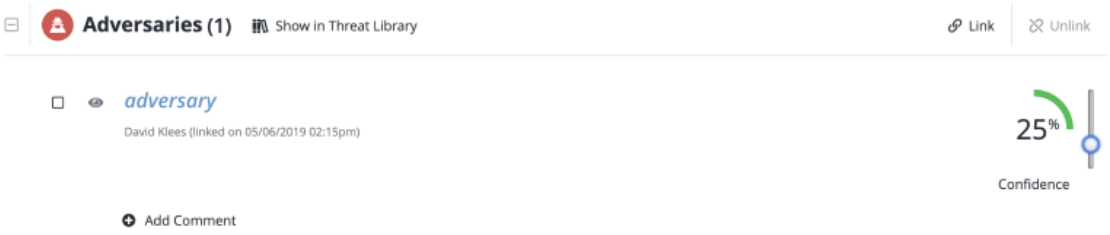
4. Click **Add**.

Configuring Confidence Level

You can configure a related adversary's confidence level from the Adversaries pane.

To configure the confidence level of a related adversary:

1. Locate the Adversaries pane on the object details page.
2. Click the dropdown arrow to the right of the adversary, and slide the scale to the desired confidence level.



The confidence level can be set to 0, 25, 50, 75, and 100.

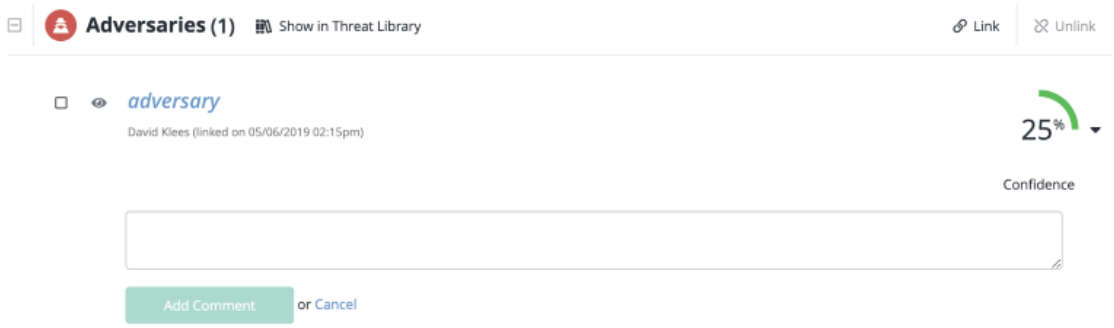
The displayed confidence level will be modified to reflect your selection.

Commenting on Related Adversaries

You can add, edit, and remove comments to related adversaries.

To add a comment to a related adversary:

1. Locate the Adversaries pane on the object details page.
2. Select **Add a Comment**.
   The Comments text field opens.



3. Enter a comment.
4. Click **Add Comment**.

To edit a related adversary comment:

1. Locate the Related Adversaries pane on the object details page.
2. Select **Edit** under the comment to update.
3. Update the comment.
4. Click **Save Changes**.

To delete a related adversary comment:

1. Locate the Related Adversaries pane on the object details page.
2. Select **Delete** under the comment to update.
   A confirmation dialog box opens.

3. Select **Delete Comment**.

Unlinking Related Adversaries

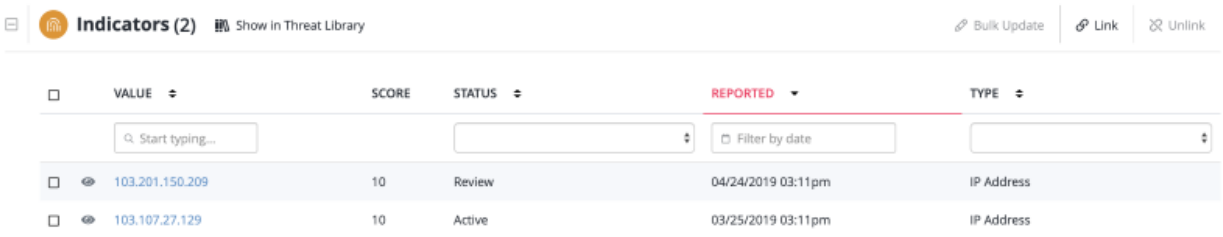
You can unlink related adversaries for an object.

To unlink related adversaries:

1. Locate the Adversaries pane on the object details page.
2. Select the checkbox(es) next to the adversary(ies) to unlink.
3. Select the Unlink icon.

Indicators Pane

The Indicators Pane allows users to link and unlink indicators to an object as well as perform a bulk update to selected linked indicators.



The Indicators pane will only load if there is an existing indicator linked to the object. Click on the **Action Menu** and select **Add Relationship** to add the first indicator.

Related Topics:

- Linking Indicators
- Performing Bulk Updates to Related Indicators
- Unlinking Related Indicators

Linking Indicators

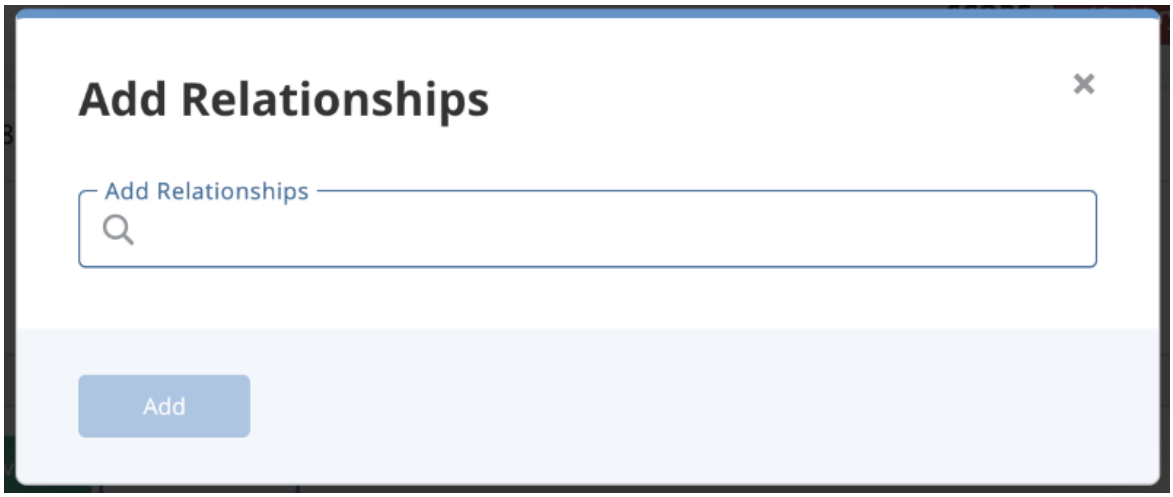
You can link indicators to a system object.

To link an indicator:

1. Locate the Indicators pane on the object details page.

2. Select Link icon.

   The Add Relationships dialog box opens.



3. Use the supplied text field to select an indicator.

   Repeat Step 3 to select multiple indicators.

4. Click **Add**.

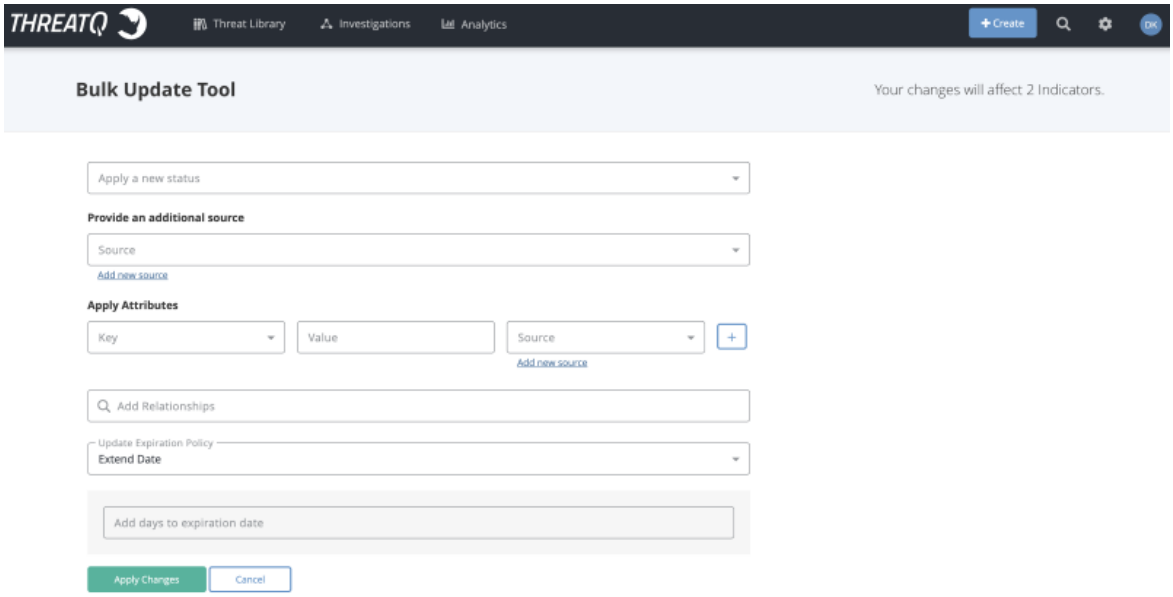
Performing Bulk Updates to Related Indicators

You can perform bulk updates to linked indicators listed in the Indicators pane of an object.

To perform a bulk update:

1. Locate the Indicators pane on the object details page.
2. Select the checkbox(es) next to the indicator(s) to update.

3. Select the Bulk Update icon.



The Bulk Update form loads.

4. Select the desired changes and click **Apply Changes**.

Unlinking Related Indicators

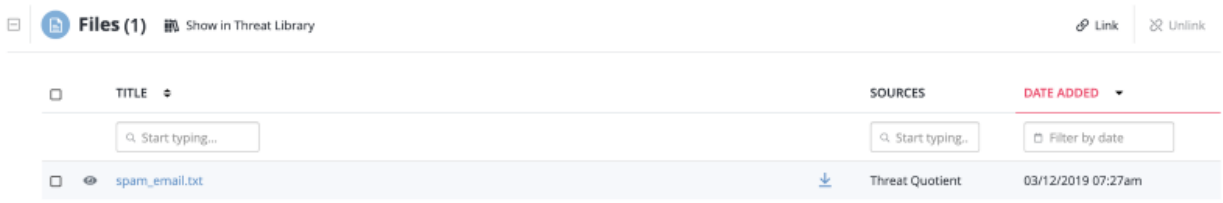
You can unlink related indicators for an object.

To unlink related indicators:

1. Locate the Indicators pane on the object details page.
2. Select the checkbox(es) next to the indicators to unlink.
3. Select the Unlink icon.

Files Pane

The Files Pane allows you to link and unlink files to an object.



You can view a quick summary of the file by clicking the on the eye icon to the left of the file name or click on the name itself to navigate to its object details page. You can click on the **Show in Threat Library** link to view the related events in the Threat Library or download a copy of the file by clicking on the ⬇ icon .

The Files pane will only load if there is an existing file linked to the object. Click on the **Action Menu** and select **Add Relationship** to add the first file.

Related Topics:

- Linking Files
- Unlinking Related Files

Linking Files

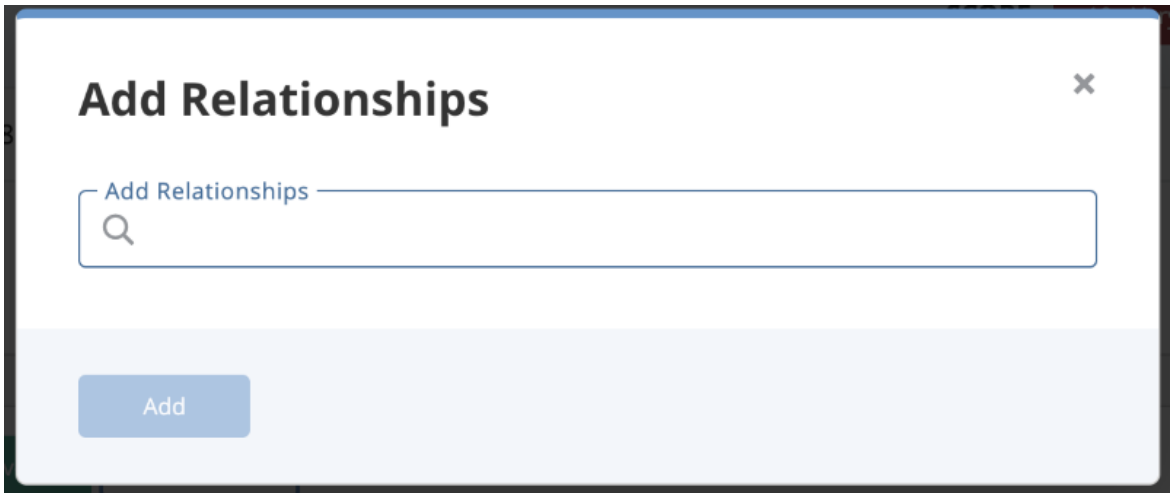
You can link Files to a system object.

To link a file:

1. Locate the Files pane on the object details page.

2. Select Link icon.

   The Add Relationships dialog box opens.



3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple files.

4. Click **Add**.

Unlinking Related Files

You can unlink related files for an object.

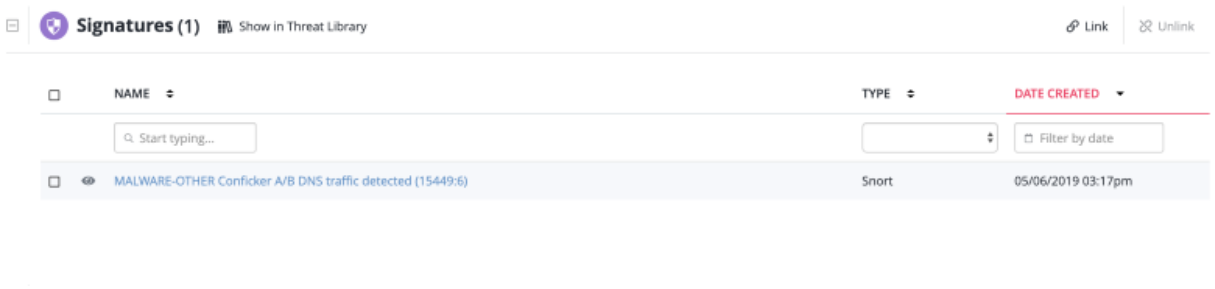
To unlink related files:

1. Locate the Files pane on the object details page.
2. Select the checkbox(es) next to the files to unlink.
3. Select the Unlink icon.

Signatures Pane

The Signatures Pane allows you to link and unlink signature to an object. You can click on the **Show in Threat Library** link to view the related signatures in the Threat Library or on a

specific signature name to open its object details page.



The Signatures pane will only load if there is an existing signature linked to the object. Click on the **Action Menu** and select **Add Relationship** to add the first signature.

Related Topics:

- Linking Signatures
- Unlinking Related Signatures

Linking Signatures

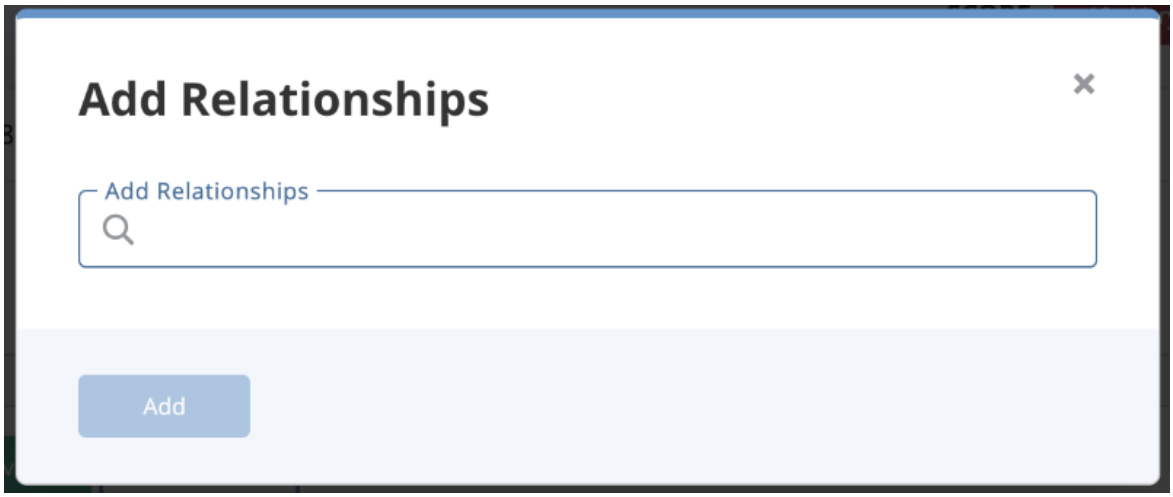
You can link Signatures to a system object.

To link a file:

1. Locate the Signatures pane on the object details page.

2. Select Link icon.

   The Add Relationships dialog box opens.



3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple signatures.

4. Click **Add**.

Unlinking Related Signatures

You can unlink related signatures for an object.

To unlink related indicators:

1. Locate the Signatures pane on the object details page.
2. Select the checkbox(es) next to the signatures to unlink.
3. Select the Unlink icon.

Investigations Pane

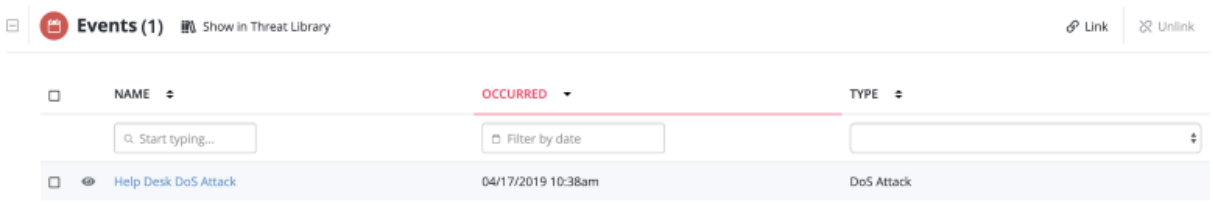
ThreatQ Investigations requires a separate license.

The Related Investigations pane displays any ThreatQ Investigation related to the object. Adding and removing an object to an investigation is controlled through the Investigations interface.

You can click on the investigation to open ThreatQ Investigations.

Events Pane

The Events Pane allows you to link and unlink events to a system object. You can click on the **Show in Threat Library** link to view the related events in the Threat Library or on a specific event name to open its object details page.



The Events pane will only load if there is an existing adversary linked to the object. Click on the **Action Menu** and select **Add Relationship** to add the first event.

Related Topics:

- Linking Events
- Unlinking Related Events

Linking Events

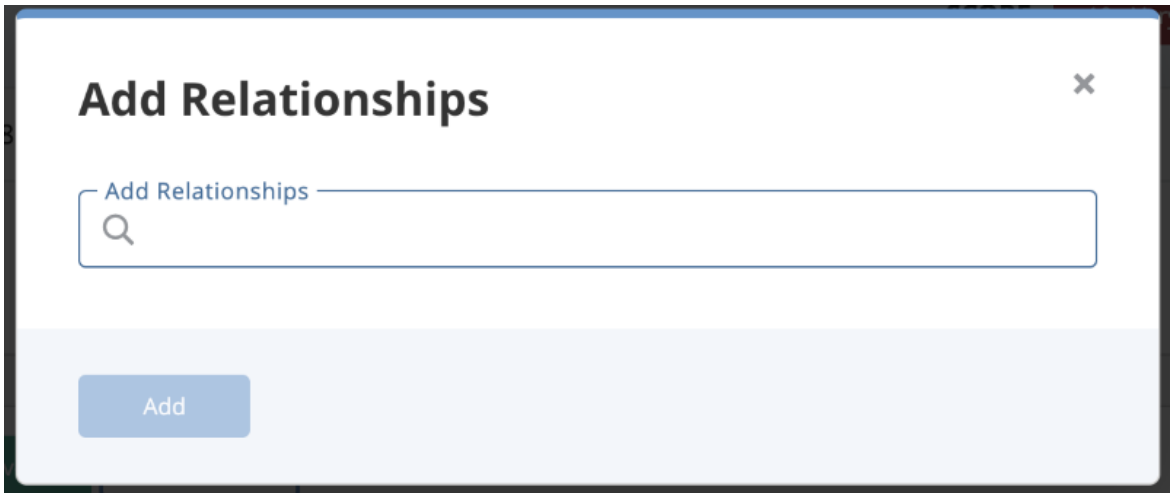
You can link events to a system object.

To link an event:

1. Locate the Events pane on the object details page.

2. Select Link icon.

   The Add Relationships dialog box opens.



3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple events.

4. Click **Add**.

Unlinking Related Events

You can unlink related events for an object.

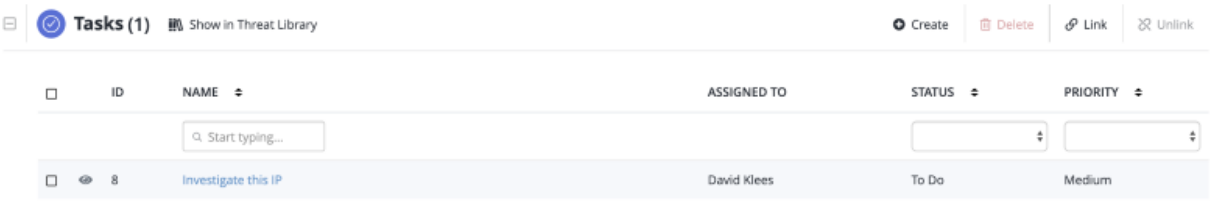
To unlink related events:

1. Locate the Events pane on the object details page.
2. Select the checkbox(es) next to the event(s) to unlink.
3. Select Unlink icon.

Tasks Pane

The Tasks Pane allows you to create, link, unlink, and delete tasks associated with an object. You can click on the **Show in Threat Library** link to view the related tasks in the Threat Library or on a specific task name to open its object details page. You can also view

a quick summary of the task by clicking the on the eye icon to the left of the task name.



The Tasks pane will only load if there is an existing task linked to the object. Click on the **Action Menu** and select **Create Task** to add the first task.

Related Topics:

- Linking Tasks
- Unlinking Related Tasks
- Deleting Related Tasks

Linking Tasks

You can link Tasks to a system object from its object details page.

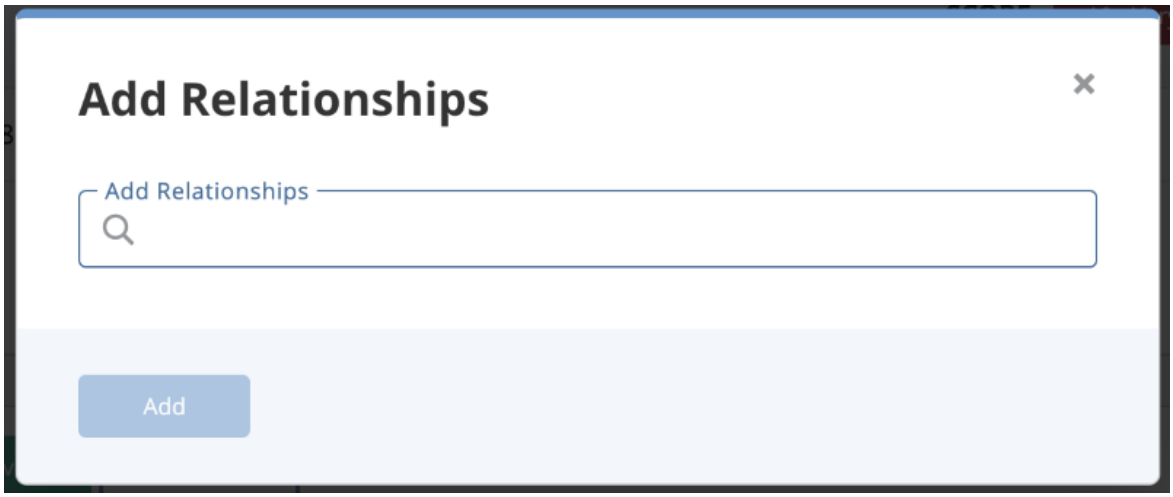
You can also related a task to a system object while creating a task.

To link a task:

1. Locate the Tasks pane on the object details page.

2. Select the Link icon.

   The Add Relationships dialog box opens.



3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple files.

4. Click **Add**.

Unlinking Related Tasks

You can unlink related tasks for an object.

To unlink related tasks:

1. Locate the Tasks pane on the object details page.
2. Select the checkbox(es) next to the files to unlink.
3. Select the Unlink icon.

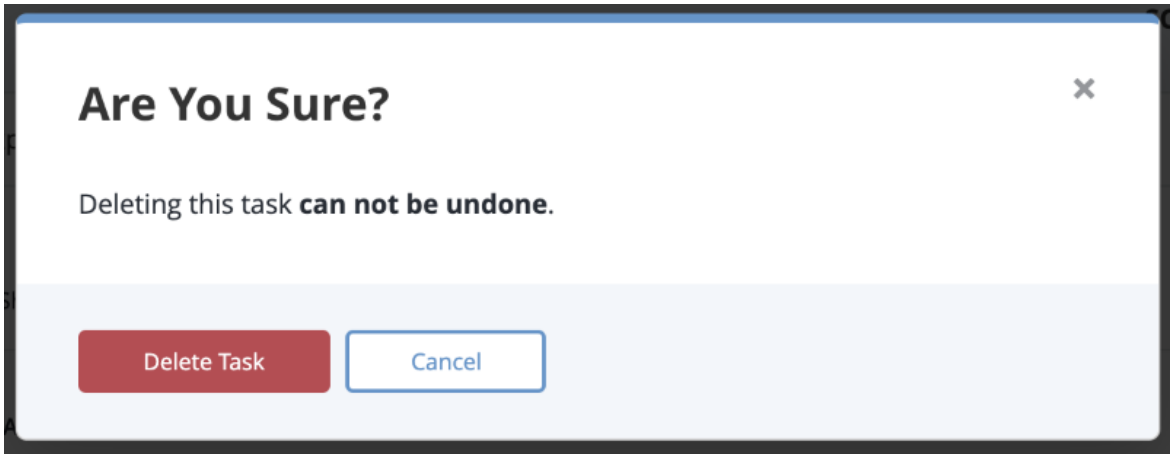
Deleting Related Tasks

You can delete Tasks related to a system object from its object details page.

To delete a task:

1. Locate the Tasks pane on the object details page.
2. Select the checkbox next to the task to delete.
3. Select the Delete icon.

   A confirmation dialog box opens.



4. Select **Delete Task**.

Comments Pane

The Comments pane allows users to record comments about the system object for other users to see.

The following functions can be performed:

- Adding Comments
- Editing Comments
- Deleting Comments

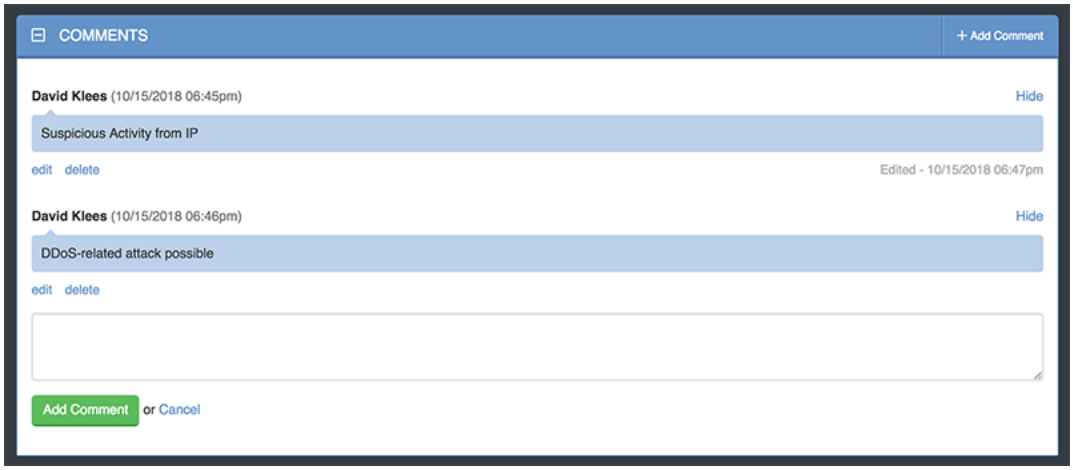
Adding Comments

Users can also click on the **Actions** menu and select the **Comment** option.

From the Object Details page:

1. Click on the expand icon to expand the Comments pane.
2. Click on the **Add Comment** link located at the top-right and lower-left of the pane.

   The new comment text box opens.



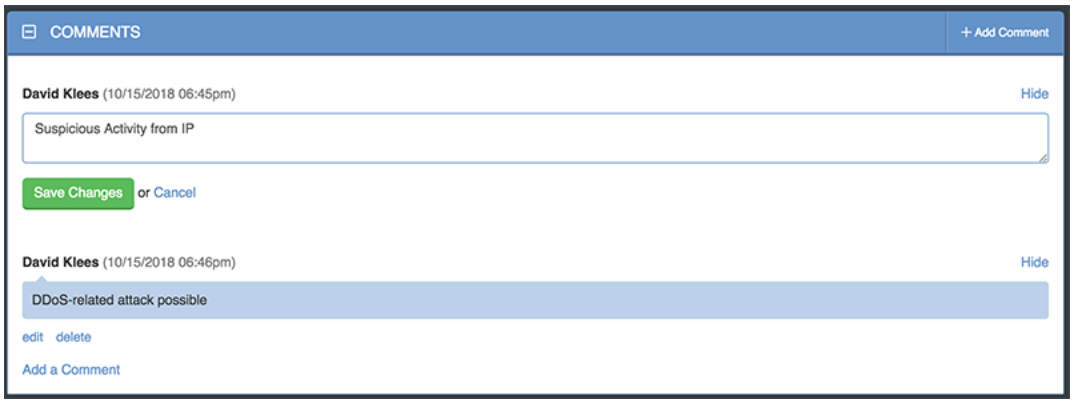
3. Enter a comment.
4. Click on the **Add Comment** button.

Editing Comments

From the Object Details page:

1. Click on the expand icon to expand the Comments pane.
2. Click on the **Edit** link located beneath the comment to update.

   The edit comment text box opens.



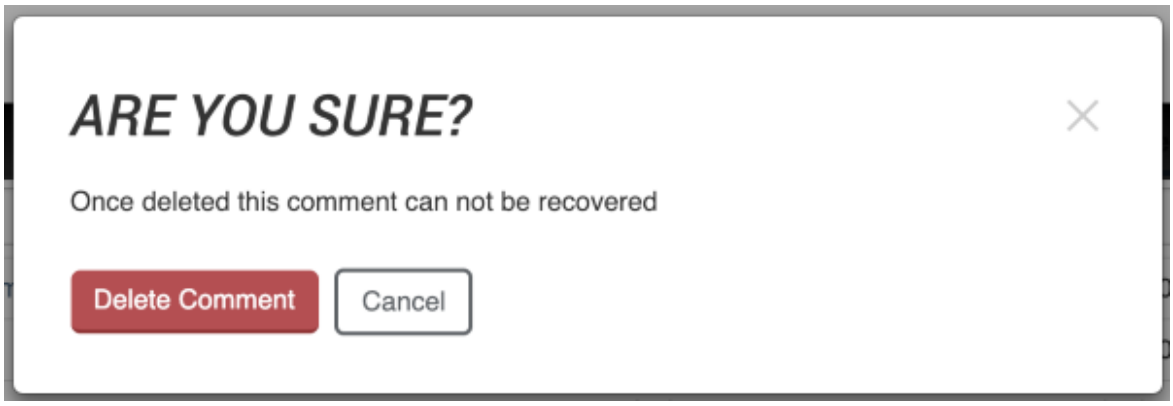
3. Edit the comment.
4. Click on the **Save Changes** button.

Deleting Comments

From the Object Details page:

1. Click on the expand icon to expand the Comments pane.
2. Click on the **Edit** link located beneath the comment to update..

   The delete confirmation dialog text box opens.



3. Click on the **Delete Comment** button.

Analytics

The Analytics tab provides a summary view of Adversary, Event, File, and Indicator Object Types.

Search filters are not available for these views nor can you modify the types of columns used. Use the Advanced Search to utilize these options.

Analytics pages include:

- Adversaries
- Events
- Files
- Indicators

Adversaries

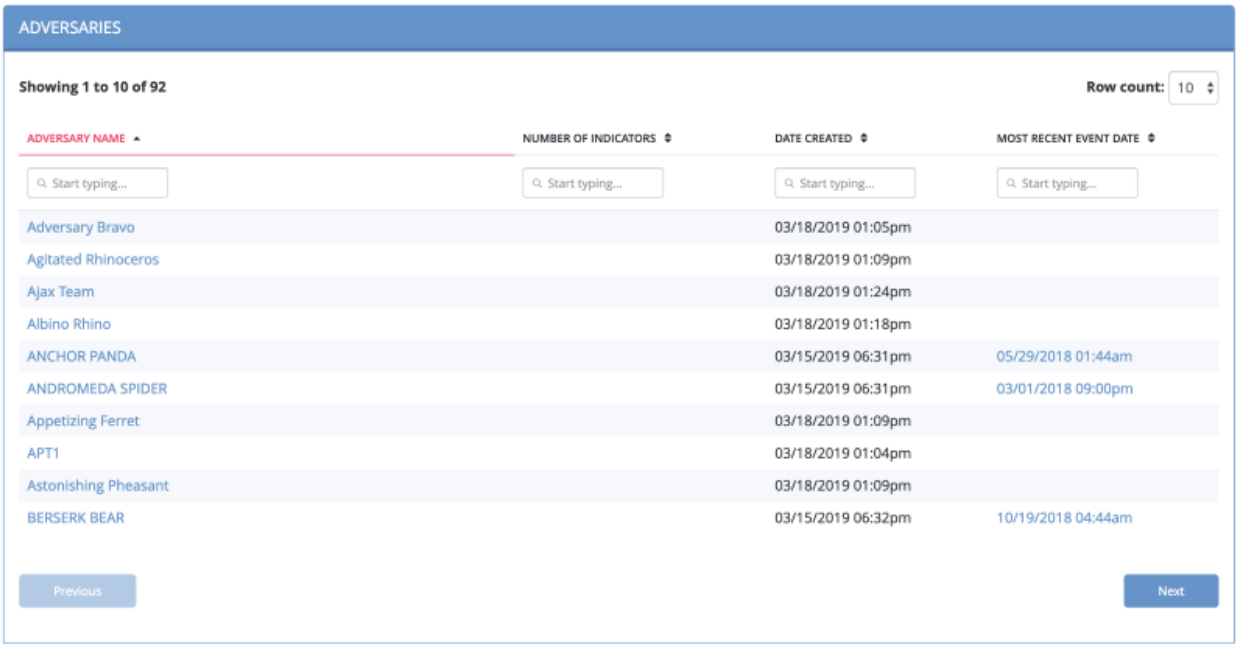
The Adversaries page provides an overview of all the adversaries within ThreatQ as well as overlapping use of specific indicators.

There are three sections:

- Adversaries Summary Table
- Adversaries Overlap Table.
- Indicator Distribution Pie Chart

Adversaries Summary Table

The Adversaries Summary table lists adversaries by name, number of indicators, date created, and the most recent event date associated with the adversary.



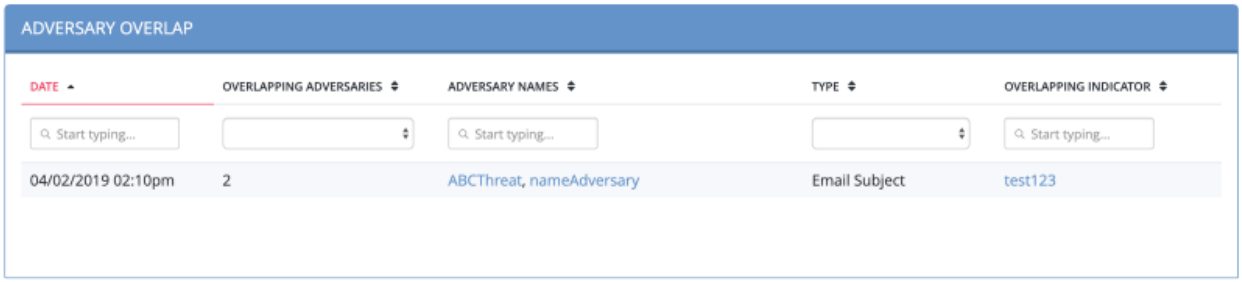
The following functions are available:

Function	Details
Opening the Adversary Details page for an adversary	1. Click the name in the Adversary Name column.
Performing a search for related indicators	1. Click the number in the Number of Indicators column to set the adversary name as a search criterion and open the Advanced Search page.
Opening the Event Details page for an adversary event	1. Click the date in the Most Recent Event Date to open the Event Details page.
Changing the number of entries displayed in the table	1. Click the paging batch option located to the bottom-right of the table.
Sorting the table by a	1. Click the column header. To reverse the column sorting

Function	Details
column	order, click the header a second time.
Searching within the Adversary Name column	1. Click within the search box at the top of the column, and enter your search criteria.

Adversaries Overlap Table

The Adversary Overlap table lists adversaries, the date and time they were created, their type, and any overlapping indicators.



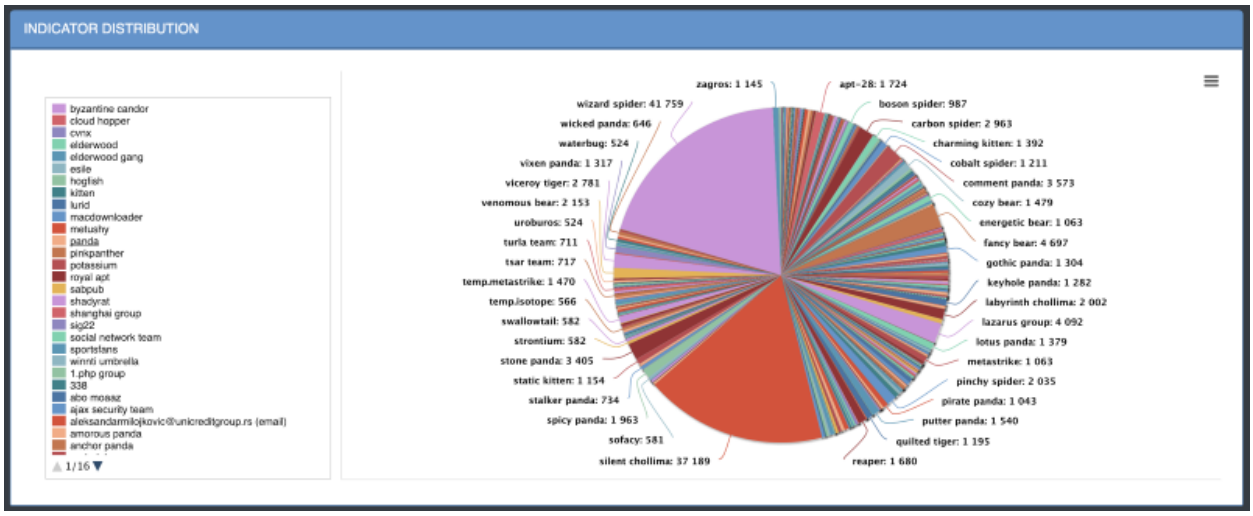
The following functions are available:

Function	Details
Opening the Adversary Details page for an adversary	1. Click the name in the Adversary Name column.
Opening the Indicator Details page for an overlapping indicator	1. Click the identity in the Overlapping Indicator column.
Changing the number of entries displayed in the table	1. Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	1. Click the column header. To reverse the column sorting order, click the header a second time.

Function	Details
Searching within a column	1. Click within the search box at the top of the column, and enter your search criteria.

Indicator Distribution Pie Chart

The Adversary Overlap table lists adversaries, the date and time they were created, their type, and any overlapping indicators.



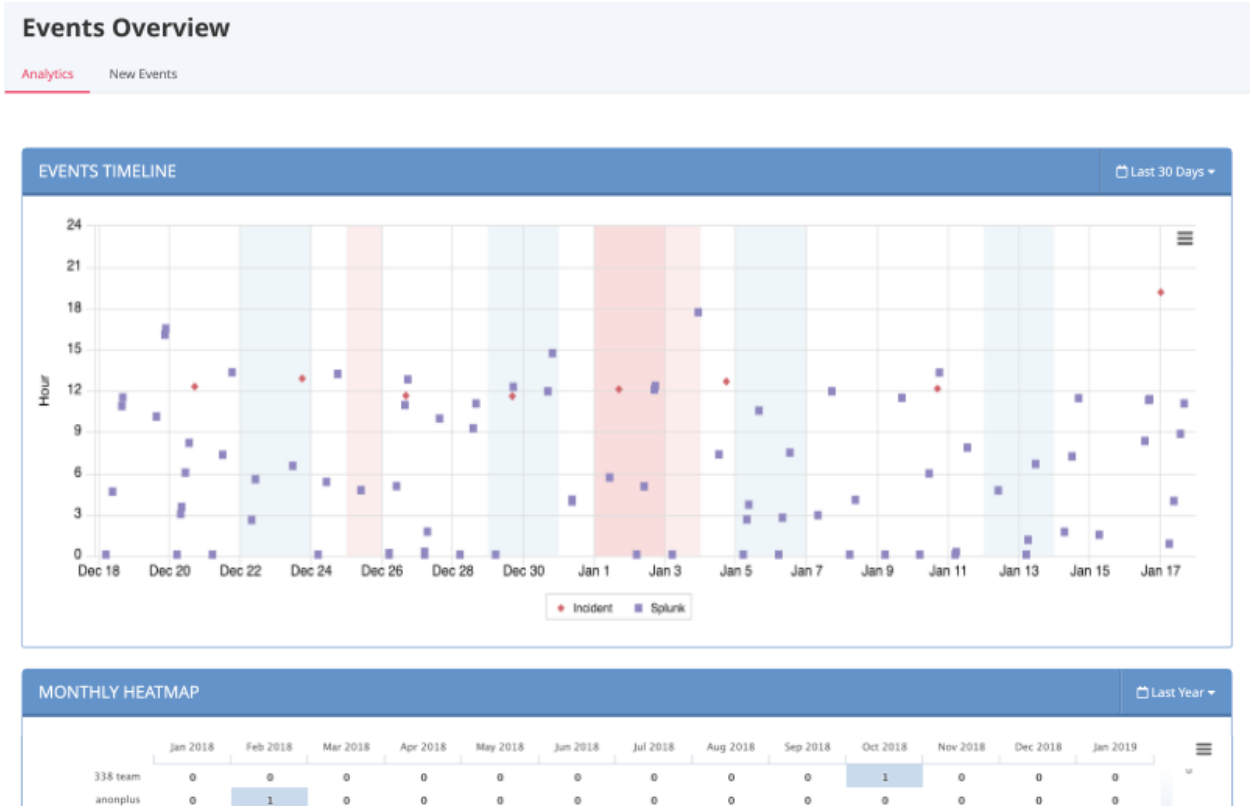
The following functions are available:

Function	Details
Viewing more information about a selected value	1. Hover over a colored section of the pie chart to open a popup identifying the indicator. The number of times the indicator was found within the specified time frame, and what percentage of the total number of indicators it represents.
Hiding or unhiding one of the values from the pie chart	1. Click the indicator on the left of the pie chart to remove it; click a second time to reinstate it.

Function	Details
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired timeframe. You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	1. Click the hamburger menu ☰ and select the desired option.

Events

The Events page provides a high-level view of what types of events have occurred and how frequently they are occurring.



To Access the Events page:

1. In the navigation menu, choose **Analytics** > **Events**.

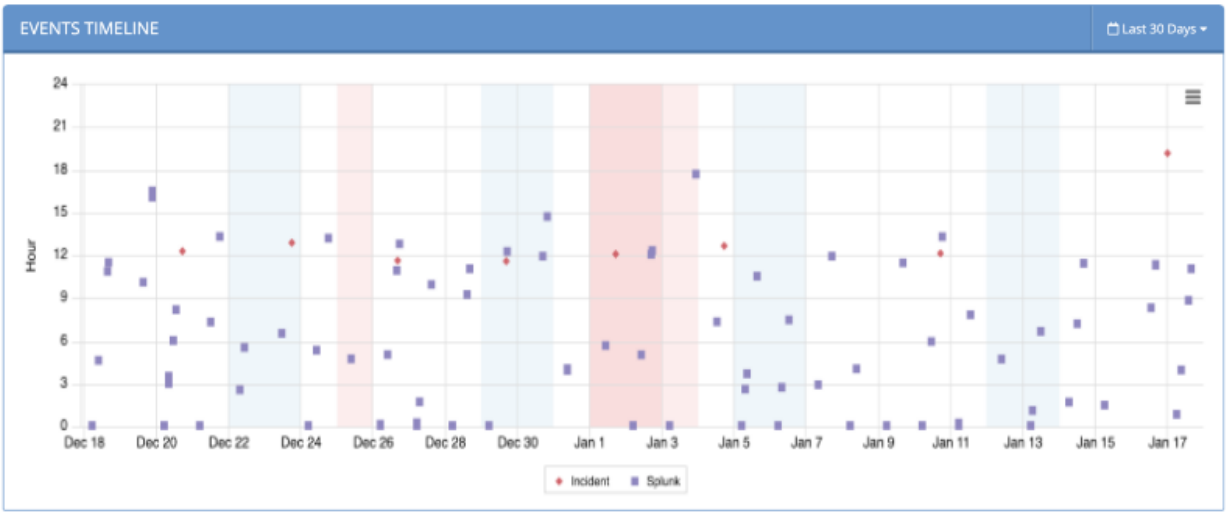
   The Events Overview page opens.

The tab options include:

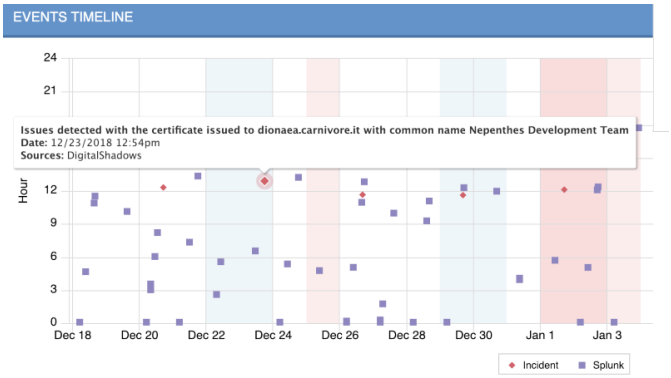
- Events History Scatter Plot
- Monthly Heatmap
- New Events Summary

Events History Scatter Plot

The scatter plot points are plotted by date (x-axis) and hour (y-axis). The legend under the scatter plot identifies the different kinds of events shown.



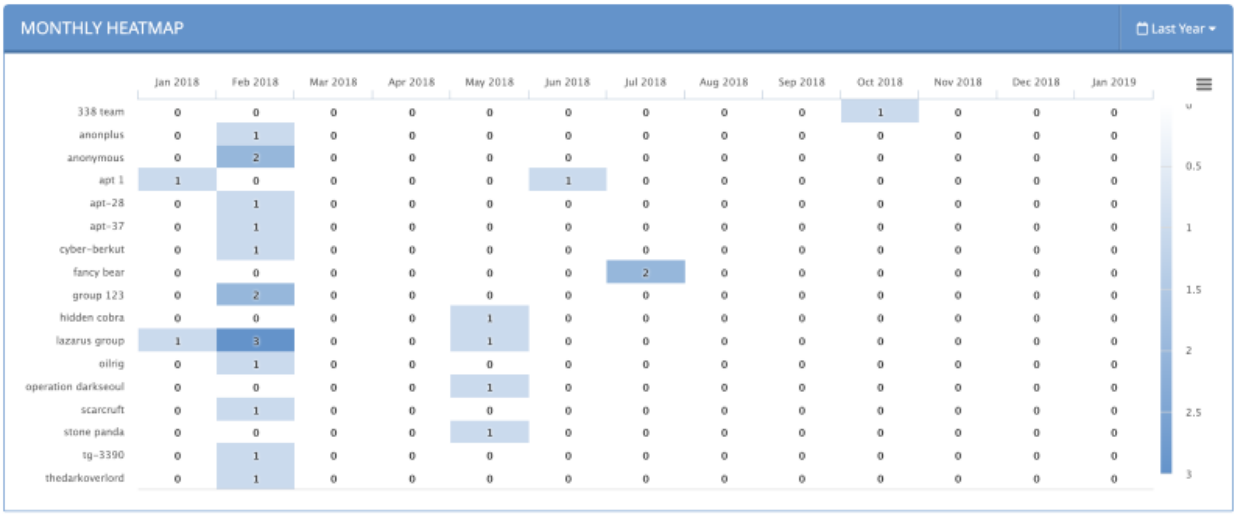
The following functions are available:

Function	Details
Viewing an event's name, date and time, and source	1. Hover your mouse over an event on the scatter plot to see its name, date and time, and source. 
Opening the Event Details page for one of the events	1. Click the event in the scatter plot. For more information, see Object Details Page.
Hiding or unhiding one or more of the event types	1. Click the event type in the legend immediately below the scatter plot to remove it from the graph; click it again to reinstate it.

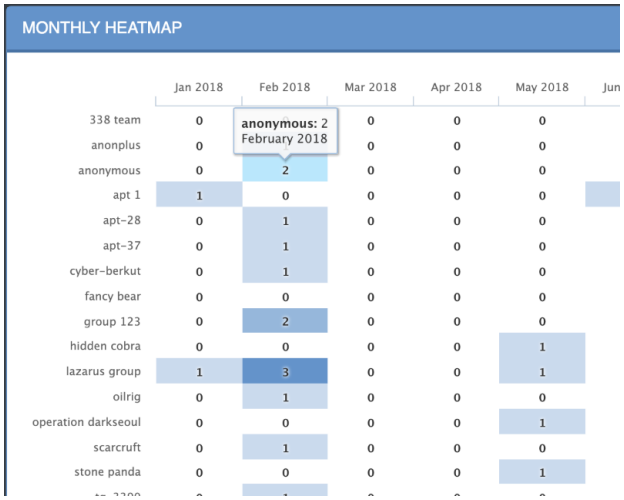
Function	Details
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired time frame. You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Printing or downloading the scatter plot as a PNG, JPEG, PDF, or SVG file	1. Click the hamburger menu ☰ and select the desired option.

Monthly Heatmap

The Monthly Heatmap table lists events that happened per adversary each month. Shading of the monthly totals is used to allow you to quickly scan for patterns in the events and to quickly detect events with higher monthly counts.

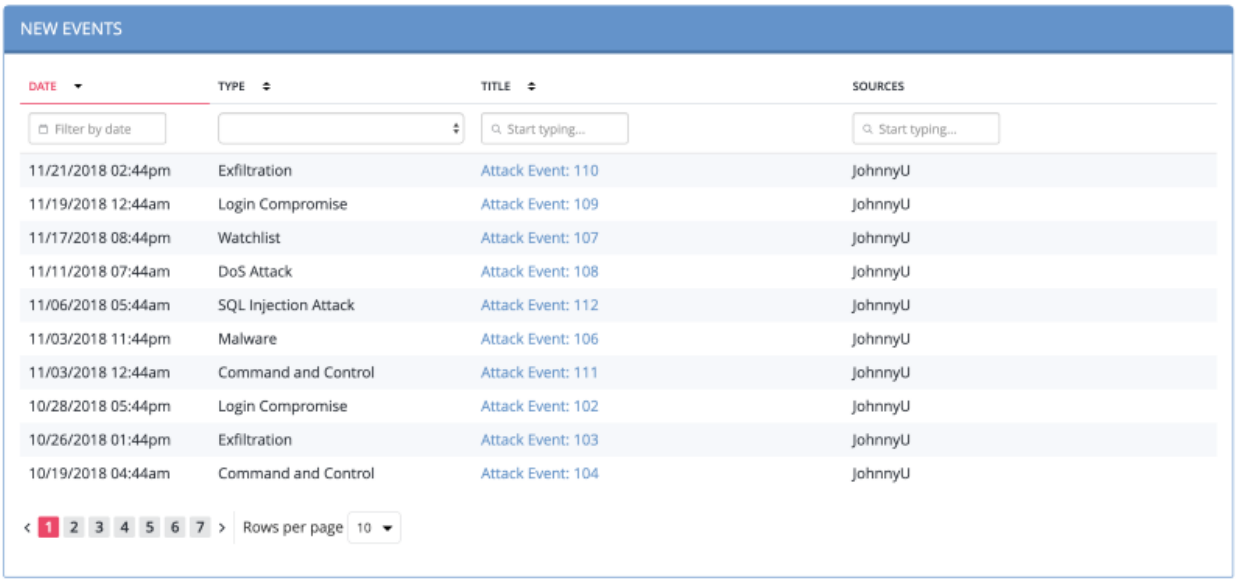


The following functions are available:

Function	Details
Viewing an event's name and monthly count	1. Hover your mouse over an event on the heatmap to see its name and monthly count. 
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired time frame. You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	1. Click the hamburger menu ☰ and select the desired option.

New Events Summary

The New Events Summary table provides a breakdown of events by date, type, title, and sources.



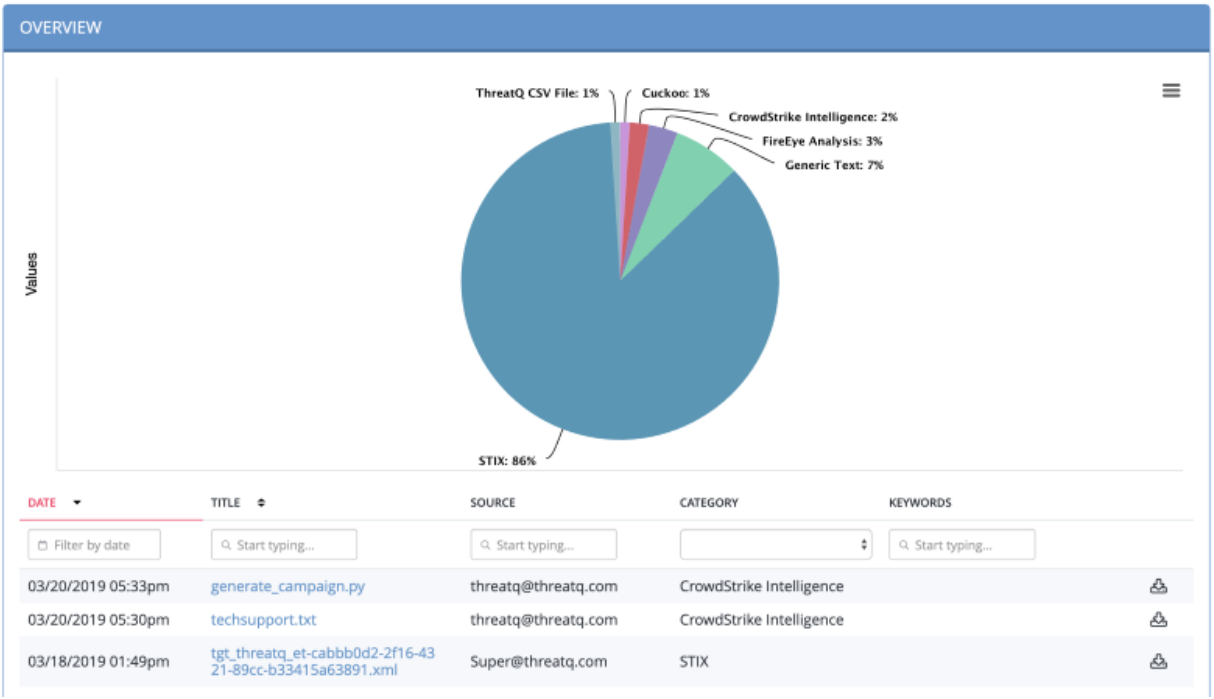
The following functions are available:

Function	Details
Opening the Event Details page for one of the events	1. Click the event title. For more information, see Object Details Page.
Changing the number of entries displayed in the table	1. Click the dropdown menu at the top right of the table, and select the desired option.
Sorting the table by a column	1. Click the column header. 2. Click the header a second time to reverse sort order.
Searching within a column	1. Click within the search box at the top of the column, and enter your search criteria.

Files

The Files page provides you with a pie chart displays the percentage of different types of files within the system and a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.

Files Overview

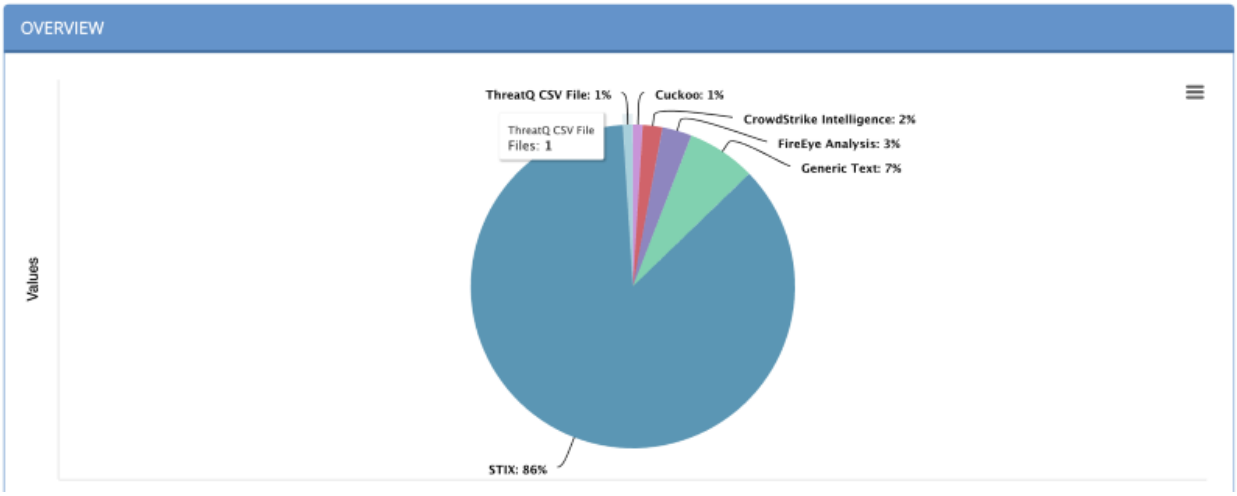


Available views include:

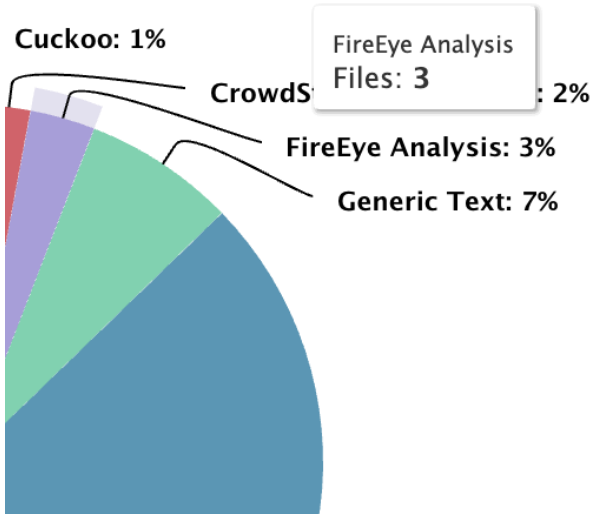
- Files Pie Chart
- Files Table

Files Pie Chart

The File Types pie chart displays the percentage of different types of files within the system.



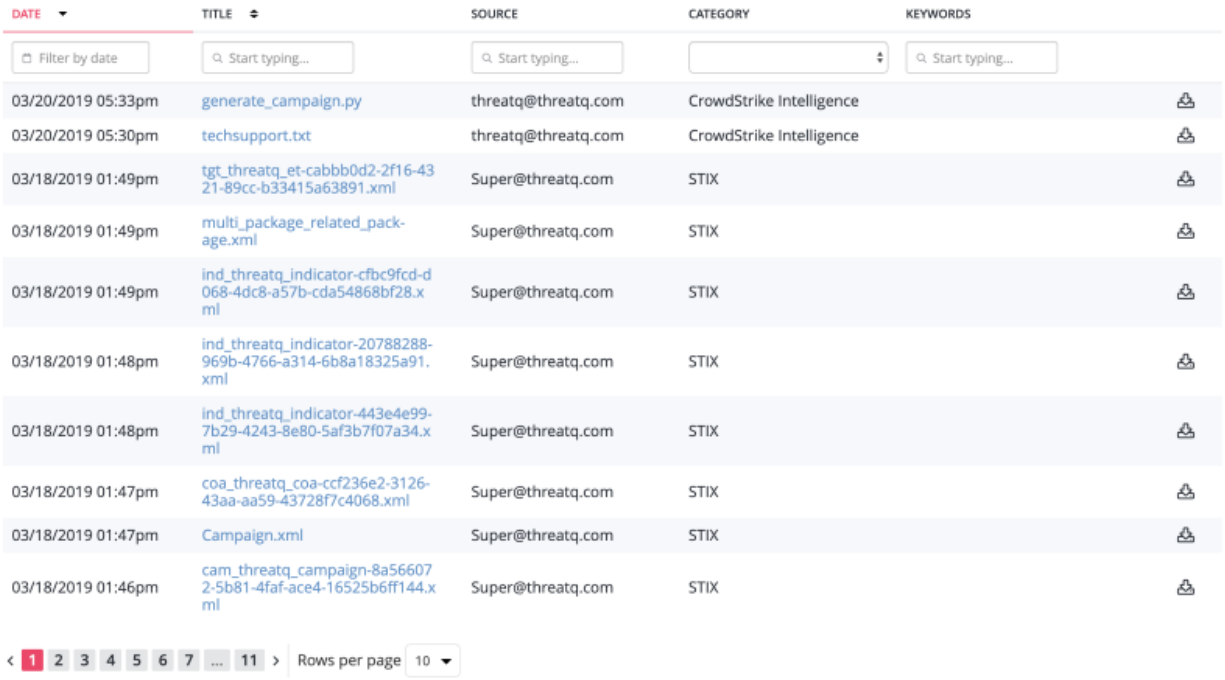
The following function is available:

Function	Details
Viewing more information about a selected file	1. Hover over a colored section of the pie chart to open a popup that gives the number of attachment types. 
Printing the graph or saving it	1. Click the hamburger menu ☰ and select the

Function	Details
as a PNG, JPEG, PDF, or SVG	desired option.

Files Table

Immediately below the Browse pie chart is a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.



The following function is available:

Function	Details
Opening the File Details page for a file	1. Click the name in the Title column.
Changing the number of entries displayed in the table per page	1. Click the paging batch option located to the bottom-right of the table.

Function	Details
Sorting the table by a column	1. Click the column header. 2. To reverse the column sorting order, click the header a second time.
Searching within a column	1. Click within the search box at the top of a column, and enter your search criteria.
Downloading a file	1. Click the download icon .

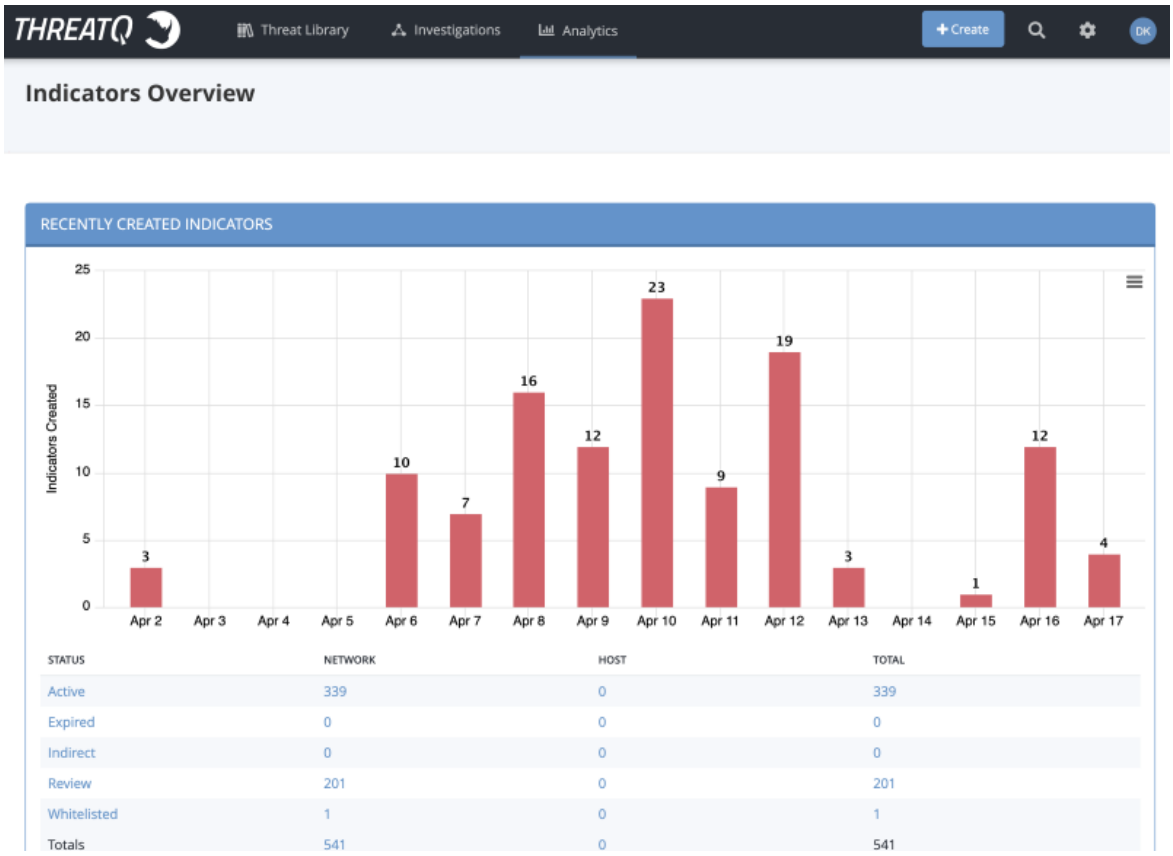
Indicators

The Indicators page provides an insight into what indicators have been added to the system within the last 15 days, as well as an overview of how many indicators fall under each indicator type.

To Access the Indicators Page:

1. From the navigation menu, click on **Analytics** and choose **Indicators**.

The Indicators Overview page will open with three view tab options at the to of the page.



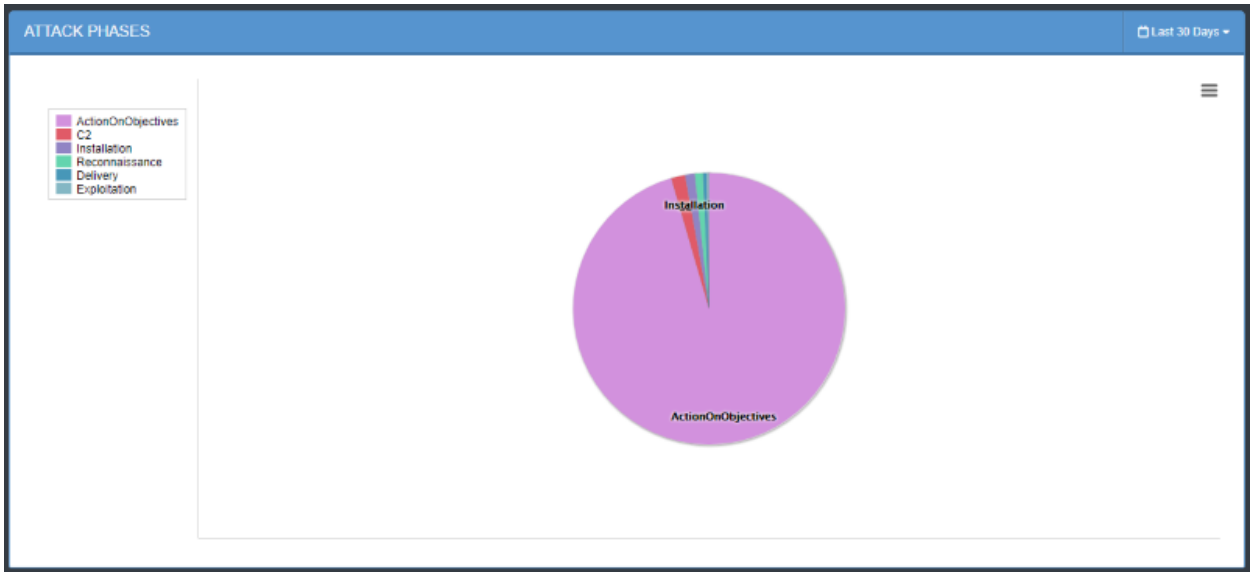
The page is broken down into different Indicator class views that are accessible via the tabbed navigation located at the top of the page.

Summaries included on the Indicator Page Include:

- Recently Created Indicators Histogram
- Most Recent 100 Indicators
- Attributes Table
- Recent Sources
- Attack Phases

Attack Phases

Attack Phases are the ways an indicator might be used and are listed as indicator attributes. The Attack Phases pie chart displays the number of indicators that fall under each attack phase.



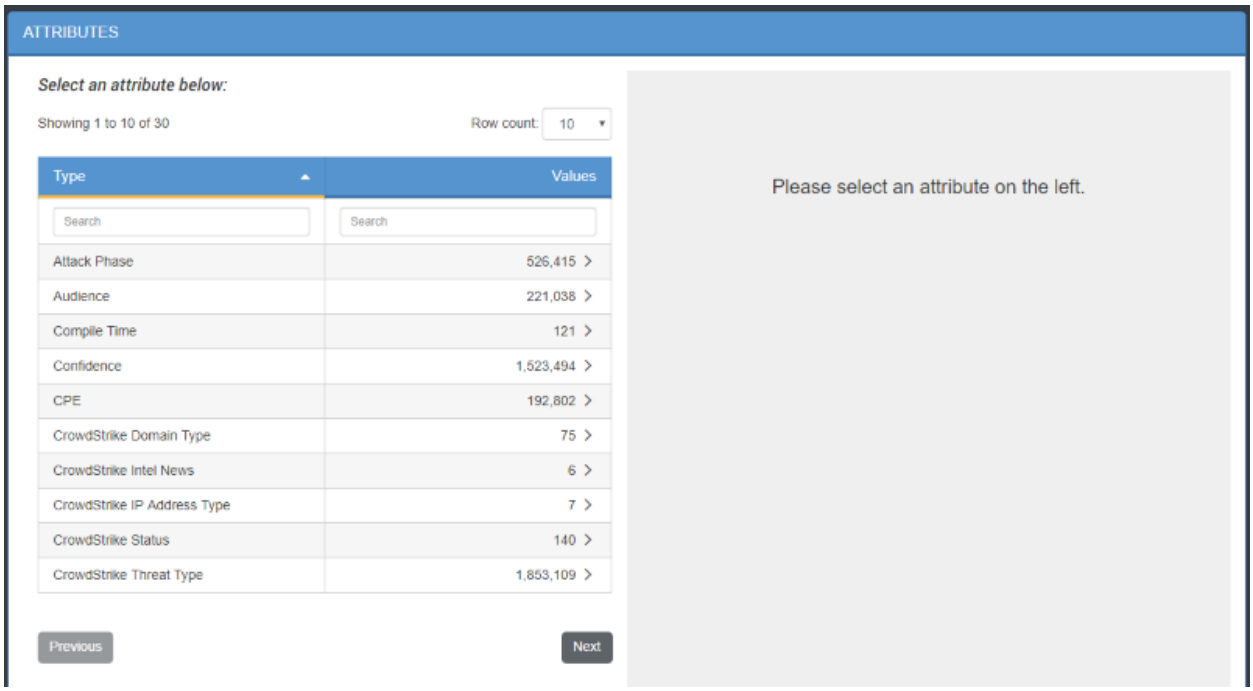
The following functions are available:

Function	Details
View the Number of Indicators for an Attack Phase	1. Hover the mouse over a portion of the pie chart to view a popup the Attack Phase and number of indicators associated with it. 2. Clicking on a pie chart section will open the Advanced Search page with the specific filter settings used for that selection.
Adjust the Date Range for the Information Displayed	The default Date Range is 30 days. 1. Click the date range icon located to the top-right of the

Function	Details
	chart and use the dropdown menu select the desired range. Users can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Hide a Values from the Pie Chart	1. Click on a Attack Phase in the legend to the left of the pie chart to hide it. The Attack Phase will be removed from the pie chart and the source in the legend appear greyed out. 2. Click on the Attack Phase again to add it back to the pie chart.

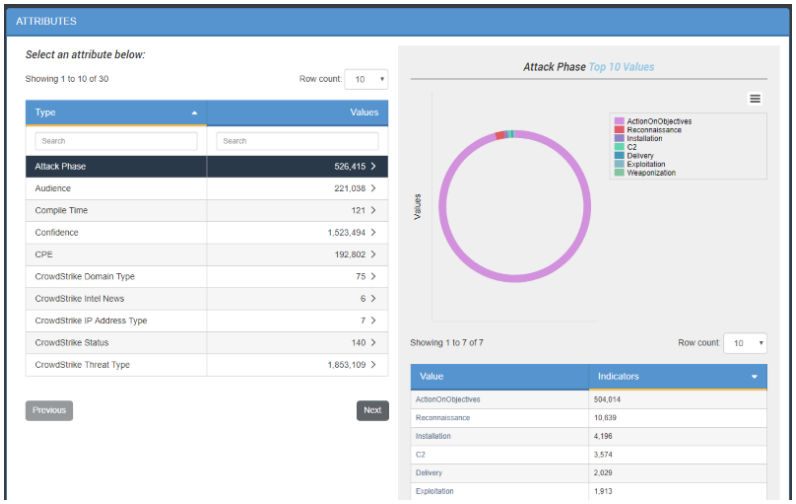
Attributes Table

The attributes list on the left side displays attributes related to indicators in your system.



The following functions are available:

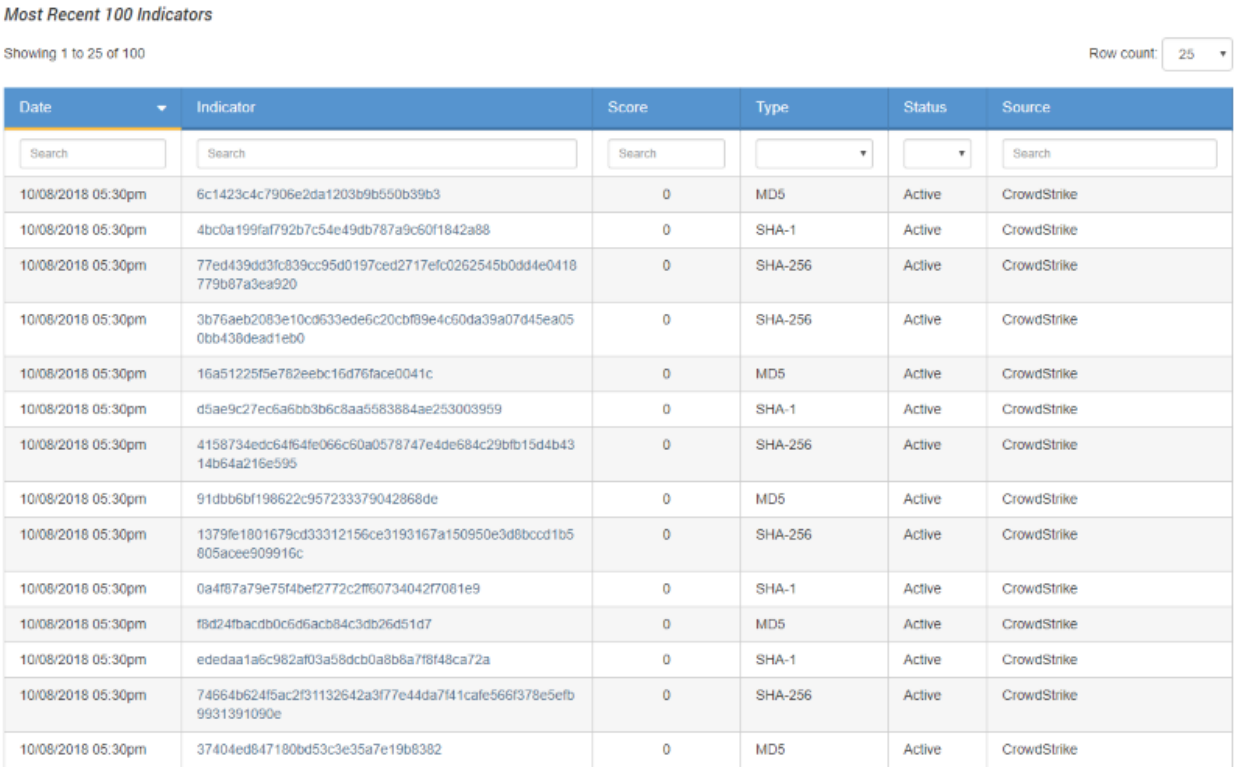
Function	Details
Change the Number of Entries Displayed in the Table	1. Click the **Row Count** icon located to the top-right of the chart and select a new display count from the drop-down.
Search/Filter Attributes and Values	1. Click within the search box at the top of the column, and enter your search criteria.
View More Information About a Selected Attribute	1. Click on an attribute row in the table to view additional information in the right pane.

Function	Details
	 2. Hover the mouse over different portions of the pie chart to reveal the segment's value. 3. Click on an **Attribute Value** in the summary table below the pie chart to open the Advanced Search page with those attribute values applied.

.

Most Recent 100 Indicators

The Most Recent 100 Indicators list displays the 100 most recently reported indicators.



Most Recent 100 Indicators

Showing 1 to 25 of 100 — Row count: 25

Date	Indicator	Score	Type	Status	Source
Search	Search	Search			Search
10/08/2018 05:30pm	6c1423c4c7906e2da1203b9b550b39b3	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	4bc0a199faf792b7c54e49db787a9c60f1842a88	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	77ed439dd3fc839cc95d0197ced2717efc0262545b0dd4e0418779b87a3ea920	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	3b76aeb2083e10cd633ede6c20cbf89e4c60da39a07d45ea050bb438dead1eb0	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	16a51225f5e782eebc16d76face0041c	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	d5ae9c27ec6a6bb3b6c8aa5583884ae253003959	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	4158734edc64f64fe066c60a0578747e4de684c29bfb15d4b4314b64a216e595	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	91dbb6bf198622c957233379042868de	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	1379fe1801679cd33312156ce3193167a150950e3d8bccd1b5805acee909916c	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	0a4f87a79e75f4bef2772c2ff60734042f7061e9	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	f8d24fbacdb0c6d6acb84c3db26d51d7	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	ededaa1a6c982af03a58dcb0a8b8a7f8f48ca72a	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	74664b624f5ac2f31132642a3f77e44da7f41cafe566f378e5efb9931391090e	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	37404ed847180bd53c3e35a7e19b8382	0	MD5	Active	CrowdStrike

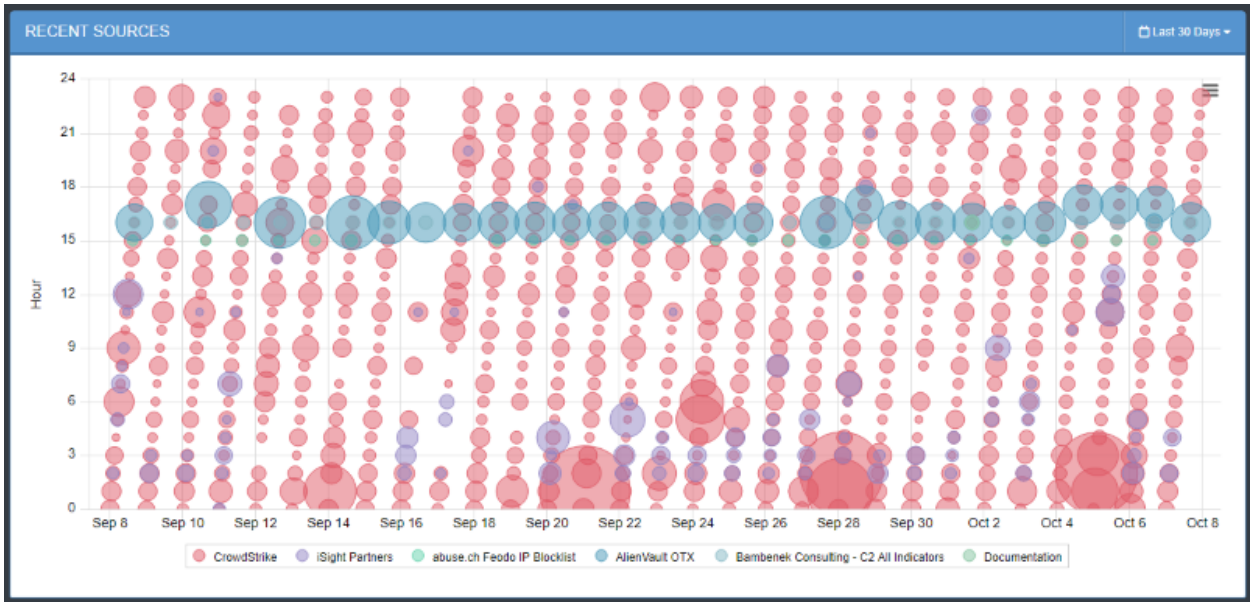
The following functions are available:

Function	Details
Resort the Table	1. Click on the different table headings to resort that table by that column.
Search and Filter Table Results	1. Click on one of the search boxes at the top of the columns and enter a keyword to filter the results. You can use the supplied dropdown selections for the Status and Type columns to filter by system-available values.
Modify the Number of	1. Click on the **Row Count** icon located to the top-

Function	Details
Rows Displayed	right of the chart and select a new display count from the dropdown.
Access the Indicator Details Page for a Specific Indicator	1. Click on the specific Indicator to review to open the Indicator's Details page.

Recent Sources

The Recent Sources Scatter plot displays how many indicators were provided by a given source each day within a specified time frame.



The following functions are available:

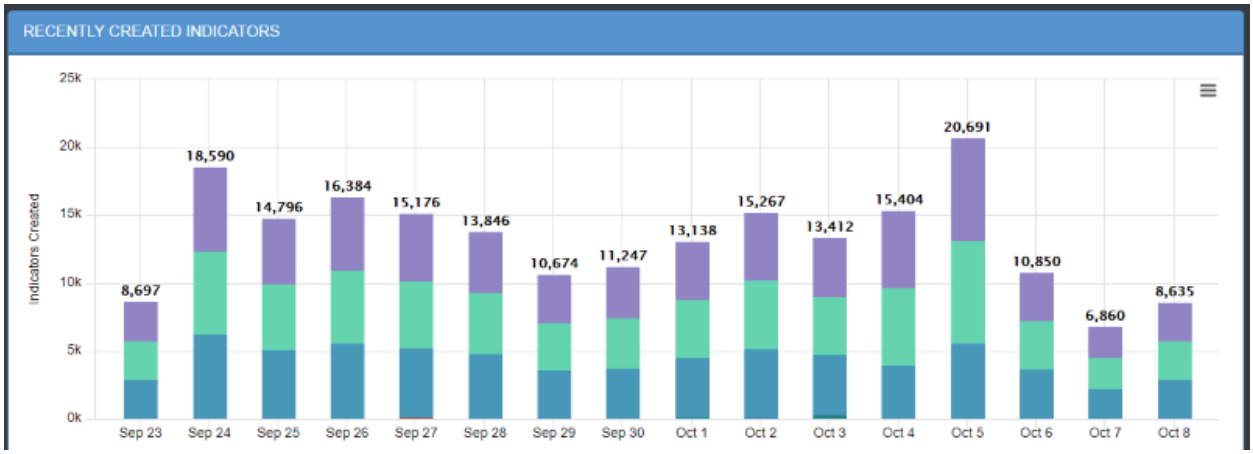
Function	Details
View the Date and Number of Indicators from a	1. Hover the mouse over one of the scatter plot circles to view a popup with the Source, Date, Time and

Function	Details
Given Source	Number of Indicators.  2. Click on the one of the scatter plot circles to open the Advanced Search page with the specific filter settings used for that selection.
Adjust the Date Range of the Information Displayed	The default date range is 30 days. 1. Click the date range icon located to the top-right of the chart and use the dropdown menu select the desired range. You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Hide Values from the Scatterplot	1. Click on a source in the legend under the scatter plot to hide it. The Source will be removed from the scatter plot and

Function	Details
	the source in the legend appear grayed out. 2. Click on the source again to add it back to the scatter plot.

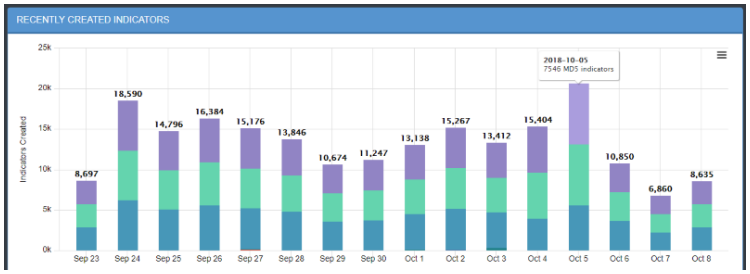
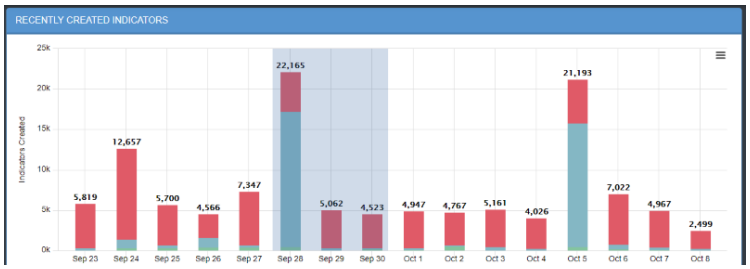
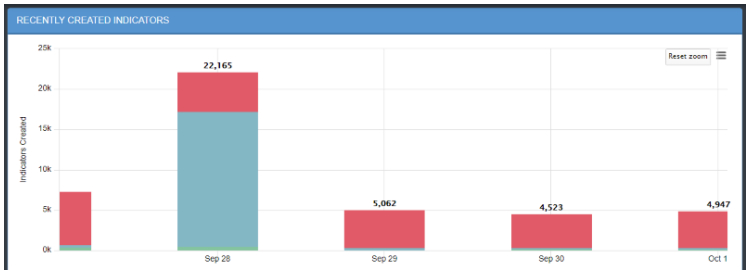
Recently Created Indicators Histogram

The histogram is organized by date. Daily indicator totals are at the top of each column. Each bar is broken down into colors, one for each indicator type.



The following functions are available:

Function	Details
Viewing the number of indicators created each day by type	1. Hover over a colored section to view a popup showing how many attempts of a particular type (for example, MD5, SHA-1, SHA-256) were made on that date.

Function	Details
	
Zooming in for a closer view	1. Drag your mouse over a section of the histogram, and your view will be magnified.   2. Click **Reset Zoom** to return to the full histogram.
Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file	1. Click the hamburger menu ☰, and select the desired option.

Incoming Feeds

The following describes how to use incoming feeds to ingest threat intelligence data.

Incoming Feeds Overview

You can enable and manage incoming feeds in ThreatQ to ingest threat intelligence data. Incoming feeds are organized into the following categories:

- Commercial
- OSINT or Open Source
- STIX/TAXII Feeds
- Labs

Commercial Feeds

Commercial feeds are provided by paid feed providers as a service. To enable these feeds in ThreatQ, you will need an API ID or API Key from the provider. Commercial feeds typically provide highly contextual threat intelligence data. You can learn more about these feeds on their vendor's websites.

OSINT Feeds

OSINT feeds are open source threat intelligence feeds. Open source feeds are free to use, but some may require you to register with the feed provider to attain an API Key.

STIX/Taxii Feeds

STIX stands for Standard Threat Information Expression, it is an emerging standard for the sharing of machine readable intelligence and incident data. A STIX package is an XML document that can contain many indicators and related context information. For the automated sharing of STIX packages, a protocol called TAXII (Trusted Automated eXchange of Indicator Information) is used to provide a feed to consumers.

ThreatQ provides a feature for consuming STIX/Taxii feeds.

Related Topic

Adding a New STIX/TAXII Feed

Labs Feeds

Labs (formerly known as ThreatQ Labs) are driven by ThreatQuotient's Threat Intelligence Services Team. Labs feeds provide a solution for data ingestion that is not provided by the feeds pre-configured with the ThreatQ platform. You should inquire with a Threat Intelligence Engineer to see what Labs are available.

Managing Incoming Feeds

Manage threat intelligence feeds on the Incoming Feeds page.

The following table describes the actions you can take to manage Incoming Feeds.

To	Do this..
Turn a feed on or off	Toggle the switch next to the feed name.
Editing a feed's display name or URL	Click **Feed Settings** for the feed you wish to edit, and make desired edits.

To	Do this..
Install/Upgrade Configuration Driven Feed (CDF)	See the Adding/Upgrading a CDF from the ThreatQ Interface topic.
Uninstall Configuration Driven Feed (CDF)	See the Removing a CDF from the ThreatQ Interface topic.

Adding/Upgrading CDF Command

Use the steps below to add or upgrade a Configuration Driven Feed (CDF) using the Command Line Interface (CLI). The command creates connectors for each feed defined in the feed definition file.

To install a CDF:

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Place the application into maintenance mode - see the Maintenance Mode topic.
4. Run the following command:

```
sudo php artisan threatq:feed-install <Feed
Definition File>
```

The application will notify you if the feed(s) in the feed definition file already exists in the system and will cancel the installation. See the

To Upgrade a CDF and Changes in User Configurations sections below for more information.

```
threatq:feed-install 6266 Started > 2019-02-21 18:47:24
threatq:feed-install 6266 Command failed:
The provided definition file contains the following installed feeds:
Testing at 5 AM. Proceed with the update by using the --upgrade flag.
```

5. Bring the application out of maintenance mode - see the Maintenance Mode topic.

To Upgrade a CDF

This command can be used to update a feed's Category and Namespace. If the category exists on the appliance, the command will update both fields and link the feed to the designated category. ThreatQ will confirm that the defined category exists before completing the update command. If the category does not exist, ThreatQ will not update the feed.

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Place the application into maintenance mode - see the Maintenance Mode topic.
4. Run the following command:

```
sudo php artisan threatq:feed-install <Feed
Definition File> --upgrade
```

5. Bring the application out of maintenance mode - see the Maintenance Mode topic.

Changes in User Configurations

When upgrading an existing feed using the **--upgrade flag**, the application will compare the existing version of the feed with the new version for differences in the user configuration. If a difference is detected, the application will inform you that the current user configuration for that feed will be overwritten. The application will require user input to continue with the feed upgrade.

```
threatq:feed-install 6674 Started > 2019-02-21 18:48:28
threatq:feed-install 6674 Warning: The provided definition file
contains updated user configurations. It is highly recommended to
create a copy of the configuration values for the following feeds
before proceeding with the update: Testing at 5 AM.
Do you want to continue? (Y/N) Y
threatq:feed-install 6674 Number of connectors in the definition file:
1
threatq:feed-install 6674 Number of existing connectors updated: 1
threatq:feed-install 6674 Finished > 2019-02-21 18:48:34 > 6.19s
```

It is recommended that you create a copy of the existing configuration values before proceeding with the upgrade.

Command Flag Help

You can also see a full list of command flags using the following command while under the /var/www/api directory:

```
sudo php artisan threatq:feed-install --help
```

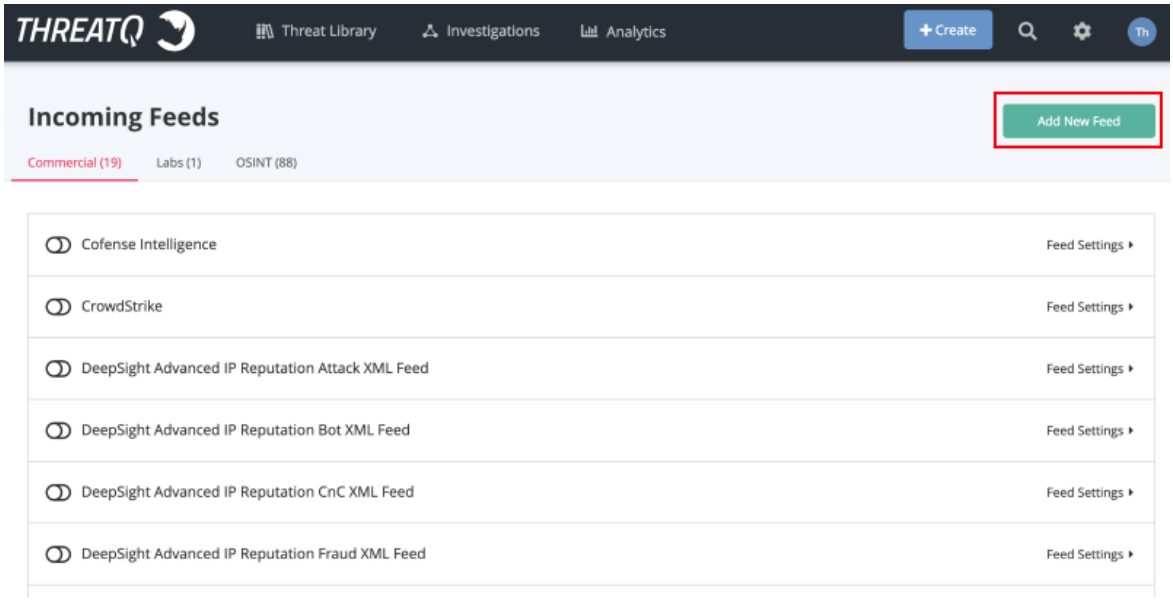
Adding/Upgrading a CDF from the ThreatQ Interface

You can add or upgrade a CDF from the **Incoming Feeds** page of the ThreatQ interface.

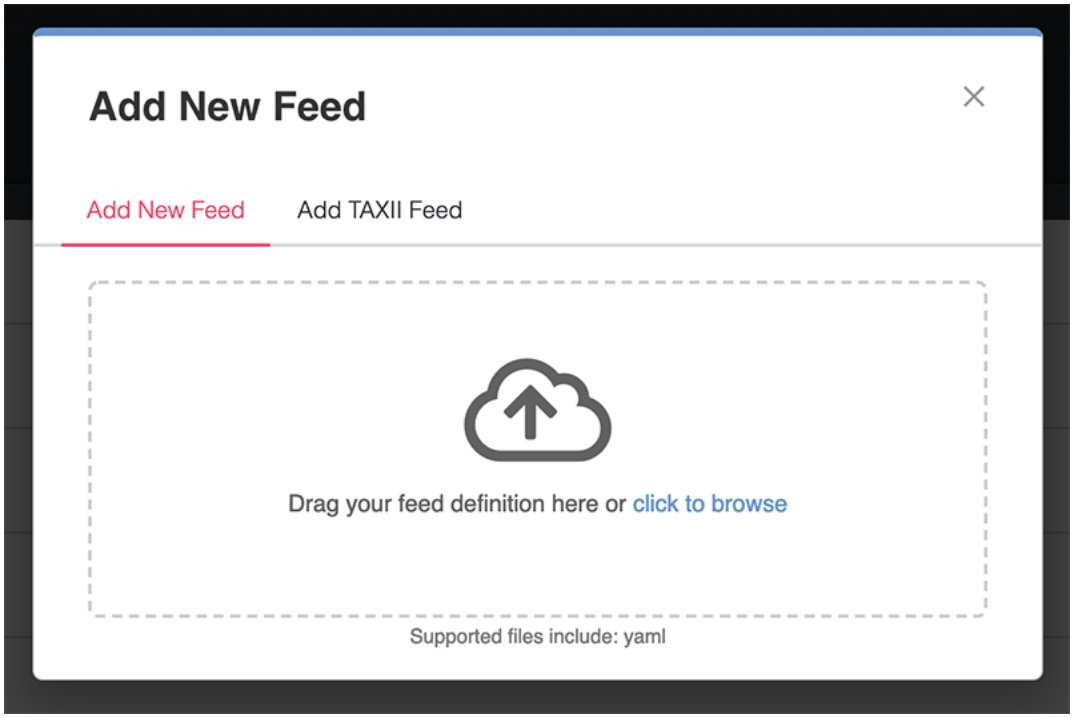
The process to upgrade a CDF is the same as adding a new CDF.

To add a CDF from the ThreatQ Interface:

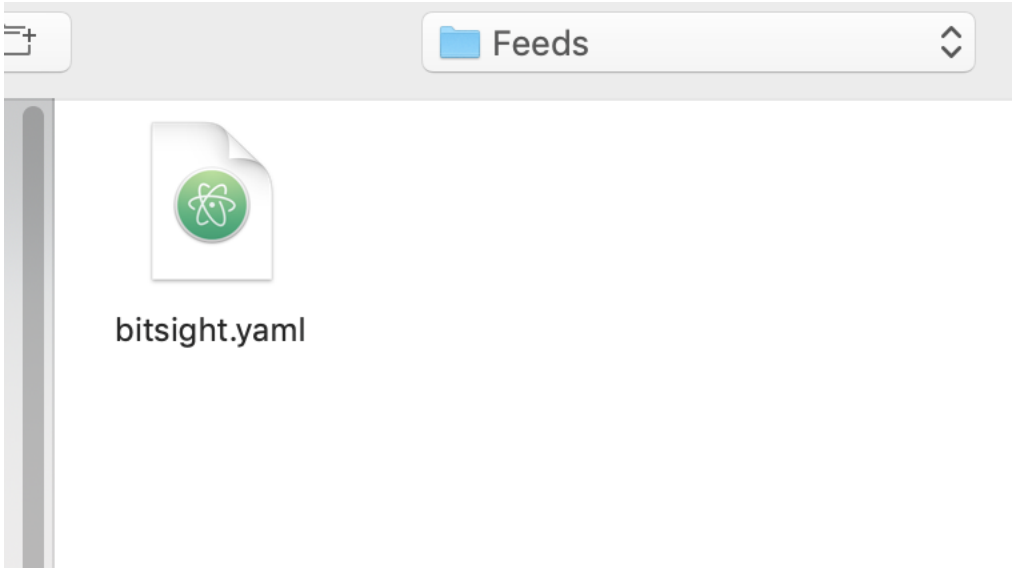
1. Go to **System Settings** > **Incoming Feeds**.
2. Click on the **Add New Feed** button.



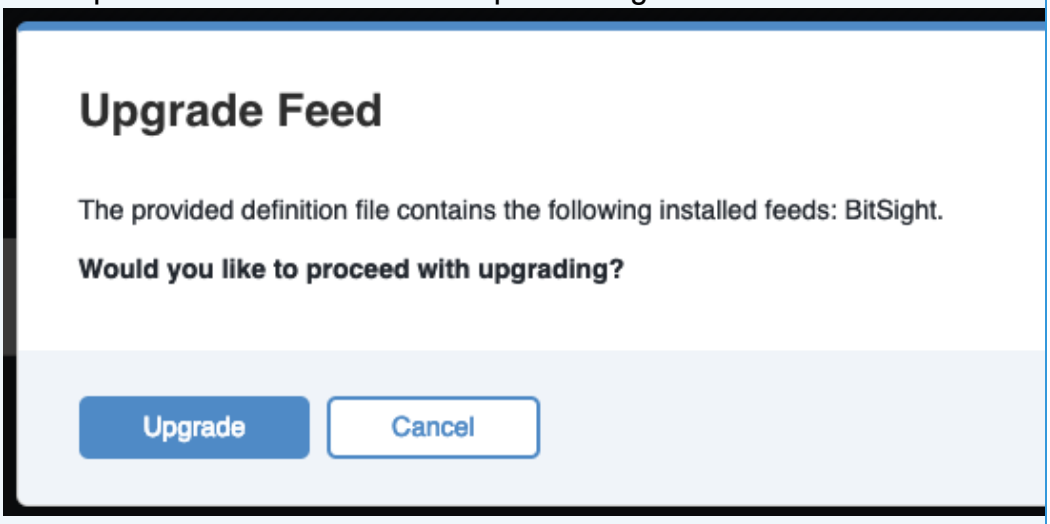
The Add New Feed dialog box opens.



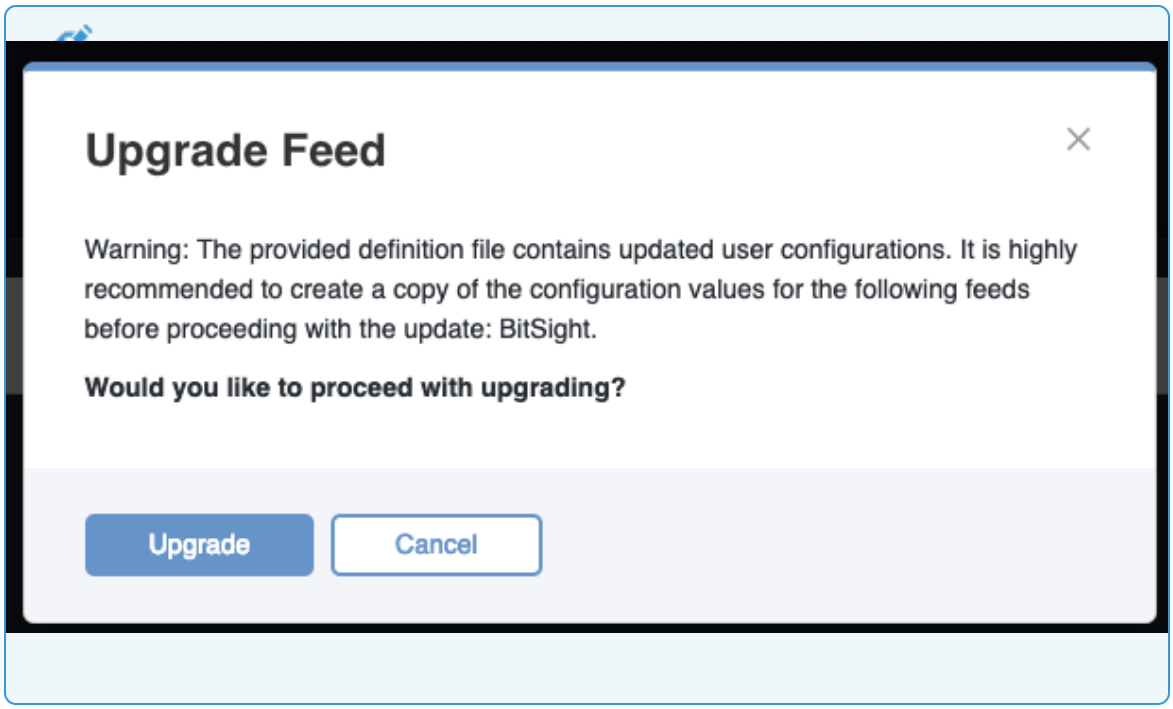
3. Select the file to upload by either clicking and dragging the file onto the dialog box or using the link supplied to browse for the file on your local machine.



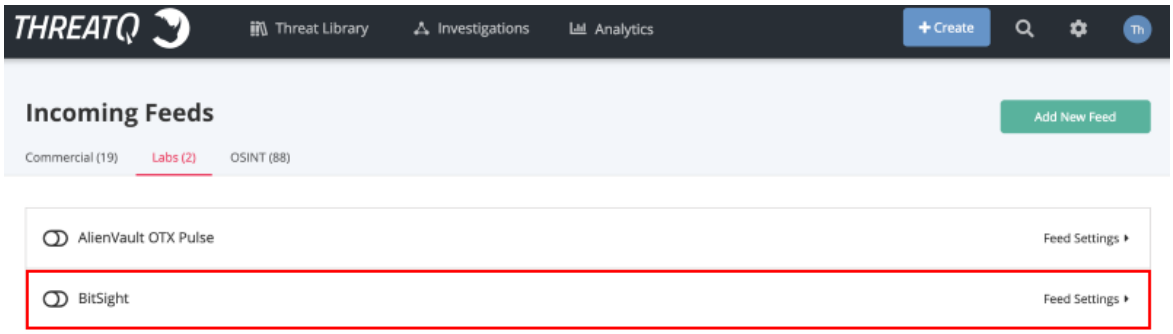
Existing Feeds
ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding.



User Configurations
ThreatQ will also inform you if the new version of the CDF contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed. The platform will require user confirmation before proceeding.



4. The new feed(s) will be added.



You will need to configure and enable the feed.

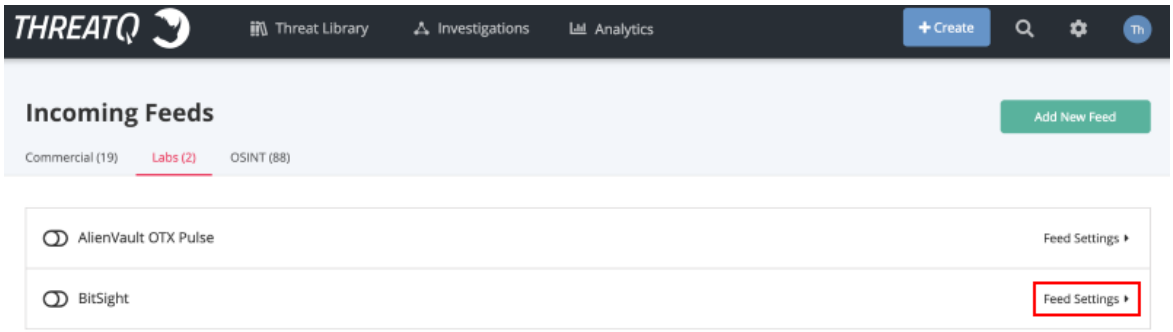
Removing a CDF from the ThreatQ Interface

You can remove CDFs from the **Incoming Feeds** page of the ThreatQ interface.

This feature only applies to CDFs.

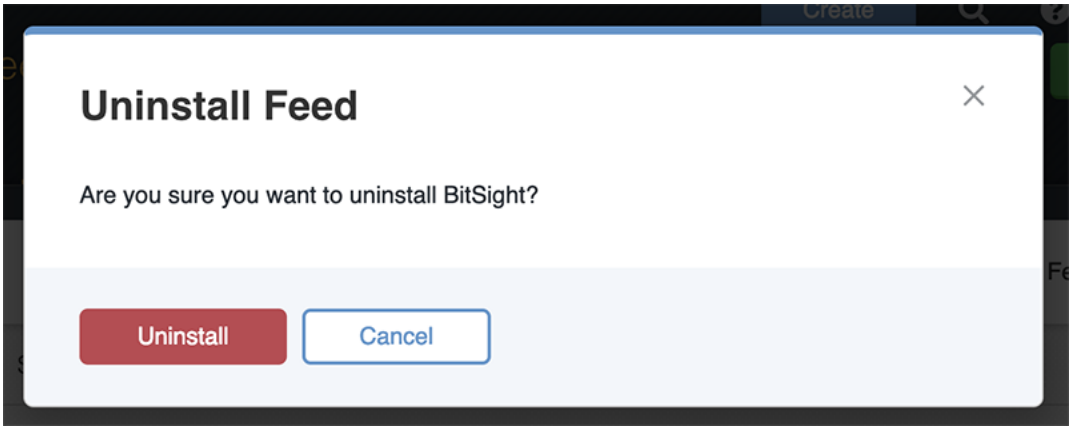
To remove a CDF from the ThreatQ Interface:

1. Go to **System Settings** > **Incoming Feeds**.
2. Click on the **Feed Settings** link for the feed.



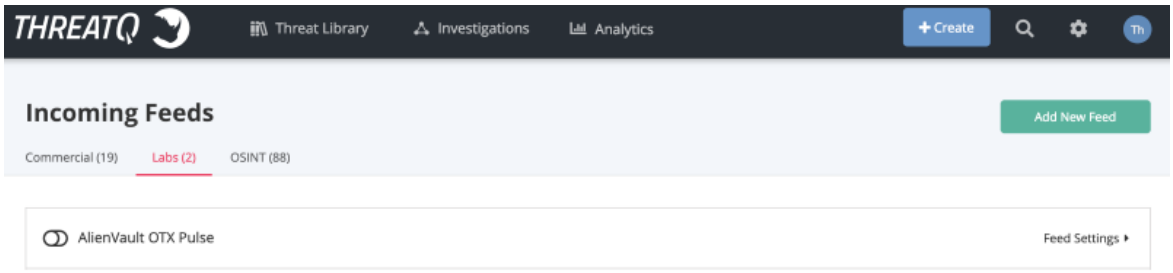
3. Click on the **Uninstall Feed** button.

The Uninstall Feed dialog box opens.



4. Click on **Uninstall**.

5. The feed will be removed.



Enabling a Commercial Feed

To enable a commercial feed, you will need an API ID and API Key provided by the feed provider.

Procedure:

1. Choose the **Settings icon > Incoming Feeds**.
2. Click the toggle switch next to the feed you want to enable.

   Green indicates enabled.

3. Expand **Feed Settings**.
4. On the Connection tab, enter:
   - Feed Name - the name displayed in ThreatQ
   - API ID - provided by the feed vendor for authorization
   - API Key - provided by the feed vendor for authorization
   - Feed URL - this field is autofilled
5. On the Settings tab, select:
   - the status that incoming indicators from this feed will receive.
   - the frequency that ThreatQ pulls information from the feed.

- whether you will receive in-app and email feed health notifications for the feed.

This feature only pertains to CDF feeds. The In-App and Email Notification features must be enabled. Selecting the checkbox will not automatically enable those features. Only users with ThreatQ administrator and maintenance roles will receive in-app notifications. Your account must be included in the Notification Settings list to receive emails. See the Notification Settings topic for more details.

6. Click **Save Changes**.

Enabling an OSINT Feed

OSINT feeds do not require API IDs, but some may require an API key from the feed provider.

Procedure:

1. Choose the **Settings icon > Incoming Feeds**.
2. Click the toggle switch next to the feed you want to enable.

   Green indicates enabled.

3. Expand **Feed Settings**.
4. On the Connection tab, enter:
   - Feed Name - the name displayed in ThreatQ
   - API Key (if required) - provided the feed vendor for authorization
   - Feed URL - this field is autofilled
5. On the Settings tab, select:
   - the status that incoming indicators from this feed will receive.
   - the frequency that ThreatQ pulls information from the feed.

- whether you will receive in-app and email feed health notifications for the feed.

This feature only pertains to CDF feeds. The In-App and Email Notification features must be enabled. Selecting the checkbox will not automatically enable those features. Only users with ThreatQ administrator and maintenance roles will receive in-app notifications. Your account must be included in the Notification Settings list to receive emails. See the Notification Settings topic for more details.

6. Click **Save Changes**.

Viewing Feed Queues Command

When upgrading a feed, it is recommended to allow the previous implementation the feed to complete processing of the data it has already downloaded, prior to upgrade, to avoid any data loss.

Perform the following steps to confirm that the queues have been cleared.

1. Run the following command:

```
/var/www/api/artisan threatq:list-queues -p
feeds
```

2. Locate and confirm that the feed's Indicators and Reports rows display a value of "0" for the Messages Ready and Messages Unacknowledged columns.

The queues should be cleared, reporting 0 values, before proceeding with the update.

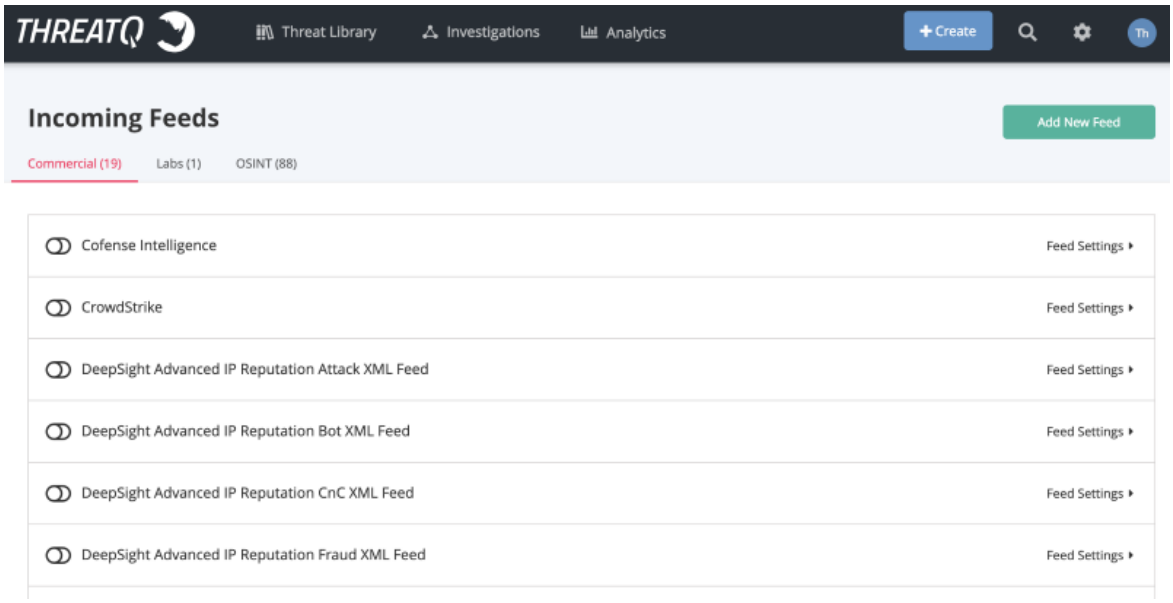
Adding a New STIX/TAXII Feed

Complete the following steps to add a new STIX/TAXII indicator feed.

Procedure:

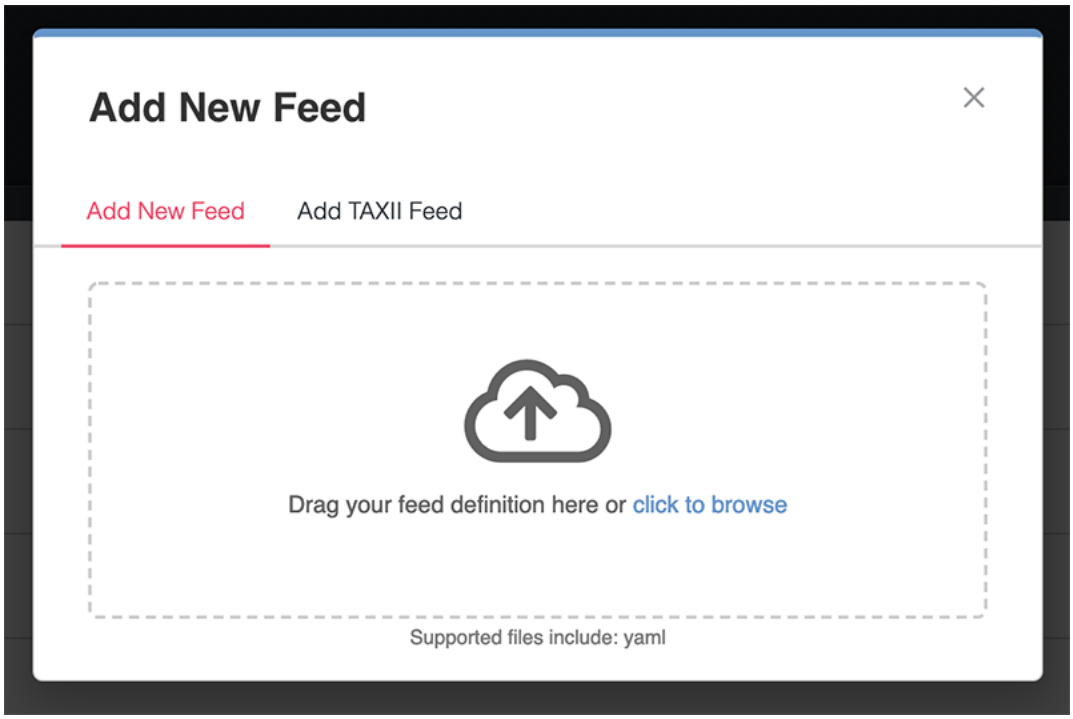
1. Click on the **Settings** icon and select **Incoming Feeds**.

   The Incoming Feeds page will load.



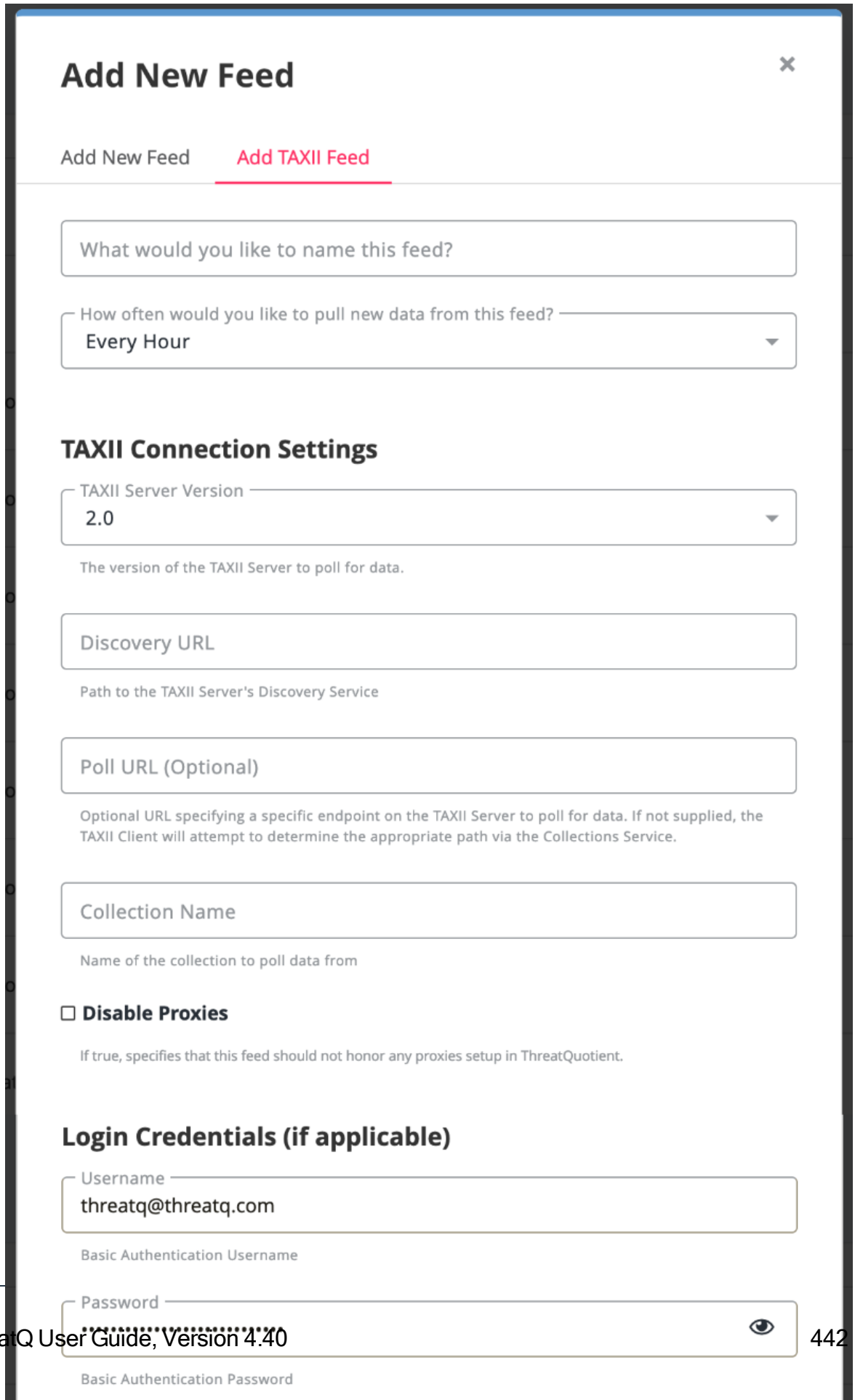
2. Click on **Add New Feed**.

   The Add New Feed dialog box opens.



3. Click on **Add TAXII Feed**.

The Add TAXII Feed form loads.


Add New Feed
Add New Feed
Add TAXII Feed
What would you like to name this feed?
How often would you like to pull new data from this feed?
Every Hour
TAXII Connection Settings
TAXII Server Version
2.0
The version of the TAXII Server to poll for data.
Discovery URL
Path to the TAXII Server's Discovery Service
Poll URL (Optional)
Optional URL specifying a specific endpoint on the TAXII Server to poll for data. If not supplied, the TAXII Client will attempt to determine the appropriate path via the Collections Service.
Collection Name
Name of the collection to poll data from
Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.
Login Credentials (if applicable)
Username
threatq@threatq.com
Basic Authentication Username
Password
Basic Authentication Password

4. Complete the following fields:

Field	Instructions
What would you like to name this feed?	Enter the feed's name that will be displayed throughout ThreatQ. The name must be at least 5 characters long It does not need to match the **Collection Name**.
How often would you like to pull new data from this feed?	Choose **Every Hour** or **Every Day**.
TAXII Connection Settings	
TAXII Server Version	Options include: 1.0, 1.2, 2.0. This field is required.
Discovery URL	This is where the TAXII server can be reached. This field is required.
Poll URL	An optional URL that specifies a specific endpoint on the TAXII Server to poll for data.
Collection Name	The name of the collection of data in the feed you will access. This field is required.

Field	Instructions
Client User Authentication	
Username	Enter a username if required for the feed.
Password	Enter a password if required for the feed.
Client TLS/SSL Authentication	
Client Certificate	Enter a certificate if required for the feed.
Client Key	Enter a private key if required for the feed.
Server Authentication	
Verify SSL	Leave the checkbox checked to require that the TAXII client verify the provider's SSL certificate.
Host CA Certificate Bundle	The provider's CA Certificate used to verify SSL. The Host CA Certificate Bundle will not be honored if the Verify SSL option is not selected.

5. Click on **Add TAXII Feed**.

CrowdStrike CDF

Starting with ThreatQ version 4.2, the CrowdStrike feed will be updated to use the configuration driven method. This update will allow users to review an Activity Log that will

provide a summary of the feed and including important details such as:

- how the feed was triggered,
- start and completion time,
- raw response received from the vendor,
- how many objects were processed by ThreatQ.

Query Range

Query Range is a new feature with this update that uses the exact date/time that ThreatQ queried CrowdStrike's API for information.

This feature, unique to the updated CrowdStrike feed, ensures that there isn't a gap in feed coverage in the event of a feed run failure or server downtime. ThreatQ will use the last completed run time when performing a new run.

Example: *Customer has CrowdStrike configured to perform scheduled runs every hour. The customer powers down the server for three hours for maintenance. The next time the feed runs, it will automatically use the last successful run time in its range which will cover the three-hour gap when the server was down.*

PlaceHolder Files

The Placeholder file concept is currently used by the updated CrowdStrike feed with expanded support to other feeds to be added in future releases. Placeholder files prevent linking information delays between the vendor and ThreatQ by creating a placeholder file immediately after receiving a file or report from the vendor. ThreatQ will fulfill the placeholder and update the object information accordingly. ThreatQ will mark placeholder files on the details and file overview pages.

Related Information

- CrowdStrike Update Instructions
- Performing Manual Feed Runs

CrowdStrike Update Instructions

CrowdStrike users must update their proxy server settings to use http: for their https: traffic before upgrading CrowdStrike.

Prior to upgrade, and to avoid any data loss, it is recommended to allow the previous implementation of CrowdStrike to complete processing of the data it has already downloaded.

Perform the following steps to confirm that the queues have been cleared.

1. Run the following command:

```
/var/www/api/artisan threatq:list-queues -p
feeds
```

2. Locate and confirm that the **CrowdStrike Indicators** and **Reports** rows display a value of "**0**" for the **Messages Ready** and **Messages Unacknowledged** columns.

   The queues must be cleared, reporting 0 values, before proceeding with the update.

3. Proceed with the standard feed update procedures.

   The update process is quick. A confirmation message will confirm that the update process is complete. The **Activity Log** feature will load once CrowdStrike is enabled and a feed run instance has been created or completed.

Source Consolidation Command

Use the steps below to consolidate/deduplicate similarly named sources and to remove unused sources from the ThreatQ application. A source that have been removed or merged will have its data mapped to a new source.

The command does not require recalculation of scoring.

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Place the application into maintenance mode - see the Maintenance Mode topic.
4. Run the following command:

```
sudo php artisan threatq:consolidate-sources
```

5. Bring the application out of maintenance mode - see the Maintenance Mode topic.

Example Scenario:

1. User manually adds ABC as a source.
2. User enables ABC.

   There are now two ABC sources in the system.

3. User runs consolidation command.
4. The application merges the sources and remaps any items linked to the correct source.

Source Merge Command

Use the steps below to merge a user-created source (source origin) with another source (source destination). After merging, the source origin will be deleted and source changes will be reflected in the Audit log (Example: Source A becomes Source B).

The command does not affect date stamps nor does it require a recalculation of scoring.

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Place the application into maintenance mode - see the Maintenance Mode topic.
4. Run the following command:

```
sudo php artisan threatq:merge-sources --origin-source="<source a>" --destination-source-e="<source b>"
```

5. Optionally, append the `--no-interaction` parameter, which runs the command without requiring user confirmation. The command would run as follows:

```
sudo php artisan threatq:merge-sources --origin-source="<source a>" --destination-source-e="<source b>" -n
```

6. Bring the application out of maintenance mode - see the Maintenance Mode topic.

Example Scenarios:

Scenario	Details
Merge user-created source (origin source) with a system source (destination source).	1. User places the platform into main-

Scenario	Details
	tenance mode. 2. User runs Source Merge command. 3. User is presented with merge confirmation dialog. 4. User consents to the merge. 5. The platform will merge the origin source into the destination source and then delete the origin source after completion. 6. The platform will record the source merge in the audit log for affected data. 7. User receives a command success message. 8. User brings the platform out of maintenance

Scenario	Details
	mode.
Merge system source (origin source) with a user-created source (destination source).	1. User places the platform into maintenance mode. 2. User runs Source Merge command. 3. The platform will inform the user that a system source cannot be merged into another source. 4. User brings the platform out of maintenance mode.
Merge user-created source (origin source) with a system source (destination source) with duplicate records.	1. User places the platform into maintenance mode. 2. User runs Source Merge command. 3. The platform will inform the user that there are duplicate records between the two

Scenario	Details
	sources and prompt the user to run the Source Consolidation Command before proceeding with the merge. 4. User runs the Source Consolidation command. 5. User runs Source Merge command. 6. User is presented with merge confirmation dialog. 7. User consents to the merge. 8. The platform will merge the origin source into the destination source and then delete the origin source after completion. 9. The platform will

Scenario	Details
	record the source merge in the audit log for affected data. 10. User receives a command success message. 11. User brings the platform out of maintenance mode.
Merge user-created source (origin source) with a system source (destination source) with an assigned TLP.	1. User places the platform into maintenance mode. 2. User runs Source Merge command. 3. User is presented with merge confirmation dialog. 4. User consents to the merge. 5. The platform will merge the origin source into the destination source, and then delete the origin

Scenario	Details
	source after completion. 6. The platform will then apply the destination source's default TLP settings to the merged data and record the source merge in the audit log for affected data. 7. User receives a command success message. 8. User brings the platform out of maintenance mode.

Feed Activity Log

The feed activity log summarizes each feed run, including information such as how the feed was triggered, its start time, completion time, the raw response received from the feed vendor, and how many objects were processed.

The activity log is currently available for the following Configuration-Driven Feeds (CDF):

Commercial Feeds

- CrowdStrike
- Cofense Intelligence (formerly known as Phishme Intelligence)
- Emerging Threats IQRisk Rep List FQDNs
- Emerging Threats IQRisk Rep List IPs

OSINT Feeds

- AlienVault OTX
- All abuse.ch feeds, except for abuse.ch SSBL (Extended)
- Bambenek
- BitSight
- CI Army List IPs
- Cybercrime Tracker
- Emerging Threats Block IPs
- Emerging Threats Compromised IPs
- malc0de Domain
- malc0de IP
- Malware Domain List (IP)
- Malware Patrol
- Phishtank
- www.dan.me.uk Tor Node List

Viewing a Feed's Activity Log

To view a feed's activity log, that feed must be enabled.

Procedure

1. From the main menu, choose the **Settings icon > Incoming Feeds**.
2. Choose a feed and expand **Feed Settings**.
3. Choose the **Activity Log** tab.

Historic Feed Pulls

Historic pulls provide a method for you to ingest threat intelligence data from a particular vendor prior to the date you enabled the incoming feed. The procedure for running historic feeds varies based on the type of feed.

See the following topics for more information:

- Feeds that do not Support Historic Pulls
- Performing Manual Feed Runs
- iSight Historic Pull Command
- General Historic Pull Commands
- Threat Intelligence Services Custom Feeds Historic Pull Commands

Feeds that do not Support Historic Pulls

The following feeds do not support historic pulls:

- All OSINT feeds
- The following Commercial Feed:
  - DeepSight

Performing Manual Feed Runs

For some feeds, you can perform a manual feed run for a selected date range. This allows you to generate a historic feed pull from the user interface.

You can perform a manual feed run for the following feeds:

- CrowdStrike

Procedure:

1. From the main menu, choose the **Settings icon > Incoming Feeds**.
2. Select a feed and expand **Feed Settings**.
3. Click **+Manual Run**.
4. Select a **Start Date**, **Start Time**, and **Time Zone** for your run.
5. Select an **End Date**, **End Time**, and **Time Zone** for your run.
6. Click **Queue Run**.

iSight Historic Pull Command

To run an iSight historic pull, run the following command from the command line, substituting your desired start and end date:

```
sudo isight_connector -s MM-DD-YYYY -e MM-DD-YYYY
```

General Historic Pull Commands

If not called out specifically in Historic Feed Pulls, use the following commands at the command line to run historic pulls for most other connectors, including most TAXII feeds.

1. Run the following command to determine the feed name ($FEEDNAME):

   ```
   tqconnector -h
   ```

   Take note of the desired feed name.

2. Run the following command to run the historic pull, substituting your desired start and end date:

```
sudo -u threatq tqconnector -f $FEEDNAME -s MM-
DD-YYYY -e MM-DD-YYYY
```

Threat Intelligence Services Custom Feeds Historic Pull Commands

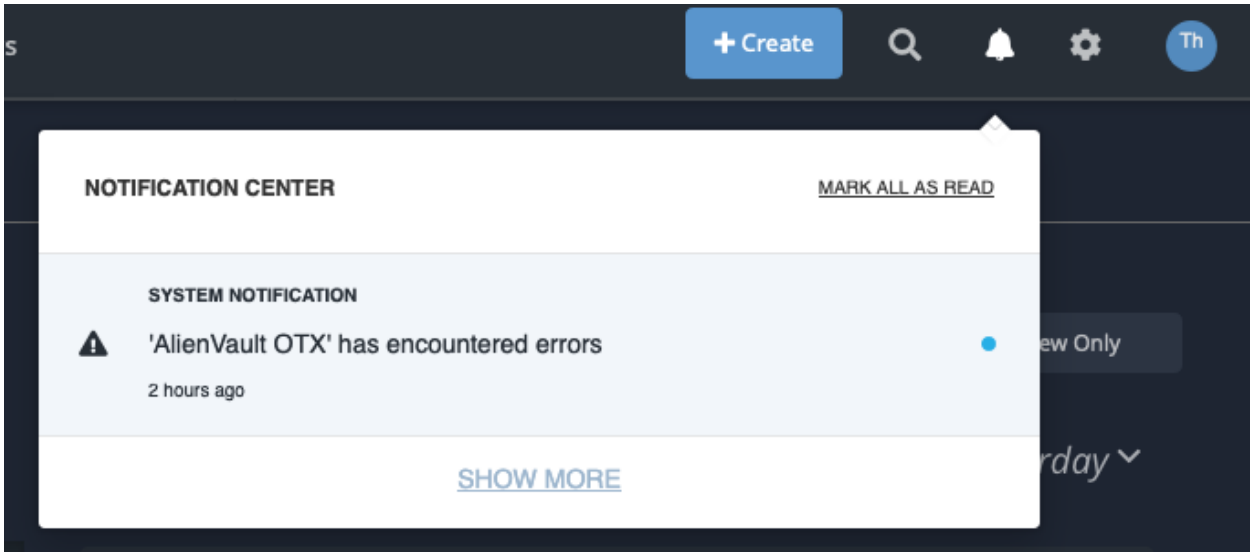
Custom feeds provided by Threat Intelligence Services provide a mechanism for you to generate a historic pull during the initial feed run. After the initial feed run, feeds typically perform an hourly pull, but can be adjusted within cron.

Refer to the documentation for your custom feed or integration for more information.

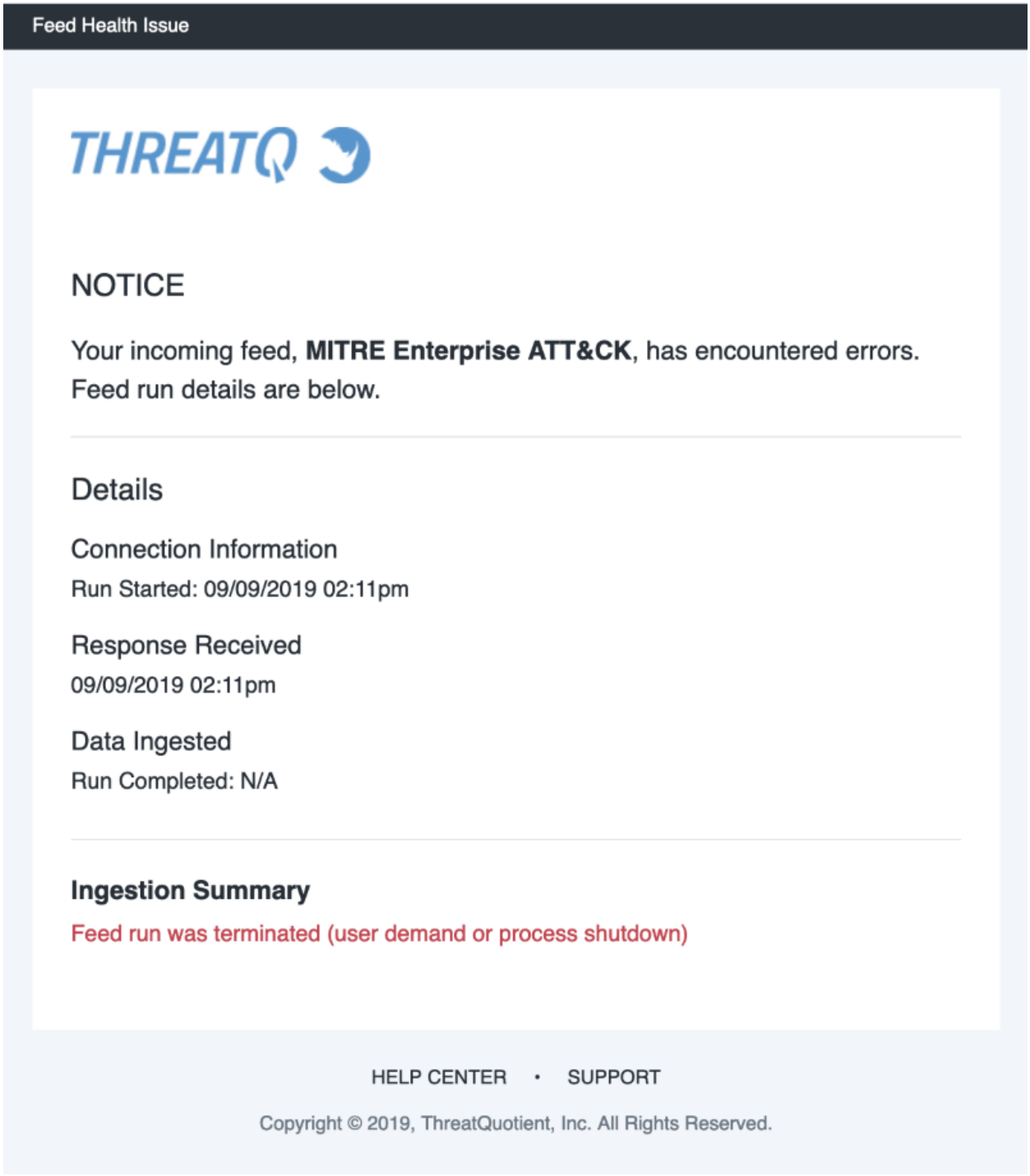
Feed Health Notifications

Feed Health Notifications allows the ThreatQ application to send you, and other designated users, email and in-app notifications when a feed encounters an issue.

The in-app notifications will appear in Notification Center for users with an administrator or maintenance account.



The emails, sent to users designated on the Notification Settings page, will contain useful information such as connection information, data ingested, and an ingestion summary.



See the Notification Settings topic for more information.

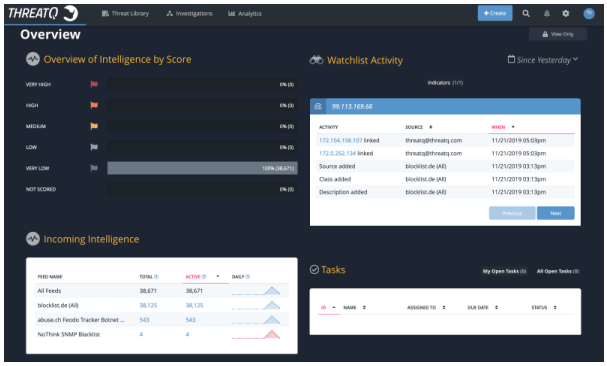
Dashboard

The following describes how to use the dashboard to view various threat intelligence metrics.

- Default Dashboard (Overview)
- Custom Dashboards

Default Dashboard (Overview)

The system default dashboard, Overview, displays metrics and visualizations to provide at-a-glance views of your threat intelligence data.



Views include:

- Overview of intelligence by score
- Watchlist activity
- Incoming intelligence
- Open assigned tasks

The dashboard serves as your landing page when you log in to ThreatQ.

You can create your own custom dashboards using system widgets. See the Custom Dashboards topic for more details.

Related Topics:

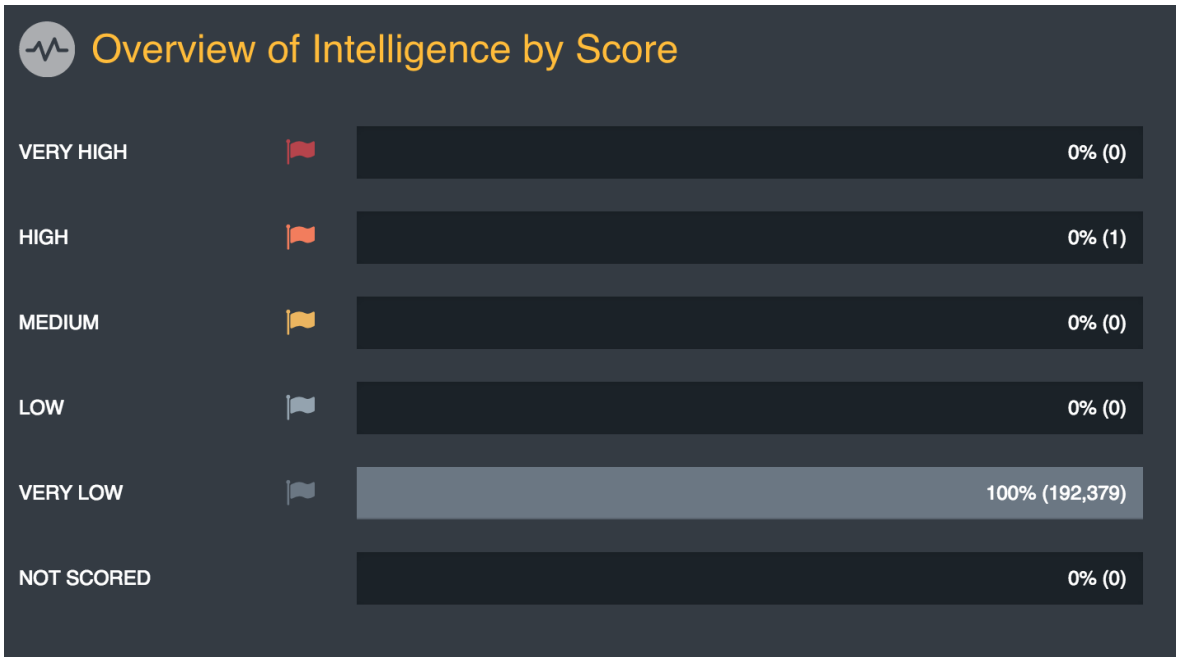
- Overview of Intelligence By Score
- Watchlist Activity
- Viewing Tasks on the Dashboard
- Custom Dashboards

Overview of Intelligence By Score

This dashboard graph provides a summary of indicator scoring in the system. It lists total indicators by score in the following order:

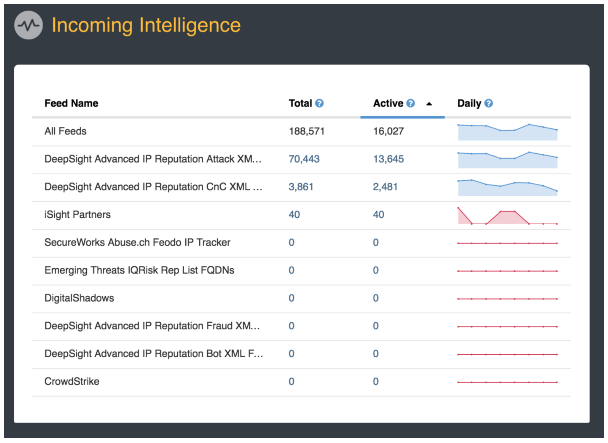
- Very High
- High
- Medium
- Low
- Very Low
- Not Scored

You may click on the percentage/number of indicators to launch an advanced search based on that criteria.



Incoming Intelligence

This dashboard graph provides a view of threat intelligence from all incoming feeds.



The system categorizes threat intelligence by:

- Feed Name
- Total number of indicators reported by a source
- Indicators reported by a source with a status of active
- All indicators reported by a source per day (includes existing indicators)

Clicking on the **Total** and Active values will navigate you to the Threat Library Advanced Search page with the appropriate filters applied

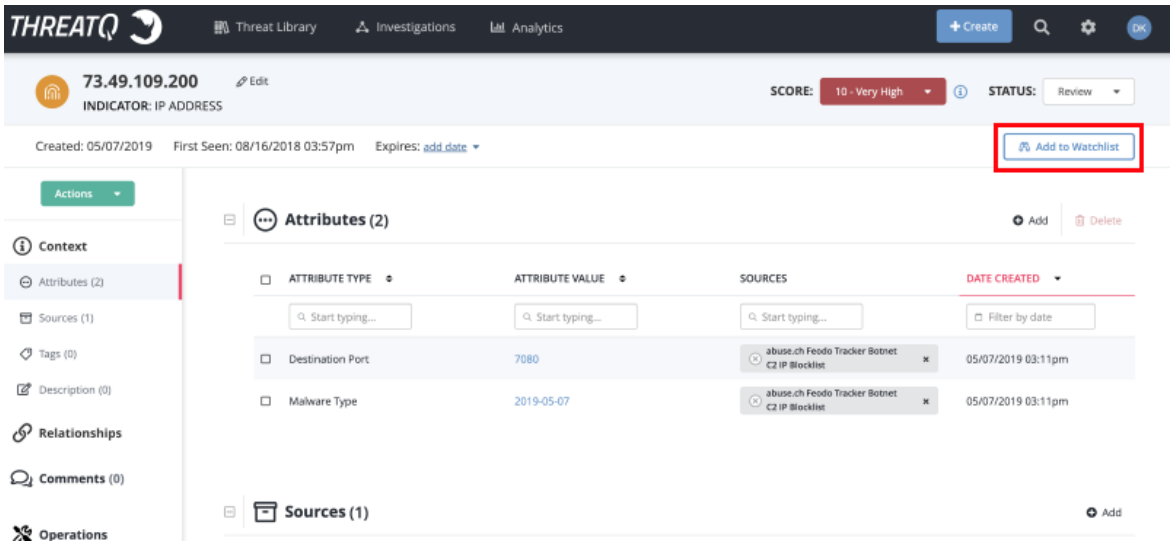
Watchlist Activity

This dashboard section provides a view of the intelligence data that you selected to watch. You may click on any accompanying link to view the details page of the item being watched.

Configuring the Watchlist

To create a watchlist that displays on the dashboard, complete the following steps:

1. From the ThreatQ user interface, navigate to the Details page of the indicator, event, adversary, file, or signature you want to track.
2. Click **Add to Watchlist** to track that item.



3. Return to the dashboard to view your watchlist.

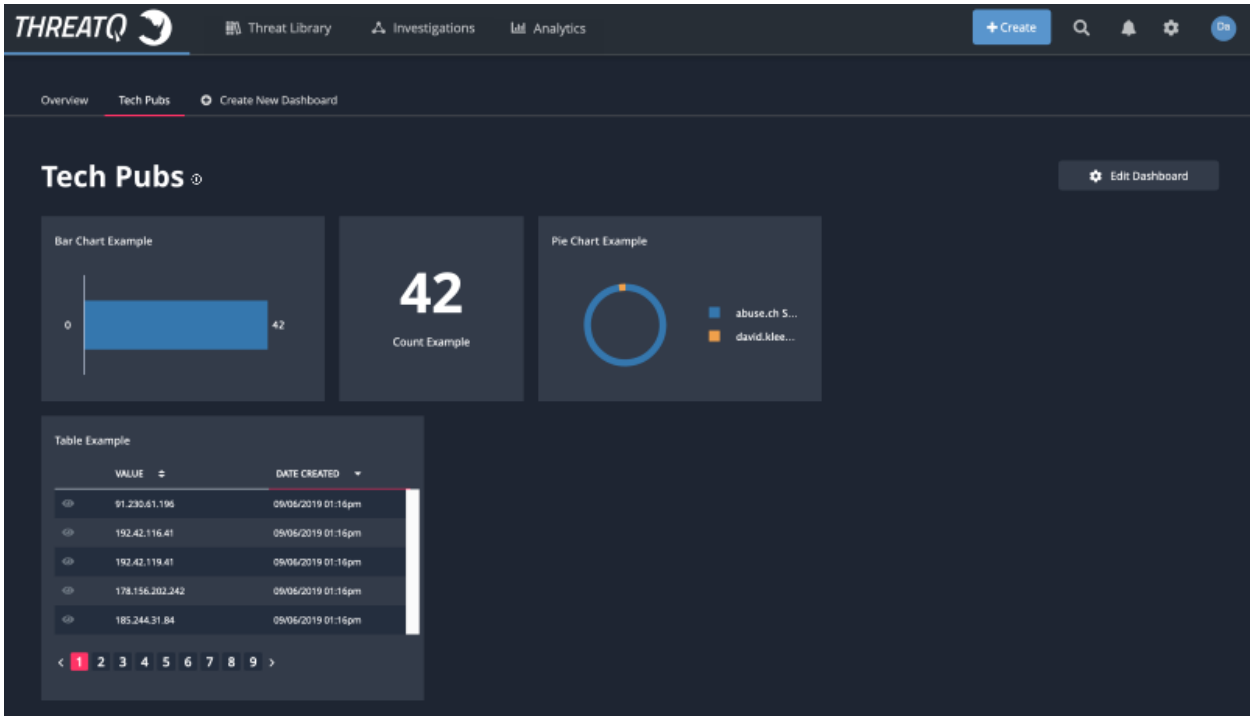
Viewing Tasks on the Dashboard

This dashboard widget provides a view of all open tasks in the platform. You can view your open tasks or view all open tasks. Tasks on the dashboard are categorized by:

- Task ID
- Task Name
- User the Task is Assigned To
- Due Date
- Status.

Custom Dashboards

You can create and share multiple custom dashboards to be used on the ThreatQ landing page.



Each dashboard is comprised of system widgets which are populated by data derived from saved searches. You can click on an individual segment of data within a widget to view it in the ThreatQ Threat Library. See the Dashboard Widgets topic for details.

With the dashboard sharing option, you can determine which dashboards you want to share with other users and which ones you want to keep private. See the Dashboard Sharing topic for more details.

You can control which shared dashboards created by other users appear in your view. You can also remove your own dashboards from your view without deleting them from the platform. See the User View Management topic for more details.

Related Topics:

- Dashboard Management
- Dashboard Widgets
- Dashboard Sharing
- User View Management

Dashboard Widgets

Custom dashboards are comprised of system widgets, populated by data derived from saved searches, that provide a graphical representation of your threat data. Once deployed, you can click on an individual segment of data within a widget to view it in the ThreatQ Threat Library.

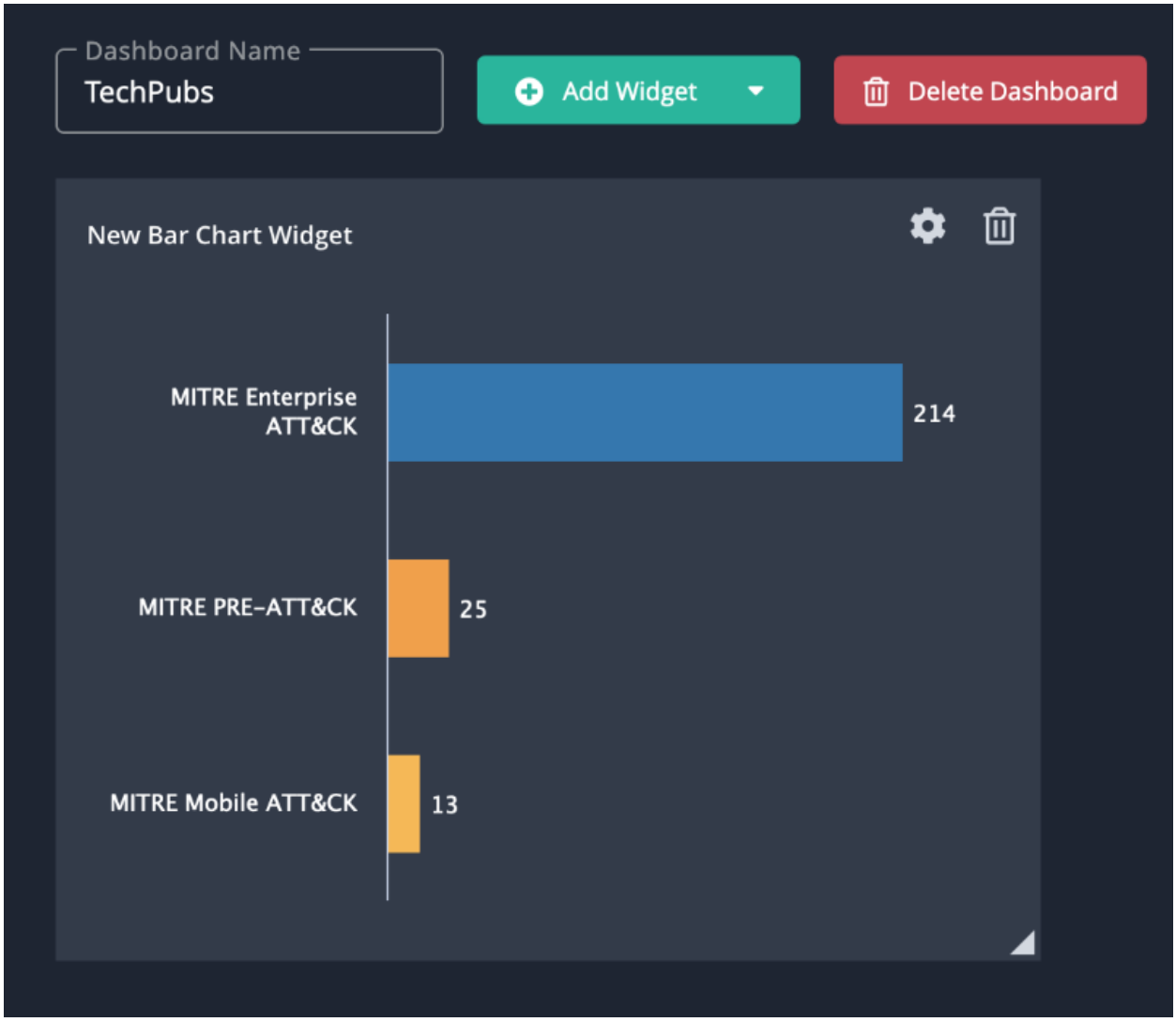
There are four different types of widgets you can deploy:

- Bar Charts
- Count
- Pie Charts
- Tables

Bar Charts

You can click on individual bars within the chart to view those results in the Threat Library.

Complete the following fields to add a Bar Chart widget to your custom dashboard.

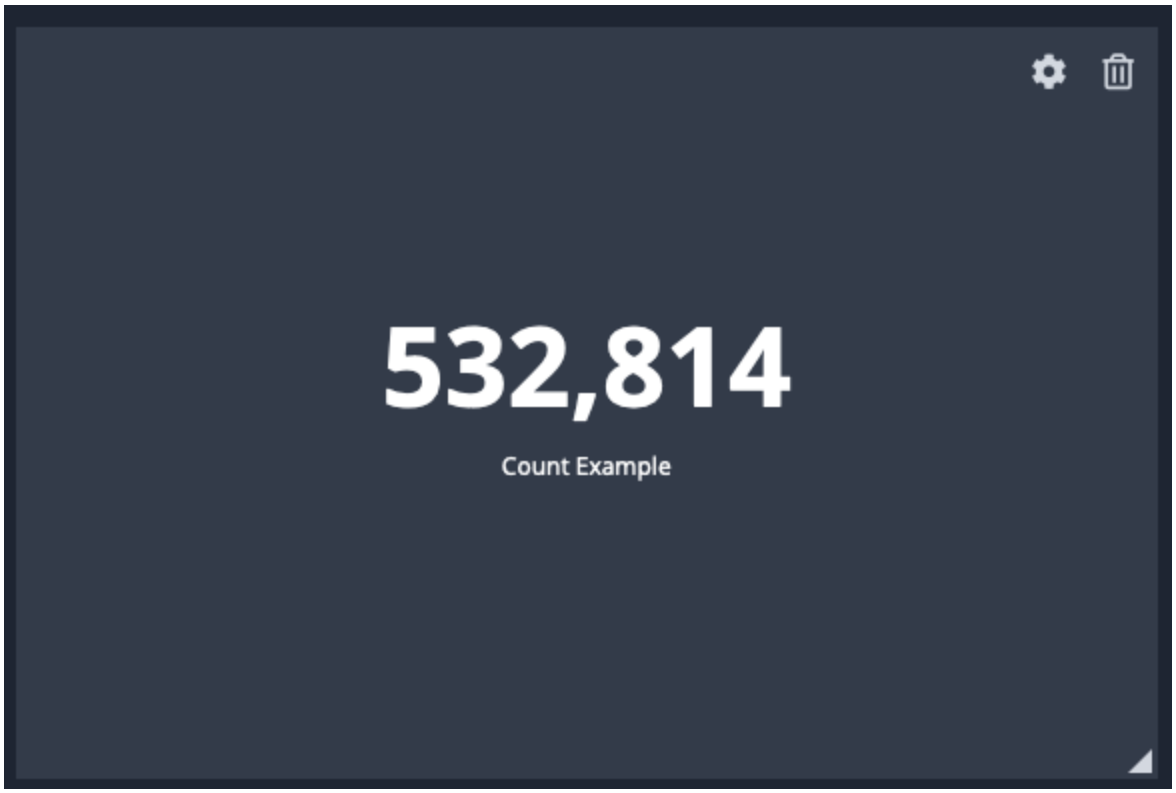


Field	Description
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes • None

Field	Description
Saved Search	Select the Saved Search to populate the data.
Object	Select a specific object type to display.
Group By	Select a data column to sort the information such as source, tags, etc.
Visual Display	Select whether to show the bar chart horizontally or vertically.
Show Top Options	Select the number of results to display. Options include: • Top 5 • Top 10

Count

The Count widget displays the total number a specific object type. You can configure the widget to display a different background color if the total number of objects associated with the widget is above or below a specific value.



Complete the following fields to add a Count widget to your custom dashboard.

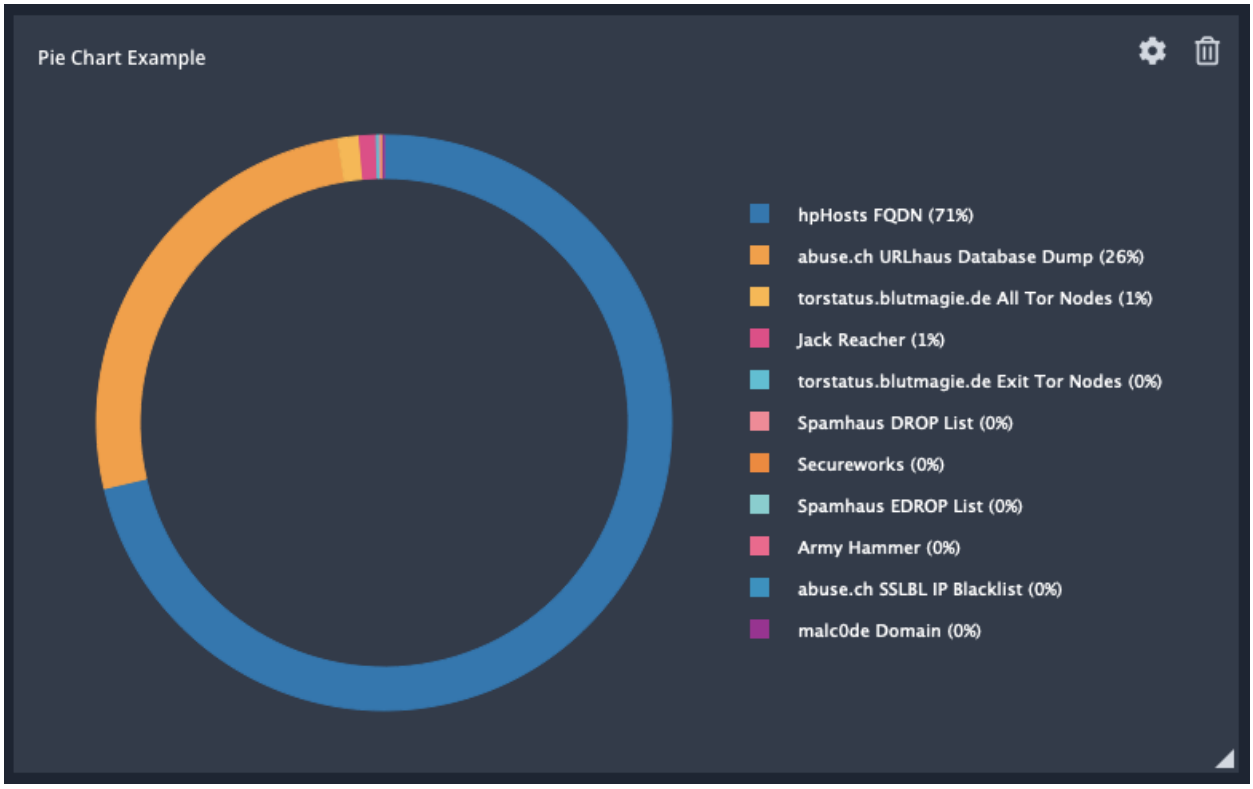
Field	Description
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include:

Field	Description
	• 15 Minutes • 30 Minutes • 60 Minutes • None
Data to Show in Widget	Select the Saved Search to populate the data.
Object	Select a specific object type to display.
Emphasize Data Using Color	Check this box to use different colors to highlight the widget if the count is less than or greater than a specific value. If checked, you will be prompted to select a count value and background color.

Pie Charts

You can click on individual segments within the chart to view those results in the Threat Library.

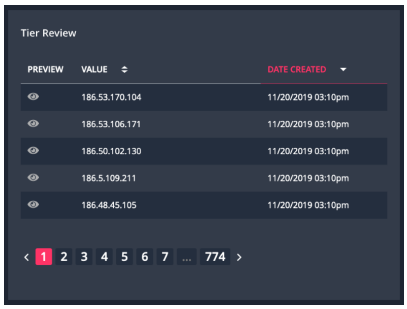
Complete the following fields to add a Pie Chart widget to your custom dashboard.



Field	Description
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes • None
Saved Search	Select the Saved Search to populate the data.
Object	Select a specific object type to display.
Group By	Select a data column to sort the information such as source, tags, etc.

Tables

Table widgets allow you to add as many column fields as needed. You can click on a row's **value** entry to view it in the ThreatQ Threat Library. You can also click on the **eye** icon for a row to view a preview of the system object.



Complete the following fields to add a Table widget to your custom dashboard.

Field	Description
Title	The title that will appear above the widget.
Automatically Update	The refresh time for the data. Options include: • 15 Minutes • 30 Minutes • 60 Minutes • None
Saved Search	Select the Saved Search to populate the data.
Object	Select a specific object type to display.
Group By	Select a data column to sort the information such as source, tags, etc.
Manage Columns	Select the data columns to display in the table.
Sorting	Select the column to sort the table and the order (ascend-

Field	Description
	ing/descending).

Dashboard Management

Users with permission roles of Primary Contributor Access, Administrative Access, Maintenance Account can :

- Create a Dashboard
- Edit a Dashboard
- Delete a Dashboard
- Reassigning a Dashboard of a Deleted User
- Set Sharing Settings for a Dashboard

Users with the Read-Only Access role cannot create custom dashboards but can add shared dashboards to their view.

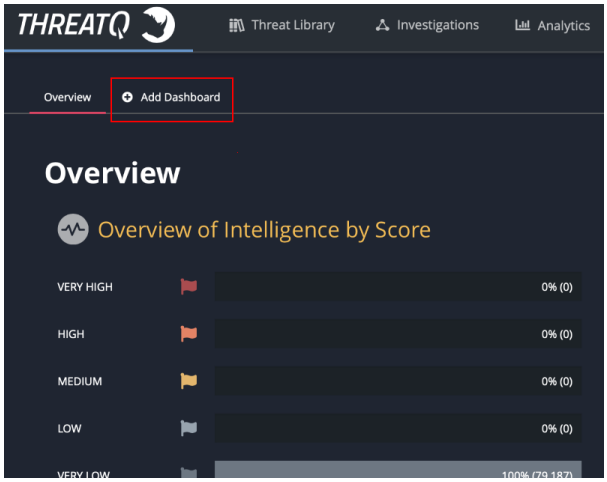
Related Topics

- Dashboard Widgets
- Dashboard Sharing
- User View Management

Creating a Dashboard

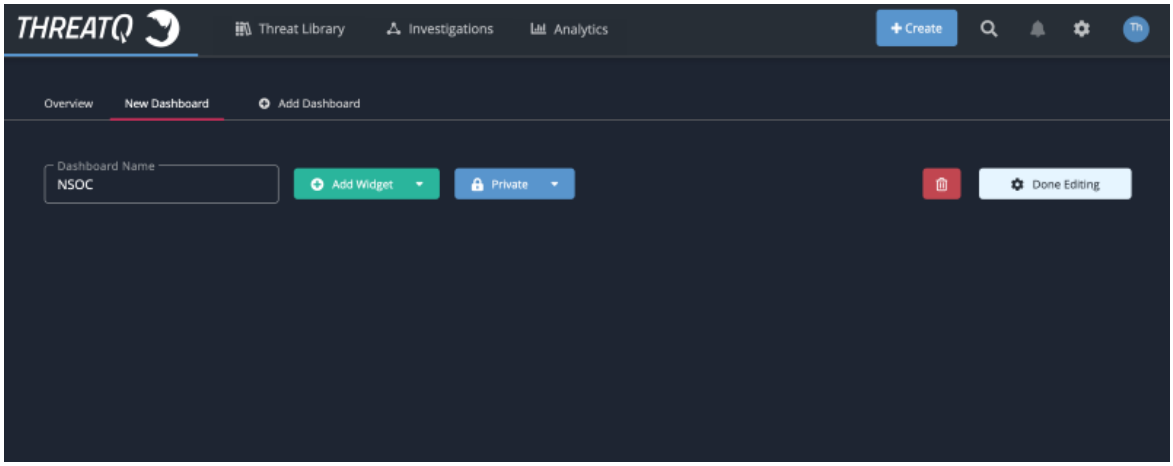
Perform the following steps to create a custom dashboard:

1. Navigate to the ThreatQ landing page.
2. Click on **Create New Dashboard**.

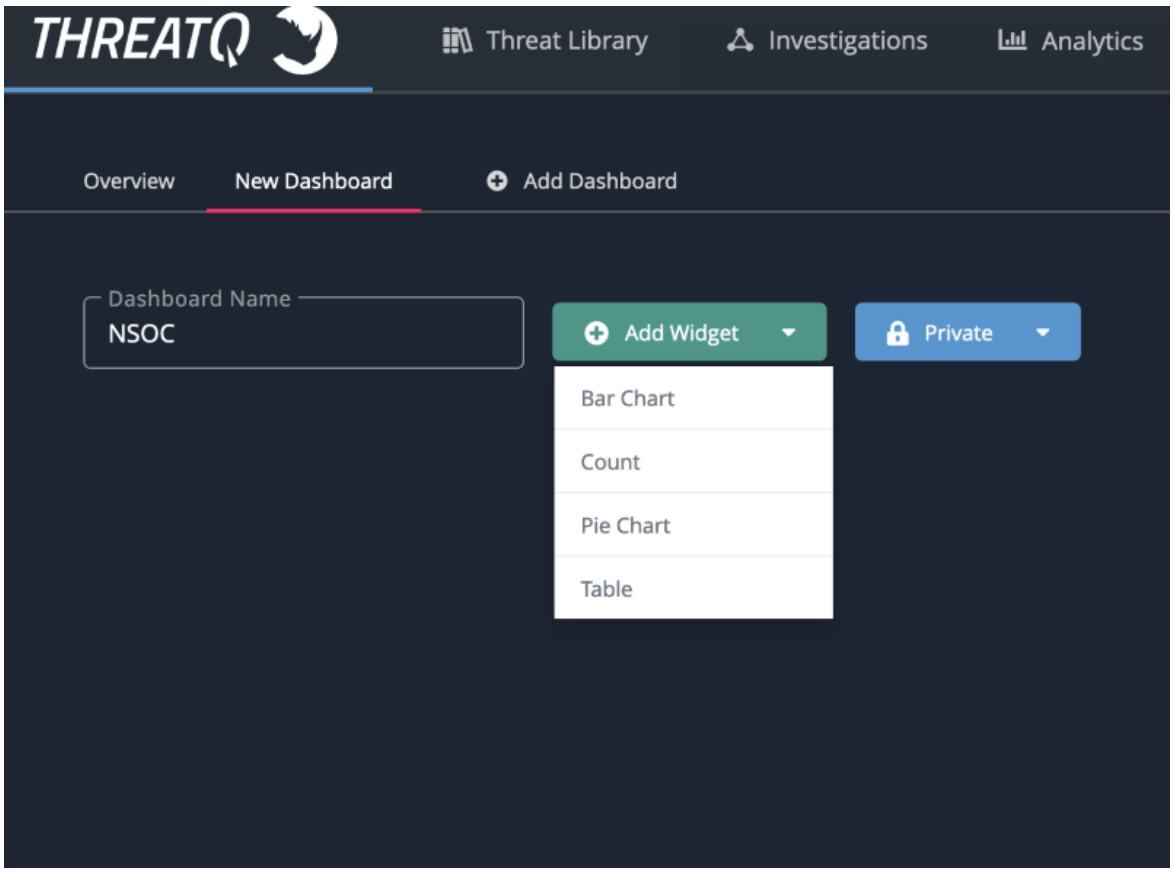


> If there are available shared dashboards or if you have any of your own dashboards that are not part of your current view, the **Create New Dashboard** link will be replaced with **Add Dashboard**. Clicking on the **Add Dashboard** link will open the dashboard dialog box with a list of available dashboards not current part of your view. Click on the **Create New Dashboard** link at the bottom of the dialog box.

3. Enter the **Dashboard Name**.



4. Click on **Add Widget** and select the type of widget to add.

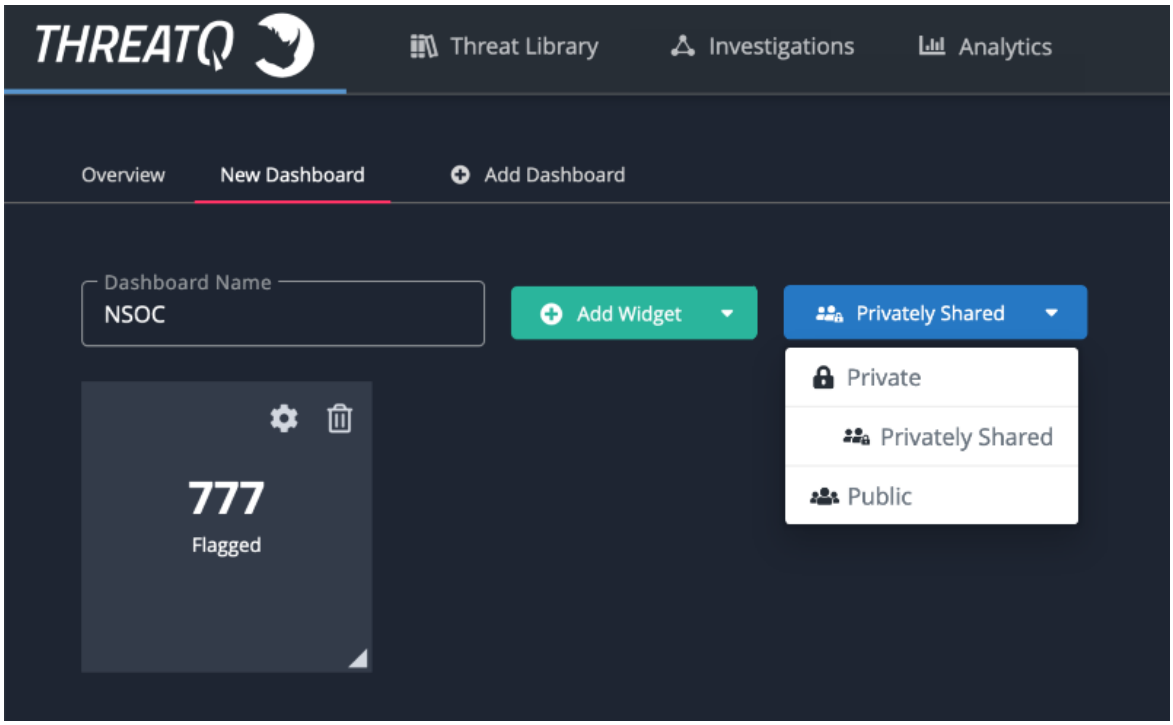


Options include:

- Bar Charts
- Pie Charts
- Count
- Tables

5. After adding a widget, you can resize it by clicking and dragging the mouse on the bottom-right grey corner.
6. You can move the widget around the dashboard by clicking on the widget header and dragging it around the page.

7. Click on the **Sharing** dropdown and select whether the new dashboard will be private or public. See the Dashboard Sharing topic for more details.

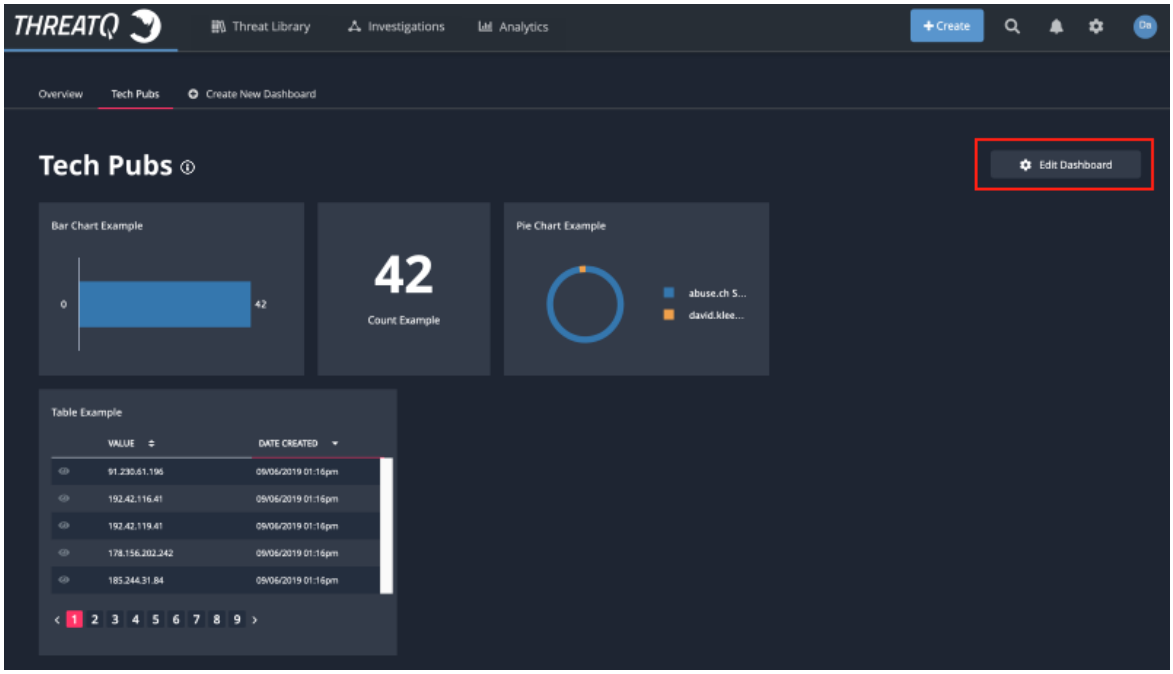


8. Click on **Done Editing** to save the dashboard.

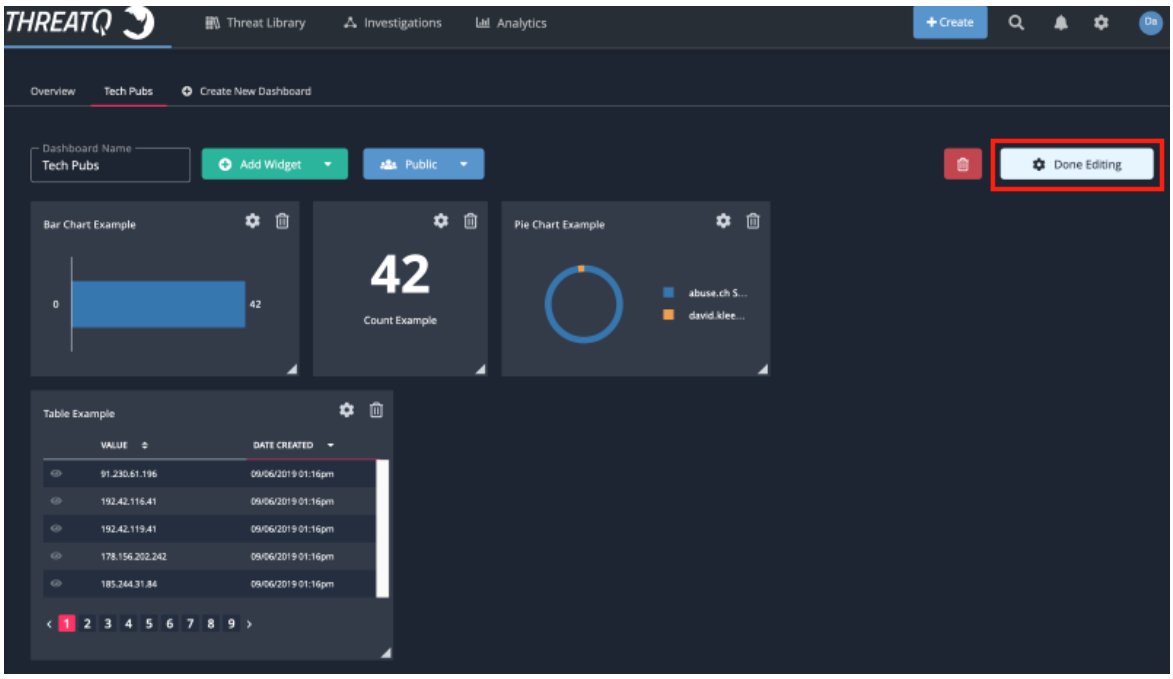
Editing a Dashboard

You can only edit a Dashboard that you have created. If you are viewing a dashboard created by another user, you will see a **View Only** icon in place of the **Edit Dashboard** link.

1. Switch to the custom dashboard to edit.
2. Click on **Edit Dashboard**.



3. Make your desired changes to the dashboard then click on **Done Editing** to save all updates.



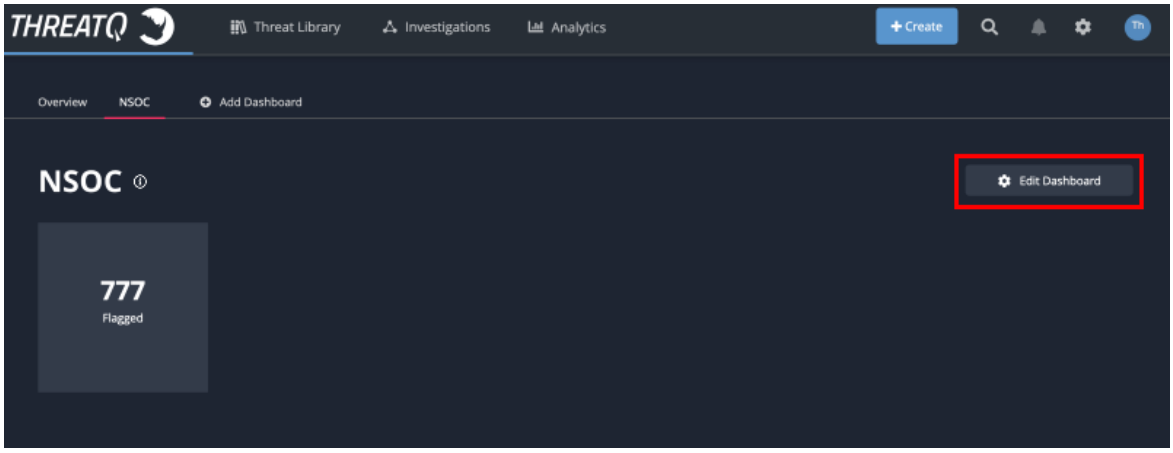
You can click on the gear icon in the header of a widget to edit individual widget settings. You can click on the delete icon to delete the widget.

Deleting a Dashboard

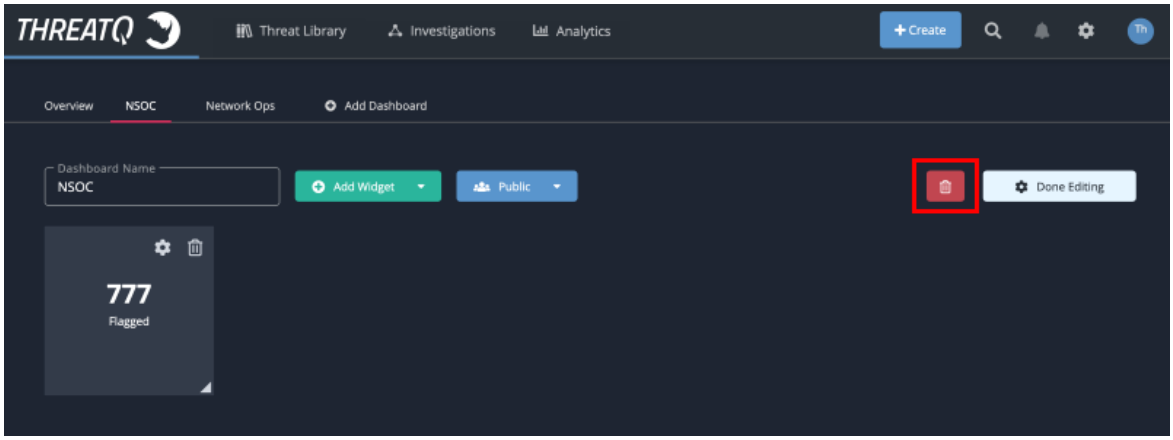
This action will delete the dashboard from the platform. You can also remove a dashboard from your view without completely deleting it from the platform. See the User View Management topic for more details.

You can not delete the default system dashboard or dashboards created by other users.

1. Switch to the custom dashboard to edit.
2. Click on **Edit Dashboard**.



3. Click on red delete icon next to the **Done Editing** button.



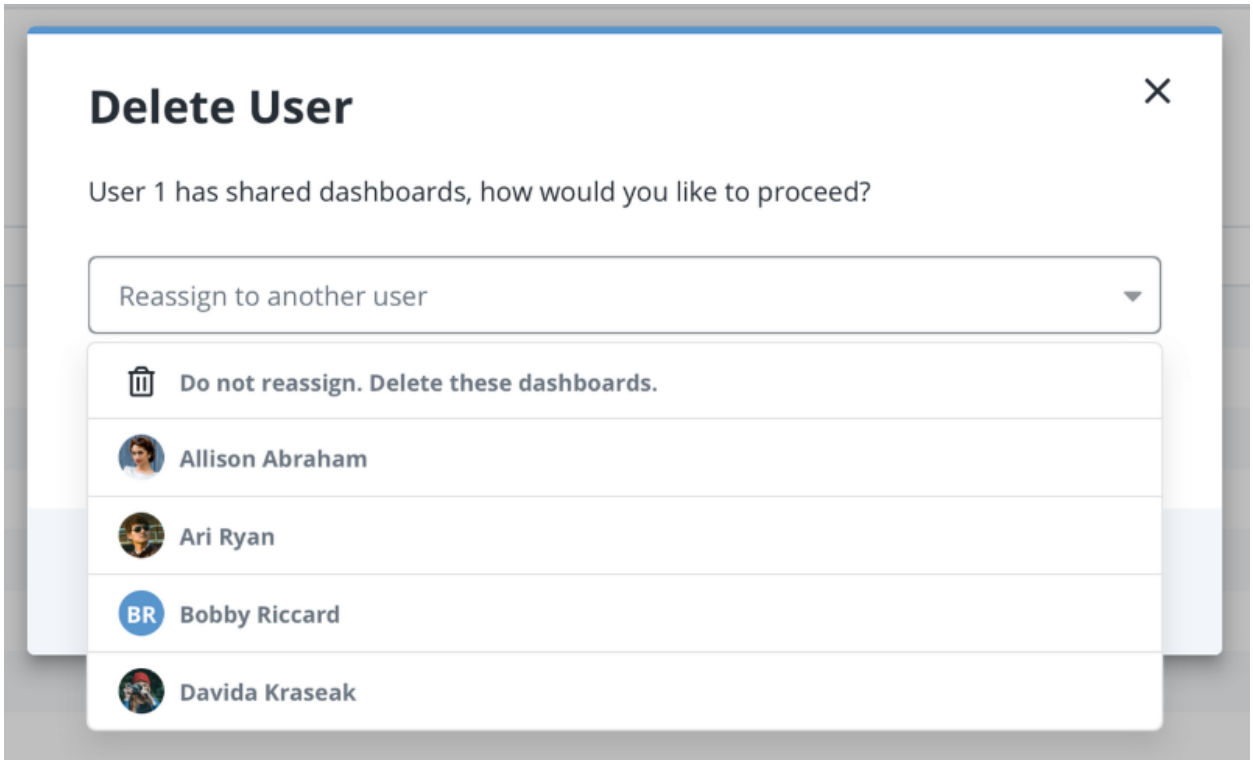
Reassigning a Dashboard of a Deleted User

Publicly and Privately Shared dashboards that are owned by a user being deleted from the platform can be reassigned during the deletion process.

Private Dashboards will be deleted along with the user.

When deleting a user, the ThreatQ platform will notify the administrator if the user has any shared (sharing setting of Public or Privately Shared) dashboards in use. The administrator at that point can decide whether to delete the dashboards associated with that user or reas-

signed ownership to another user.



See the Deleting a User topic for more details.

Dashboard Sharing

You have the ability to configure how your dashboards are shared across the ThreatQ platform.

ThreatQ provides three sharing options:

Share Option	Description
Private	Only the dashboard owner can view and edit the dashboard. This is the default sharing setting.
Privately Shared	Only individuals selected by the dashboard owner can add the dashboard to their view. Only the dashboard

Share Option	Description
	owner can edit the dashboard and the sharing control.
Public	All users can add the dashboard to their view. Only the dashboard owner can edit the dashboard. All custom dashboards created before ThreatQ version 4.25 will be set to **Public** by default.

Related Topics:

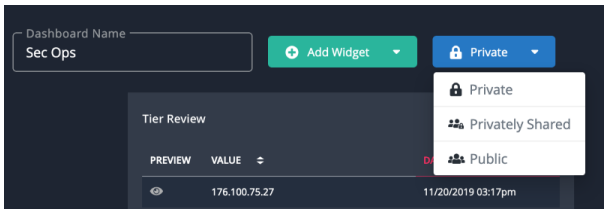
- Setting Dashboard Sharing
- Editing Privately Shared Users
- Shared Dashboards of a Deleted User

Setting Dashboard Sharing

You can update sharing settings for a dashboard at any time.

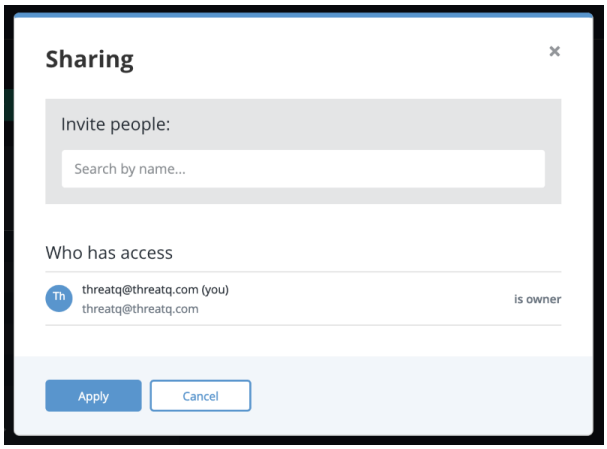
To update a dashboard's sharing setting:

1. Enter a dashboard's **Edit** view.
2. Click on the **Sharing** dropdown and select a sharing option.



3. If you selected **Private** or **Public**, click on **Done Editing** to save changes. If you selected **Privately Shared**, continue through steps 4-8.

4. The **Sharing** dialog box will open. You can view who currently has access to the dashboard.

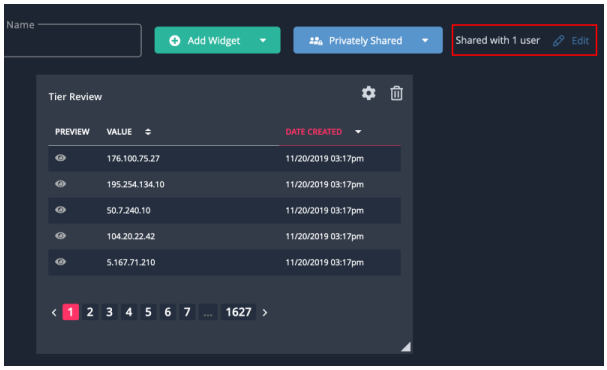


5. Enter a user's name in the **Invite People** field. The platform will return system users that fit the name criteria. Click on the correct user.
6. The user will now appear under the **Who has access** section of the dialog box.

> Repeat steps 5-6 to share with additional users.

7. Click on **Apply**.

   You will now see **Shared with x user** text next to the sharing dropdown where the x is the number of users the dashboard is currently being shared with. You will also see an **Edit** link next to the text that will allow you to further edit the list of users.



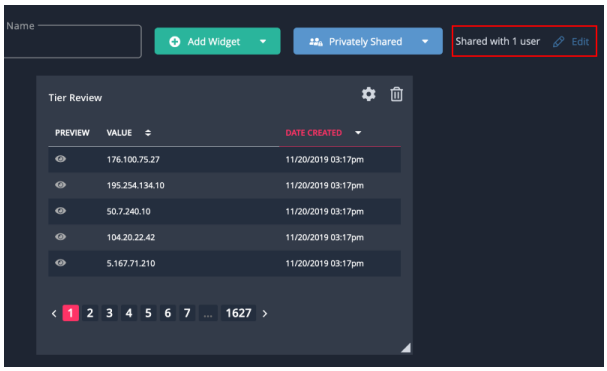
8. Click on **Done Editing** to save changes.

Editing Privately Shared Users

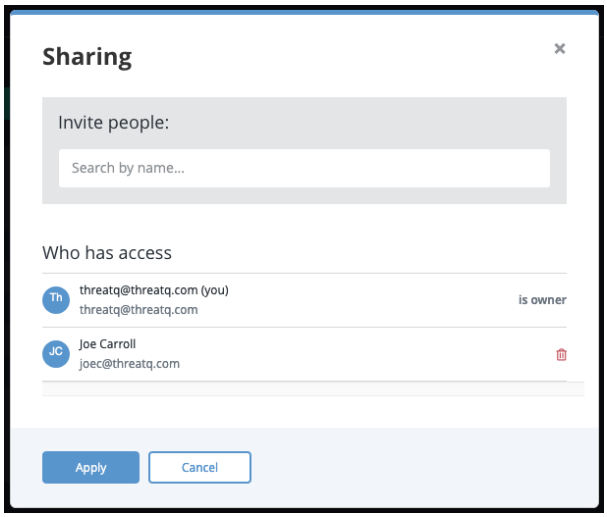
You can add and remove user access for privately shared dashboard.

To edit the privately shared list of users:

1. Enter a dashboard's **Edit** view.
2. Click on **Edit** link to the right of the **Sharing** button.



The Sharing dialog box will open. You can view who currently has access to the dashboard.



3. Use the **Invite People** field to share with additional users. See the Setting Dashboard Sharing for more details.

4. Click on the **Delete** icon next to user under the **Who has access** section to revoke an individual's access.
5. Click on **Apply** and then **Done Editing** to save the changes.

Shared Dashboards of a Deleted User

In the scenario where a user with shared dashboards is deleted from the platform, ThreatQ will automatically reassign dashboard ownership to another user. This ensures that users can continue using those shared dashboards. See the Deleting a User topic for more details.

User View Management

The User View refers to your individual view of the ThreatQ landing page. You can create custom dashboards and manage which dashboards, both shared and your own custom ones, appear in your view.

Related Topics:

- Adding a Dashboard to Your View
- Removing a Dashboard from Your View
- Changing Dashboard Order

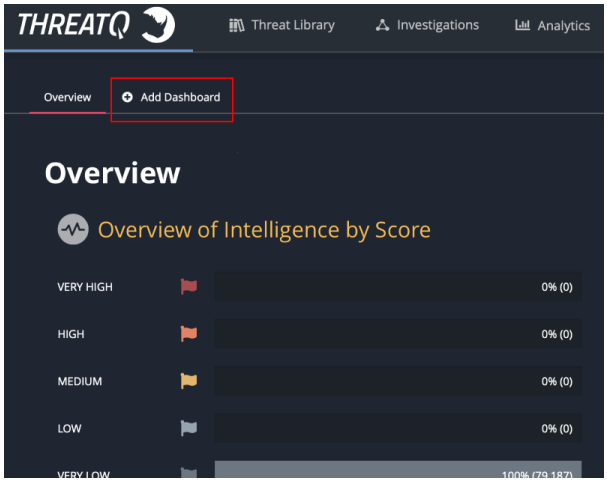
Adding a Dashboard to Your View

You can add dashboards that have been shared with you as well as your own private dashboards that not currently part of your view.

You cannot edit nor delete a dashboard that has been shared with you.

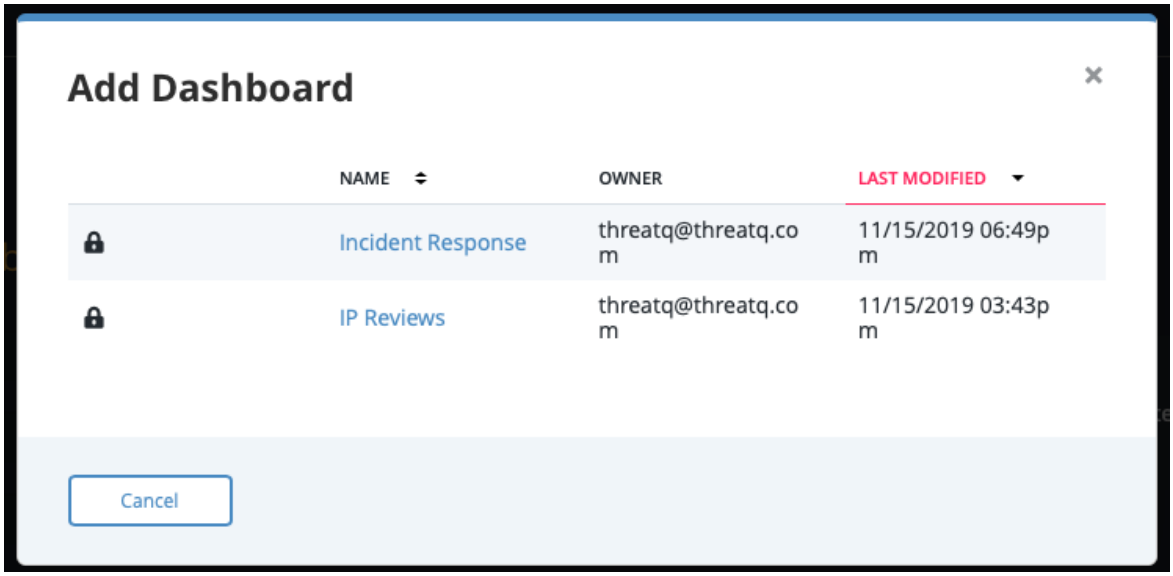
Perform the following steps to add a dashboard to your view:

1. Navigate to the ThreatQ landing page.
2. Click on **Add Dashboard**.



If there no available shared dashboards, the **Add Dashboard** link will be replaced with **Create New Dashboard**.

The dashboard dialog box opens.



> The dialog box contains a list of dashboards that have been shared with you and your own dashboards that are not currently part of your view.

3. Click on a dashboard in the list to add it to your view.

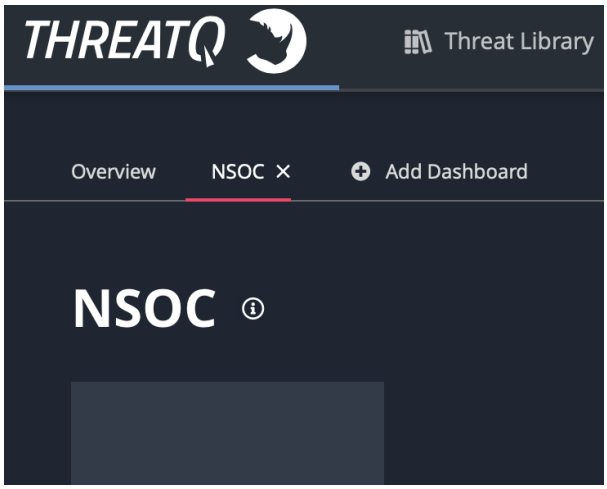
Removing a Dashboard from Your View

You can remove a shared dashboard created by another user from your view as well as your own dashboards. The process listed below does not delete the dashboard from the platform. See the Deleting a Dashboard topic for instructions on how to delete a dashboard.

Perform the following steps to remove a dashboard to your view:

1. Hover your cursor over the name of the dashboard to remove.

   An **X** icon will appear to the right of the dashboard name.



2. Click on the **X** to remove the dashboard from your view.

Changing Dashboard Order

You can change the order of dashboard tabs listed in your view, including the default Overview tab.

Perform the following steps to add a dashboard to your view:

1. Navigate to the ThreatQ landing page.
2. Click and hold the mouse down over a dashboard tab.
3. Drag the tab to your desired order and release the mouse button.

Order changes will automatically save.

Search

The following describes how to search for indicators and other objects using ThreatQ's search features.

- Search Overview
- Wildcards and Symbols in Searches

Search Overview

Search allows you to find objects you are looking for quickly, without having to browse through a large number of objects. There are three search features in ThreatQ:

- Basic Search, which offers a quick method to search if you know exactly what you are looking for.
- Advanced Search, which gives you more options for limiting your search.

  The advanced search also serves as the primary interface for the Threat Library.

- Indicator Search, which served as the legacy advanced search prior to ThreatQ version 4.0.

Using these varieties of search, you can create as broad or as granular a view of your data as desired.

For more information, see:

- Basic Search
- Advanced Search

- Indicator Search

Basic Search

Basic Search allows you to search for all objects in the system: indicators, events, adversaries, files, signatures, and so on. The search capability looks at high level aspects of each object, including:

- Indicators (network or host)
- Attachment titles, hashes, keywords
- Attributes
- Adversary name
- Event title

  If searching for *google.com*, the following indicators will also be returned:

  - www.google.com (FQDN)
  - analytic.google.com (FQDN)
  - www.google.com/analytic (URL)
  - analytic@google.com (email address)

Related Topics:

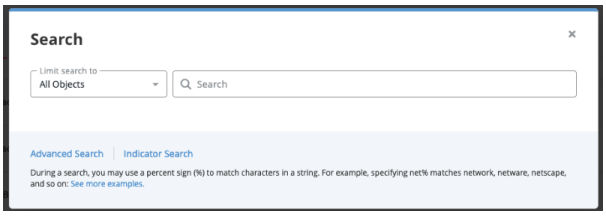
- Performing a Basic Search
- Wildcards and Symbols in Searches

Performing a Basic Search

Procedure:

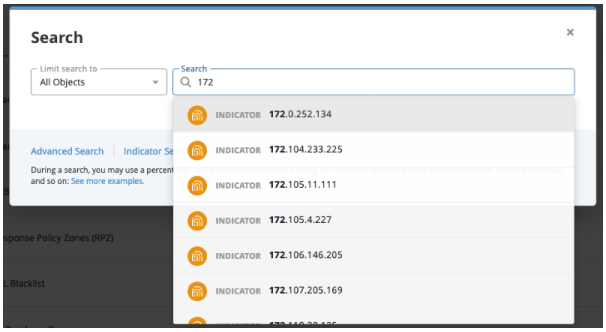
1. Choose the Search icon.

   The Search dialog box appears.



2. Use the **Limit Search** dropdown to filter your search to a specific object type.
3. Enter the search criteria.

   The Search field provides type ahead suggestions, if any, based on what you have typed. Portions of the suggestions that match your search criteria will be highlighted in bold.



4. Select the desired result.
   - If you do not retrieve any search results, we recommend trying the Advanced Search option.
   - If there is only one result, the object details page appears.

Wildcards and Symbols in Searches

During a search, you may use a percent sign (%) to match characters in a string. The percent wildcard specifies that any characters can appear in multiple positions represented by the wildcard. For example, specifying net% matches network, netware, netscape, and so on.

Here are a number of examples showing search terms with percent wildcards:

Search Query	Description
% panda	Finds any adversaries and indicators with <name> panda
%ear	Finds any character string that ends with "ear," such as bear
%panda%	Finds any character string that has panda in any position
panda%	Finds any character string that begins with panda
pan%a	Finds any character string that has pan in the first three positions and ends with an "a"

Notification Settings

The Notification Settings page allows you to configure email-based and in-app feed health notifications. You can enable/disable notifications, add/remove accounts receiving emails, and determine which feeds will be monitored for alerts.

Only System Administrators can access the Notification Settings page.

To Access the Notification Settings page:

1. Click on the **System Settings** gear icon and select the **Notification Settings** option.

You should configure mail settings on the Mail Server Configuration tab before attempting to enable email-based Feed Health Notifications.

Related Topics:

- Configuring Mail Server
- Enabling Feed Health Notifications

Configuring Mail Server

You must enter your mail server information on the Mail Server Configuration tab before enabling Feed Health Notifications.

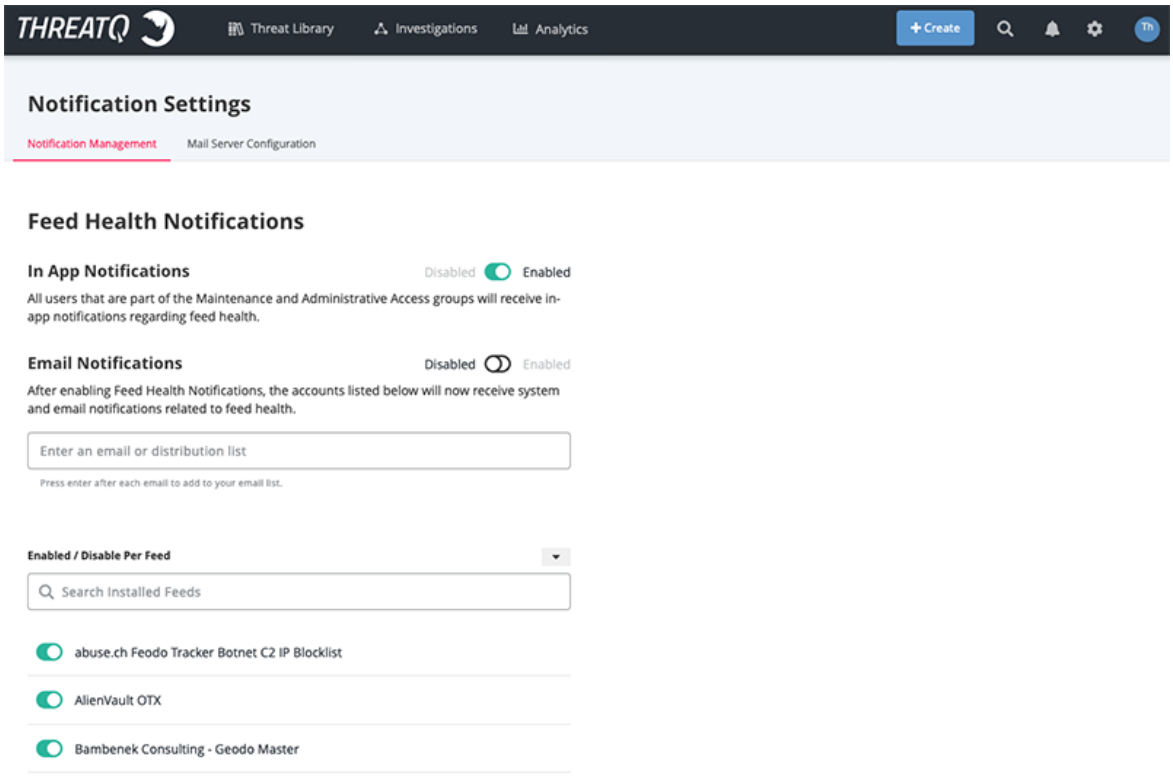
In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application to continue to use the server to send emails. A common symptom found in the error log is that you will receive an “incorrect password” error.

If you are certain that the password you provided is correct, your mail service is likely blocking the service and requires your confirmation to proceed.

To Configure Mail Server:

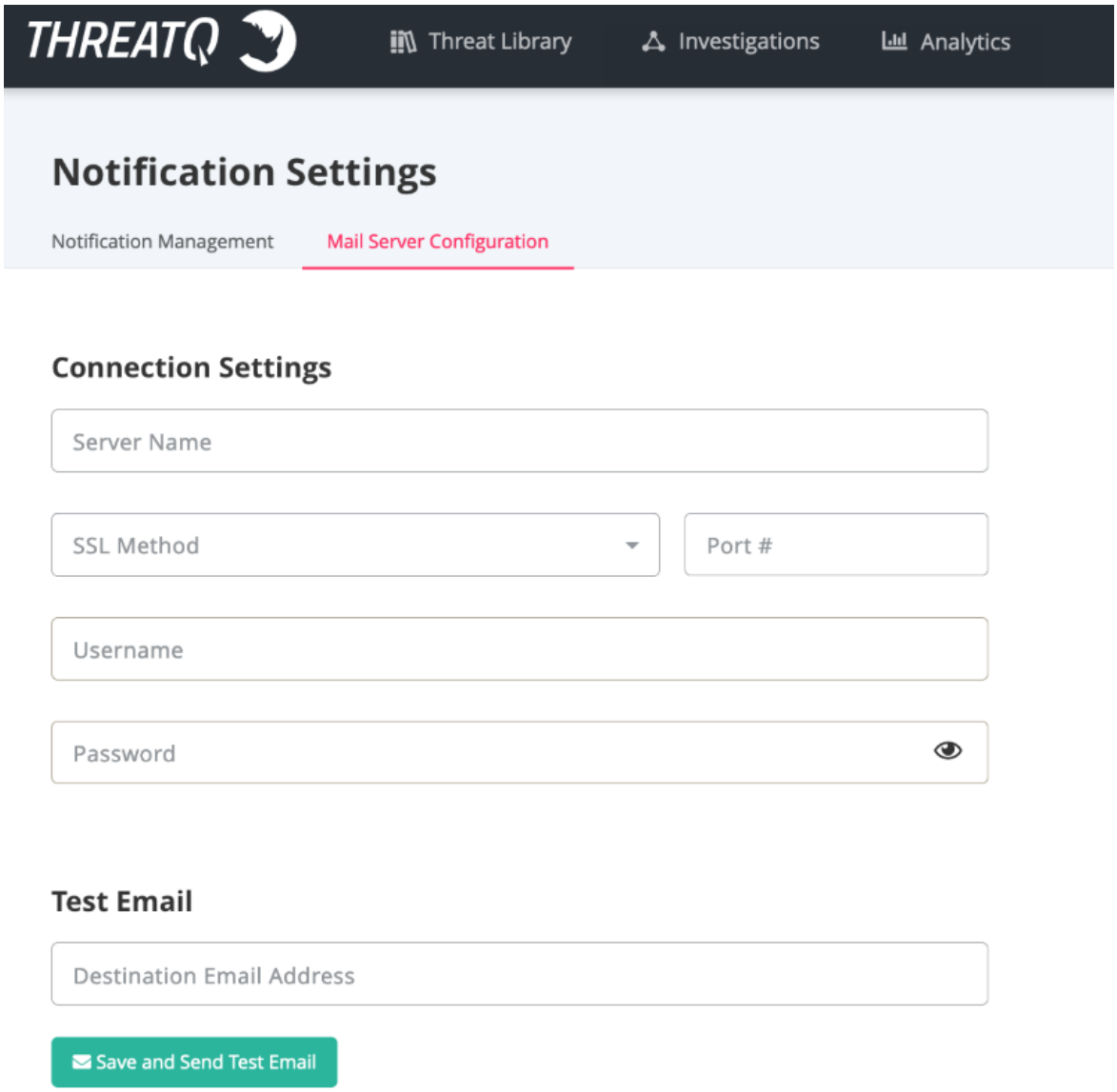
1. Click on the **System Settings** gear icon and select the **Notification Settings** option.

   The Notification Settings page loads.



2. Click on the **Mail Server Configuration** tab.

   The Mail Server Configuration page loads.

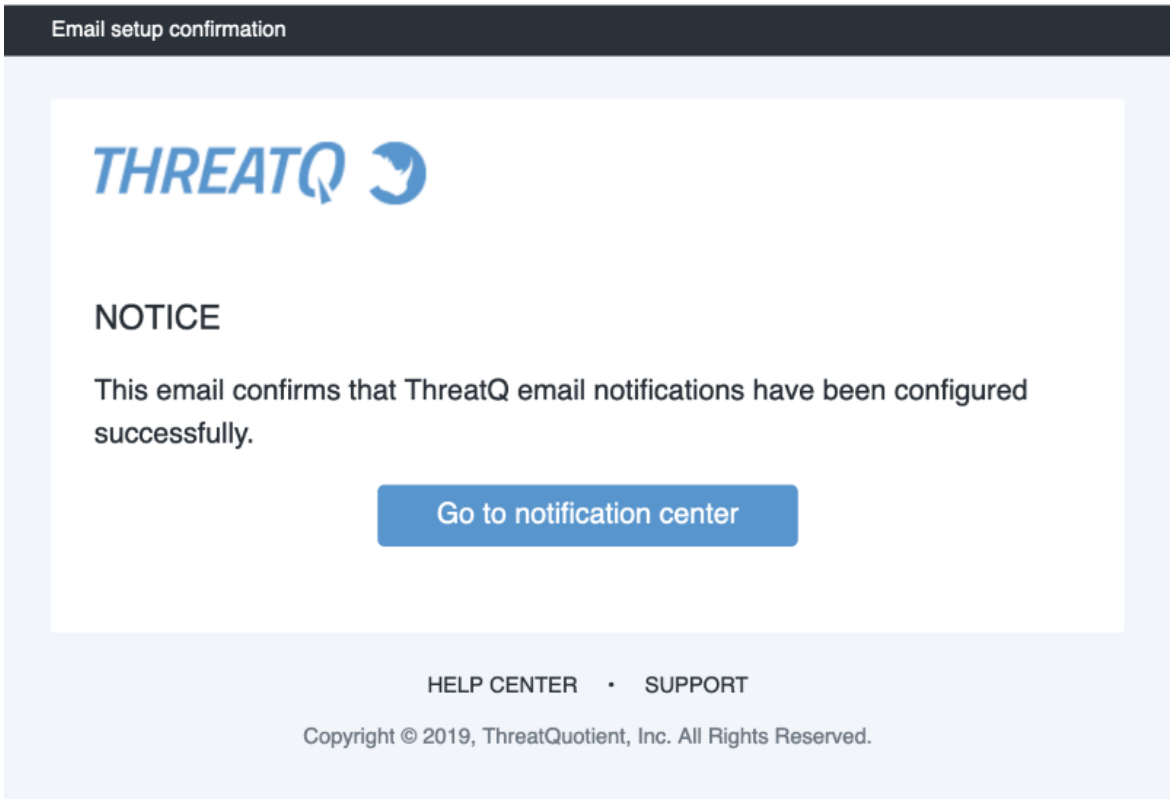


3. Complete the following fields:

Field	Description
Server Name	The address of your mail server.
SSL Method	The SSL method used. There are three options:

Field	Description
	• SSL • TLS • None
Port #	The mail server port.
User name	The mail server account username.
Password	The mail server account password.

4. Enter an email in the **Test Email** field and click **Save and Send Test Email** to confirm that the settings are correct - this is optional. You will receive a setup confirmation email.



5. If you did not use the **Save and Send Test Email** option, click on **Save Changes** to save your settings.

Enabling Feed Health Notifications

There are two different types of Feed Health Notifications that can be enabled on this page: In-App and Email. While you can enter the email address for a user to receive Email Notifications, only users with administrator and maintenance roles will receive In-App Notifications. See the Notification Center topic for more details on In-App Notifications.

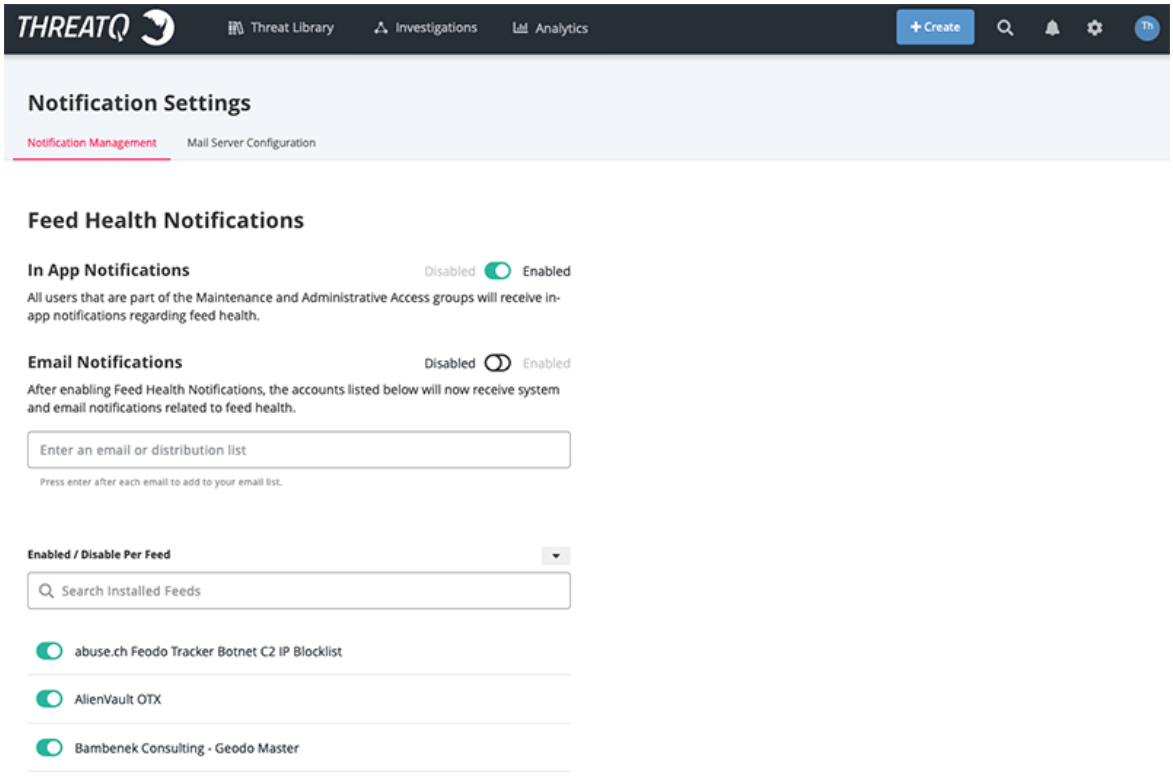
If using Email Notifications, the mail server configuration tab must completed before you enable the feature.

In the event that you have completed the mail server configuration and are still not receiving emails, your email provider may have marked the activity as suspicious. Some services, such as Gmail, will require you to confirm the activity, via an email message, before allowing the ThreatQ application to continue to use the server to send emails. A common symptom found in the error log is that you will receive an “incorrect password” error. If you are certain that the password you provided is correct, your mail service is likely blocking the service and requires your confirmation to proceed.

To Enable Feed Health Notifications:

1. Click on the **System Settings** gear icon and select the **Notification Settings** option.

The Notification Settings page loads.



2. Perform the following steps to enable email and in-app notifications:

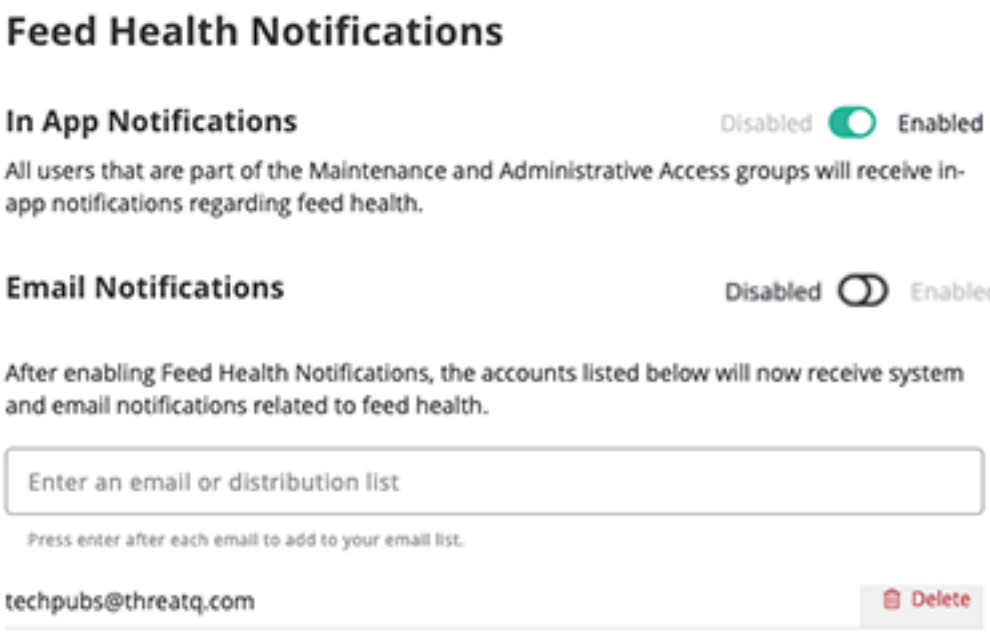
Enable In-App Health Feed Notifications

i. Click on the **Enable** toggle switch.

In-App Feed Health Notifications will now be enabled.

Enable Email Feed Health Notifications

i. Enter an email address in the account field and press the **<Enter>** or **<Return>** key.

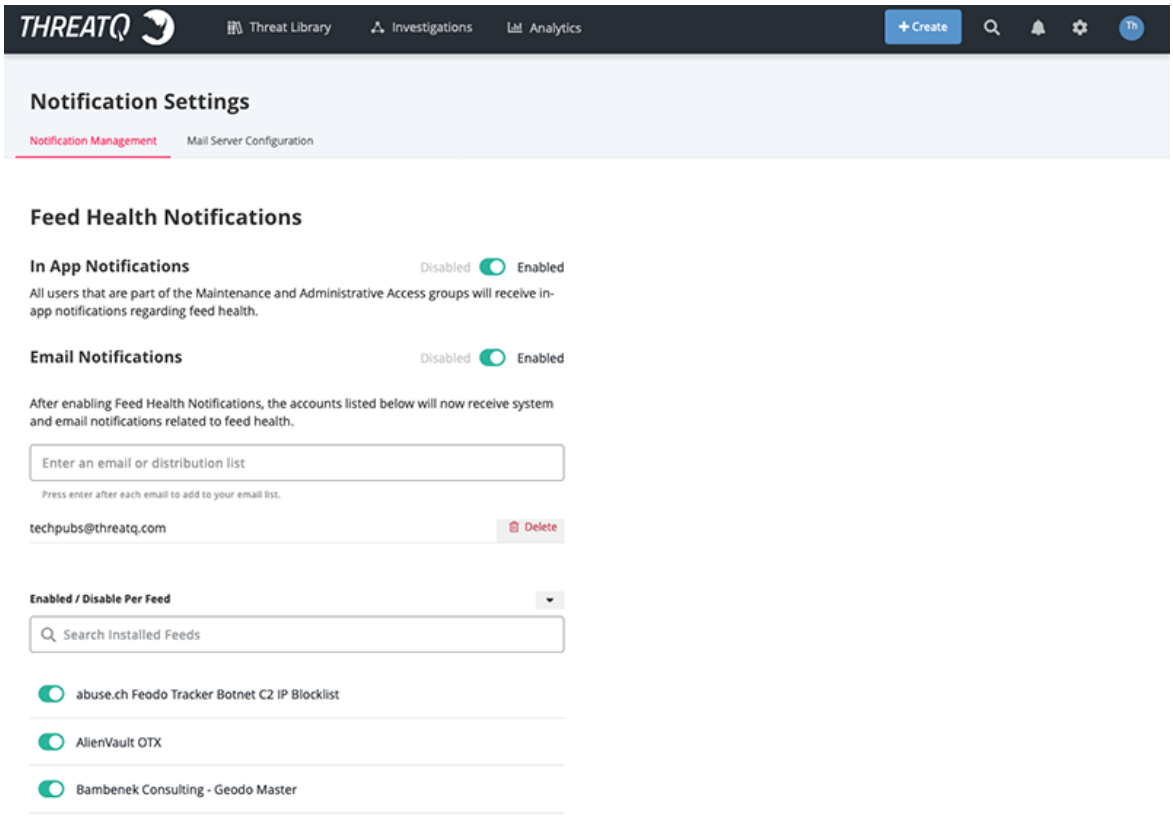


Repeat this step to add additional users.

ii. Click on the **Enable** toggle switch.

Email Feed Health Notifications will now be enabled.

3. Use the toggle switch next to each feed to enable/disable notifications for individual feeds.



You can also enable/disable individual CDF feed notifications by locating the feed under Incoming Feeds, selecting the Settings tab, and checking/unchecking the notifications checkbox.

Reports

The following describes how to generate reports in ThreatQ.

Reports Overview

You can export a PDF Summary of an object from an object's details page.

The generated PDF may contain active links to internal and external locations. Related objects in the PDF link to an internal ThreatQ instance that may require authentication. Please be aware of potential impacts before distribution of the generated report.

Google Chrome's pop-up blocker prevents object PDF summary reports from downloading. We recommend changing your browser settings to allow pop-ups from your ThreatQ instance.

Report Options

You can navigate to **Settings > Report Options** to customize the PDF reports that are generated. Report options apply to all reports generated platform-wide. You can make the following customizations:

- Customizing Report Text Colors
- Adding a Custom Disclaimer to a Report

Previewing Report Customization

You can preview report customization to view a representation of a report's output.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under Customized PDF Reports, click **Preview**.

   The sample report downloads to your computer.

Customizing the Report Header

Complete the following steps to add a custom header to your PDF.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under **Header Banner**, complete one of the following steps:
   - Drag and drop the image you want to use as the header.
   - Click **Browse** and navigate to the image you want to use as the header.
3. Optionally, click **Restore header banner to defaults**.
4. Click **Save**.

Customizing Report Text Colors

Complete the following steps to customize the colors in your PDF.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under **Colors**, use the drop down menus to select:
   - Header Text
   - Heading Text
   - Body Text
3. Click **Save**.

Adding a Custom Disclaimer to a Report

You can add a custom disclaimer to include with your report to communicate any liabilities or limitations to the end users of the report.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under **Disclaimer**,enter your disclaimer text and then use the formatting tools to customize your message.
3. Click **Save**.

Generating Reports

Complete the following steps to export a PDF Summary of an object from an object's details page.

Procedure:

1. Access the object's detail's page for which you want to generate a report summary.
2. Select **Actions > Generate PDF**.

   The PDF summary downloads and opens in a new browser tab.

Google Chrome Users: Google Chrome's pop-up blocker prevents object PDF summary reports from downloading. We recommend changing your browser settings to allow pop-ups from your ThreatQ instance. See Turning Off the Pop-up Blocker in Chrome for more information.

The generated PDF may contain active links to internal and external locations. Related objects in the PDF link to an internal ThreatQ instance that may require authentication. Please be aware of potential impacts before distribution of the generated report.

Turning Off the Pop-up Blocker in Chrome

This topic applies to ThreatQ version 4.7

By default, Google Chrome blocks pop-ups from automatically showing up on your screen. When a pop-up is blocked, the address bar will display a pop-up blocked alert. This pop-up blocker will prevent your PDF from being downloaded. Complete the following steps to allow pop-ups from ThreatQ.

Procedure:

1. Go to ThreatQ where pop-ups are blocked.
2. In the address bar, click the **Pop-up blocked** alert icon.
3. Click the link for the pop-up you want to see.
4. To always see pop-ups for the site, select Always allow pop-ups from [your ThreatQ instance].
5. Click **Done**.

Tasks

The following describes how to manage tasks in ThreatQ.

Tasks Overview

ThreatQ allows you to create and assign tasks to yourself or other users in the platform.

Once tasks are included in your deployment, you can add contextual information and correlate them with Indicators, Events, Adversaries, Signatures, and Files. You can also add comments, change the task priority, change the task status, and delete the task.

Assigning a Task

Complete the following steps to assign a task in ThreatQ.

1. From the main menu, choose **Create > Task**.

   The Add Task dialog box opens.

2. Enter a task **Name**.
3. Enter the assignee's email address in the **Assigned To** field.
4. Optionally, use the date picker to select a **Due Date**.
5. Select one of the following statuses:
   - To Do
   - In Progress

- Review
- Done

6. Select one of the following task priorities:
    - Low
    - Medium
    - High
7. Optionally, enter any **Associated Objects**.
8. Enter a **Description** for the task.
9. Click **Save**.

Managing Tasks

After a task is created, you can manage it on the task's Details page.

The following table describes the actions you can take to manage your tasks on a Task Details page.

To	You can...
Change task priority	Choose the **Priority** drop-down and select a new priority.

To	You can...
Change task status	Choose the **Status** drop-down and select a new status.
Add Attributes, Comments, Relationships, and Sources	Choose the **Add Context** drop-down and select an item.
View and Add Comments	Choose **Comments**.
View the Audit Log	Choose **Audit Log**.

Operations

The following explains how to configure and manage operations.

API keys for operations are available from the operation's provider.

Operations Overview

Operations enhance your threat intelligence data by allowing you to add attributes, as well as related indicators, from third party security services, both commercial and open source. You accomplish this by creating objects to connect to a desired service, receive threat intelligence, and display that threat intelligence in ThreatQ.

To develop custom operations, you should possess a basic functional knowledge of Python version 3 development. In ThreatQ version 3.0 and later, you can create operations for:

- Indicators
- Events
- Adversaries
- Files
- Signatures

ThreatQ operations are written in Python v3.5.2. We recommend allocating a non-production ThreatQ appliance for Operations development. You may use this development appliance to troubleshoot your operations before deploying them to production. You may also set up a local Python environment, write your script, and then copy it onto your ThreatQ appliance.

Managing Operations

Manage threat intelligence operations on the Operations Management page.

The following table describes the actions you can take to manage Operations.

To	Do this..
Turn an operation on or off	Toggle the switch next to the operation name.
Install an operation	See Installing Operations.
Uninstall an operation	See Deleting Operations.

Installing Operations

Typically, you will receive an operation installation package from a ThreatQuotient representative or download it from a designated repository.

API keys for operations are available from the operation's provider.

To install an operation:

1. From the navigation menu, choose the **Settings icon > Operations Management**.
2. Click **Install Operation**.
3. Choose one of the following:
   - Drag and drop your operation package onto the **Add Operation** dialog box.
   - Browse to your operation package, select it, and then click **Open**.

   If successful, the operation appears in your list of operations where you can enable or disable it.

Deleting Operations

To delete an operation:

1. From the navigation menu, choose the **Settings icon > Operations Management**.
2. For the operation you want to delete, expand **Operation Settings**.
3. Click **Delete Operation**.
4. Click **Uninstall**.

Exports

The following explains how to configure and manage exports of threat intelligence data from ThreatQ. Please read Exports Overview before proceeding.

Exports Overview

Exporting is one of the most important ThreatQ features, as it allows you to output non-whitelisted indicators to an external threat detection system.

ThreatQ provides a number of standard system exports that have previously been identified as useful. You have the option to use those and create your own. ThreatQ Exports are built on the Smarty PHP Template Engine; see https://www.smarty.net/.

You should NOT attempt to export all of your threat intelligence data with a single export. Attempting to do so will cause system degradation and the export will not complete.

Managing Exports

Manage Exports on the Exports page, accessible by navigating to the **Settings icon > Exports**.

The following describes the actions you can take to manage Exports.

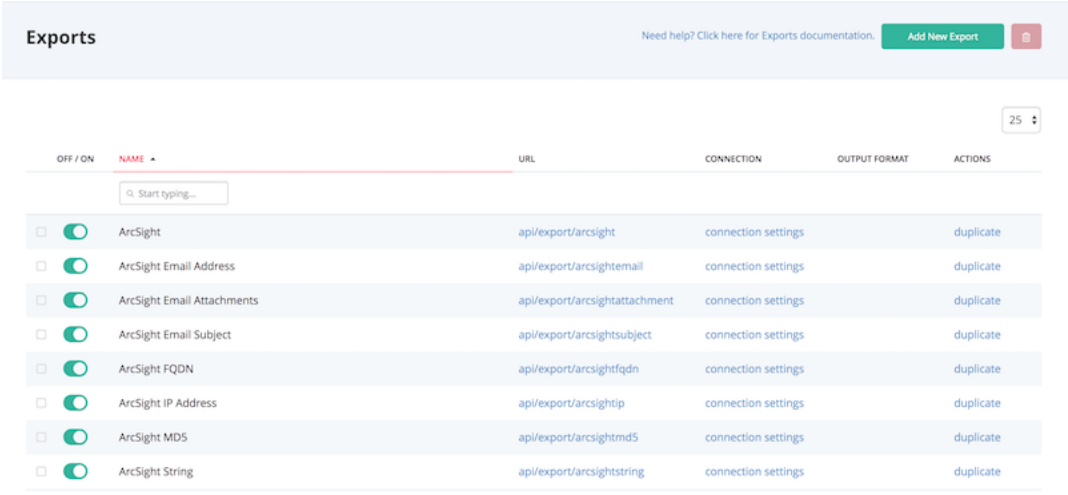
Viewing the Exports List

The Exports page provides a list of all standard and user-defined exports in the platform.

To view the exports list:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.



Enabling/Disabling an Export

To enable/disable an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Locate the export you wish to enable/disable.
3. Toggle the switch in the On/Off column to enable/disable the export.
   A confirmation of your action appears in an alert bar at the top of the page.

Viewing an Export

To view an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click the desired URL.

   A new tab opens in your browser, and you are taken to the data returned from that export.

   The load time may be lengthy depending on the amount of data being returned.

Duplicating an Export

Duplicating an export allows you to have a version that you can edit.

To duplicate an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Locate the Export you wish to duplicate.
3. Click **duplicate** in the Actions column.
4. The duplicate appears at the bottom of the Exports table. A confirmation of the

duplication appears in an alert bar at the top of the page.

By default, the copy you just created is toggled Off.

Adding an Export

To add an export

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **+ Add Export**.

   The Connection Settings dialog box opens.

3. Enter the Export name.
4. Verify or edit the token.
5. Click **Next Step**.

   The Output Format dialog box opens.

   For detailed information on formatting the Output Format dialog box, see Accessing/Editing an Export's Output Format.

6. Select which type of information you would like to export from the first dropdown menu.
7. Select the Output type from the second dropdown menu.
8. Un-select any of the checkboxes under the **Filter by TLP** section to exclude data by its source TLP classification. All classifications will be selected (included in the export) by default.

The **Filter by TLP** option will only appear if administrators have enabled TLP viewing. See the Traffic Light Protocol (TLP) topic for more information.

9. (Optional) Enter special parameters.
10. Customize the **Output Format Template** by putting your cursor where you want the variable to go and selecting the variable you'd like to use from the **Insert Variable** select box.
11. Verify the information entered.
12. Click **Save Settings**.

    The export you just created appears at the bottom of the Exports table, and a confirmation alert appears in an alert bar at the top of the page.

    By default, the new export is toggled Off.

Accessing/Editing an Export's Connection Settings

Connection settings are available for each of the exports. The Connection Settings dialog box contains the name of the export as well as the token you'll need to use when connecting a device to ThreatQ.

While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

To edit an export's connection settings:

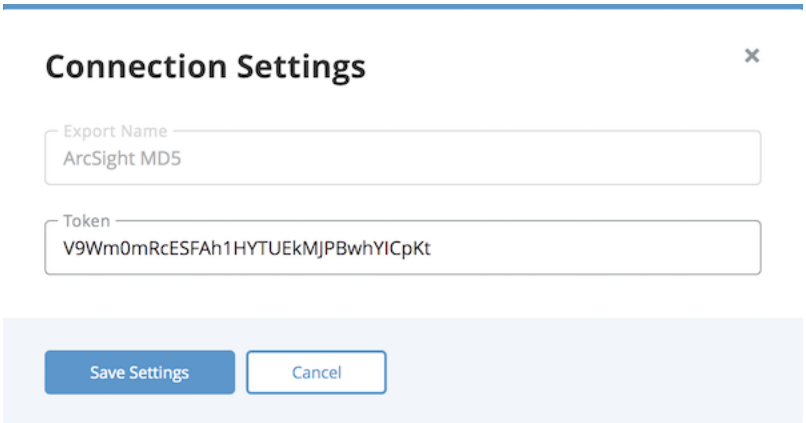
1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Locate the export you wish to edit.

3. Click **connection settings** in the Connection column.

   The Connection Settings dialog box opens.



4. Make the desired edits.
5. Click **Save Settings**.

   The settings are saved, and a confirmation alert appears in an alert bar at the top of the page.

Accessing/Editing an Export's Output Format

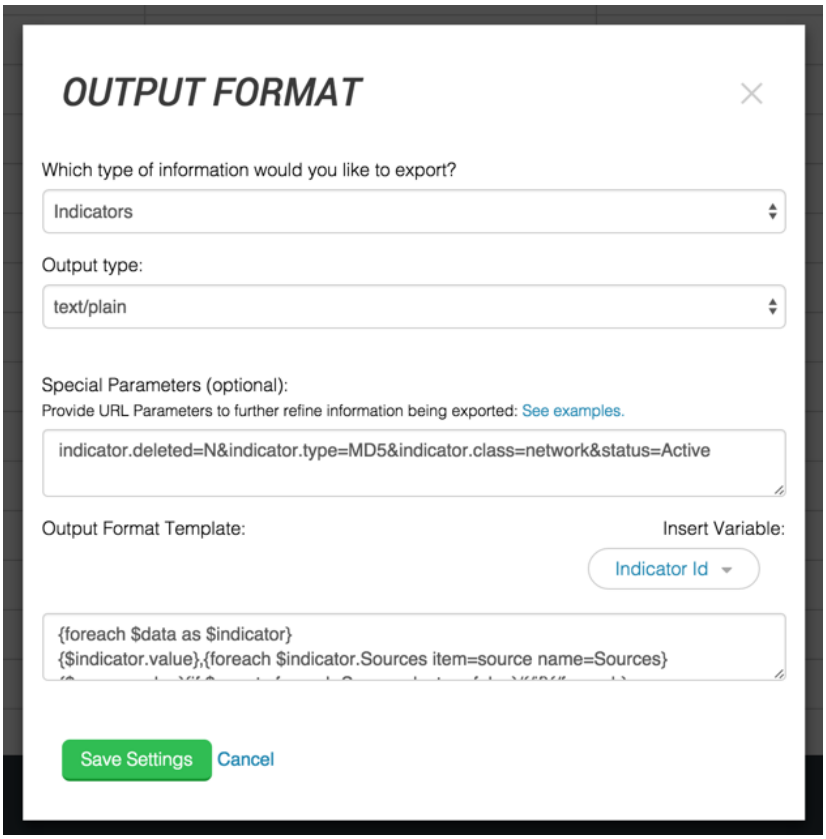
While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

To edit an export's output format:

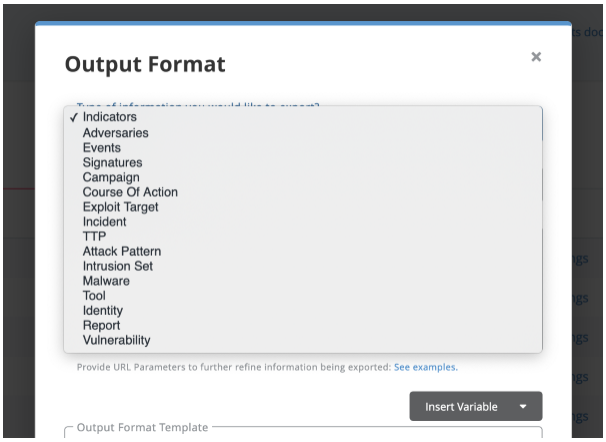
1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Locate the export you wish to edit.
3. Click **output format** in the Output Format column.
   The Output Format dialog box opens.



4. Select which type of information you would like to export from the first dropdown menu.



An admin has the ability to choose between the following options:

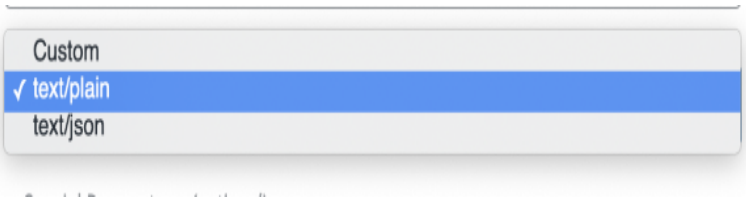
- Adversaries
- Indicators

- Attack Pattern
- Campaign
- Course of Action
- Events
- Exploit Target
- Identity
- Incident
- Intrusion Set
- Malware
- Report
- Signatures
- Tool
- TTP
- Vulnerability

5. Select the Output Type from the second dropdown menu.

   This sets the content type of the export response to a specific value (e.g. text/plain, text/json). Output Type does not have an impact on how the data is formatted but it does affect the content type within the header of the exported document. For example, if you select Output Type = text/json, when viewing the source of the export, the header will contain a Content Type = text/json attribute.

   Please see http://www.w3.org/Protocols/rfc1341/4_Content-Type.html for more information.



6. (Optional) Enter special parameters. There are two ways to do this:

   - Adding Special Parameters within ThreatQ. One advantage of using this option is that the URL for the export remains non-specific and therefore

you can change what is being exported without having to manage each external device individually.

- Customizing the Output Format Template. Choosing this option means you lose the ability to have one place to manage what is being exported.

Adding Special Parameters within ThreatQ

This is where an admin can provide additional parameters to further specify which data will be output via this export. Here are some examples.

To export all indicators with an active status	*Indicator.Status=Active*
To export all CIDR Block indicators that have an active status	Indicator.Status=Active&Indicator.Type=cidr block
To export all CIDR Block indicators and IP Addresses that have an active status	Indicator.Status=Active&Indicator.Type=cidr block&Indicator.Type=ip address
To export all indicators with a score greater than or equal to 7	Indicator.Score>=7

A wide range of filtering parameters are available:

Indicator

```
indicator.type_id
indicator.status_id
indicator.value
indicator.description
indicator.hash
indicator.last_detected_at
indicator.expires_at
indicator.expired_at
indicator.touched_at
```

```
indicator.deleted_at
indicator.deleted
indicator.sources_count
indicator.id
indicator.status
indicator.type
indicator.sincedeleted
indicator.whitelisted *
indicator.score
indicator.created_at
indicator.updated_at
indicator.Sources
indicator.Attributes
```

* Using the `indicator.whitelisted=Y` flag allows whitelisted indicators to be exported. It does not filter indicators by the whitelisted status. For that option, use the `indicator.status=whitelisted`flag. Additionally, to include only whitelisted indicators in your export, you will need to use both flags: `indicator.status=Whitelisted&indicator.whitelisted=Y`

Adversary

```
adversary.name
adversary.touched_at
adversary.deleted_at
adversary.deleted
adversary.sources_count
adversary.id
adversary.description
adversary.created_at
```

```
adversary.updated_at
adversary.Sources
adversary.Attributes
adversary.Indicators
adversary.Adversaries
adversary.Events
adversary.Attachments
adversary.Signatures
adversary.Investigations
adversary.Tasks
adversary.Campaign
adversary.Course_of_action
adversary.Exploit_target
adversary.Incident
adversary.Ttp
adversary.Attack_pattern
adversary.Identity
adversary.Intrusion_set
adversary.Malware
adversary.Report
adversary.Tool
adversary.Vulnerability
```

Event

```
event.type_id
event.title
event.happened_at
event.hash
event.description
```

```
event.deleted_at
event.deleted
event.sources_count
event.id
event.type
event.touched_at
event.created_at
event.updated_at
event.Sources
event.Attributes
event.Indicators
event.Adversaries
event.Events
event.Attachments
event.Signatures
event.Investigations
event.Tasks
event.Campaign
event.Course_of_action
event.Exploit_target
event.Incident
event.Ttp
event.Attack_pattern
event.Identity
event.Intrusion_set
event.Malware
event.Report
event.Tool
event.Vulnerability
```

Signature

```
signature.description
signature.hash
signature.last_detected_at
signature.name
signature.status_id
signature.touched_at
signature.type_id
signature.value
signature.deleted_at
signature.deleted
signature.sources_count
signature.id
signature.status
signature.type
signature.created_at
signature.updated_at
signature.Sources
signature.Attributes
signature.Indicators
signature.Adversaries
signature.Events
signature.Attachments
signature.Signatures
signature.Investigations
signature.Tasks
signature.Campaign
signature.Course_of_action
signature.Exploit_target
```

```
signature.Incident
signature.Ttp
signature.Attack_pattern
signature.Identity
signature.Intrusion_set
signature.Malware
signature.Report
signature.Tool
signature.Vulnerability
```

Campaign

```
campaign.value
 campaign.status_id
 campaign.type_id
 campaign.description
 campaign.objective
 campaign.started_at
 campaign.ended_at
 campaign.deleted_at
 campaign.deleted
 campaign.sources_count
 campaign.id
 campaign.status
 campaign.type
 campaign.touched_at
 campaign.created_at
 campaign.updated_at
 campaign.Sources
 campaign.Attributes
```

```
campaign.Indicators
campaign.Adversaries
campaign.Events
campaign.Attachments
campaign.Signatures
campaign.Investigations
campaign.Tasks
campaign.Campaign
campaign.Course_of_action
campaign.Exploit_target
campaign.Incident
campaign.Ttp
campaign.Attack_pattern
campaign.Identity
campaign.Intrusion_set
campaign.Malware
campaign.Report
campaign.Tool
campaign.Vulnerability
```

Course of Action

```
course_of_action.value
course_of_action.status_id
course_of_action.type_id
course_of_action.description
course_of_action.deleted_at
course_of_action.deleted
course_of_action.sources_count
course_of_action.id
```

```
course_of_action.status
course_of_action.type
course_of_action.touched_at
course_of_action.created_at
course_of_action.updated_at
course_of_action.Sources
course_of_action.Attributes
course_of_action.Indicators
course_of_action.Adversaries
course_of_action.Events
course_of_action.Attachments
course_of_action.Signatures
course_of_action.Investigations
course_of_action.Tasks
course_of_action.Campaign
course_of_action.Course_of_action
course_of_action.Exploit_target
course_of_action.Incident
course_of_action.Ttp
course_of_action.Attack_pattern
course_of_action.Identity
course_of_action.Intrusion_set
course_of_action.Malware
course_of_action.Report
course_of_action.Tool
course_of_action.Vulnerability
```

Exploit

```
exploit_target.value
```

```
exploit_target.status_id
exploit_target.type_id
exploit_target.description
exploit_target.deleted_at
exploit_target.deleted
exploit_target.sources_count
exploit_target.id
exploit_target.status
exploit_target.type
exploit_target.touched_at
exploit_target.created_at
exploit_target.updated_at
exploit_target.Sources
exploit_target.Attributes
exploit_target.Indicators
exploit_target.Adversaries
exploit_target.Events
exploit_target.Attachments
exploit_target.Signatures
exploit_target.Investigations
exploit_target.Tasks
exploit_target.Campaign
exploit_target.Course_of_action
exploit_target.Exploit_target
exploit_target.Incident
exploit_target.Ttp
exploit_target.Attack_pattern
exploit_target.Identity
exploit_target.Intrusion_set
```

```
exploit_target.Malware
exploit_target.Report
exploit_target.Tool
exploit_target.Vulnerability
```

Incident

```
incident.value
incident.status_id
incident.type_id
incident.description
incident.started_at
incident.ended_at
incident.deleted_at
incident.deleted
incident.sources_count
incident.id
incident.status
incident.type
incident.touched_at
incident.created_at
incident.updated_at
incident.Sources
incident.Attributes
incident.Indicators
incident.Adversaries
incident.Events
incident.Attachments
incident.Signatures
incident.Investigations
```

```
incident.Tasks
incident.Campaign
incident.Course_of_action
incident.Exploit_target
incident.Incident
incident.Ttp
incident.Attack_pattern
incident.Identity
incident.Intrusion_set
incident.Malware
incident.Report
incident.Tool
incident.Vulnerability
```

TTP

```
ttp.value
ttp.status_id
ttp.type_id
ttp.description
ttp.deleted_at
ttp.deleted
ttp.sources_count
ttp.id
ttp.status
ttp.type
ttp.touched_at
ttp.created_at
ttp.updated_at
ttp.Sources
```

```
ttp.Attributes
ttp.Indicators
ttp.Adversaries
ttp.Events
ttp.Attachments
ttp.Signatures
ttp.Investigations
ttp.Tasks
ttp.Campaign
ttp.Course_of_action
ttp.Exploit_target
ttp.Incident
ttp.Ttp
ttp.Attack_pattern
ttp.Identity
ttp.Intrusion_set
ttp.Malware
ttp.Report
ttp.Tool
ttp.Vulnerability
```

Attack Pattern

```
attack_pattern.value
attack_pattern.status_id
attack_pattern.type_id
attack_pattern.description
attack_pattern.deleted_at
attack_pattern.deleted
attack_pattern.sources_count
```

```
attack_pattern.id
attack_pattern.status
attack_pattern.type
attack_pattern.touched_at
attack_pattern.created_at
attack_pattern.updated_at
attack_pattern.Sources
attack_pattern.Attributes
attack_pattern.Indicators
attack_pattern.Adversaries
attack_pattern.Events
attack_pattern.Attachments
attack_pattern.Signatures
attack_pattern.Investigations
attack_pattern.Tasks
attack_pattern.Campaign
attack_pattern.Course_of_action
attack_pattern.Exploit_target
attack_pattern.Incident
attack_pattern.Ttp
attack_pattern.Attack_pattern
attack_pattern.Identity
attack_pattern.Intrusion_set
attack_pattern.Malware
attack_pattern.Report
attack_pattern.Tool
attack_pattern.Vulnerability
```

Identity

```
identity.value
 identity.status_id
 identity.type_id
 identity.description
 identity.contact_information
 identity.deleted_at
 identity.deleted
 identity.sources_count
 identity.id
 identity.status
 identity.type
 identity.touched_at
 identity.created_at
 identity.updated_at
 identity.Sources
 identity.Attributes
 identity.Indicators
 identity.Adversaries
 identity.Events
 identity.Attachments
 identity.Signatures
 identity.Investigations
 identity.Tasks
 identity.Campaign
 identity.Course_of_action
 identity.Exploit_target
 identity.Incident
 identity.Ttp
 identity.Attack_pattern
```

```
identity.Identity
identity.Intrusion_set
identity.Malware
identity.Report
identity.Tool
identity.Vulnerability
```

Intrusion Set

```
intrusion_set.value
intrusion_set.status_id
intrusion_set.type_id
intrusion_set.description
intrusion_set.started_at
intrusion_set.ended_at
intrusion_set.deleted_at
intrusion_set.deleted
intrusion_set.sources_count
intrusion_set.id
intrusion_set.status
intrusion_set.type
intrusion_set.touched_at
intrusion_set.created_at
intrusion_set.updated_at
intrusion_set.Sources
intrusion_set.Attributes
intrusion_set.Indicators
intrusion_set.Adversaries
intrusion_set.Events
intrusion_set.Attachments
```

```
intrusion_set.Signatures
intrusion_set.Investigations
intrusion_set.Tasks
intrusion_set.Campaign
intrusion_set.Course_of_action
intrusion_set.Exploit_target
intrusion_set.Incident
intrusion_set.Ttp
intrusion_set.Attack_pattern
intrusion_set.Identity
intrusion_set.Intrusion_set
intrusion_set.Malware
intrusion_set.Report
intrusion_set.Tool
intrusion_set.Vulnerability
```

Malware

```
malware.value
 malware.status_id
 malware.type_id
 malware.description
 malware.deleted_at
 malware.deleted
 malware.sources_count
 malware.id
 malware.status
 malware.type
 malware.touched_at
 malware.created_at
```

```
malware.updated_at
malware.Sources
malware.Attributes
malware.Indicators
malware.Adversaries
malware.Events
malware.Attachments
malware.Signatures
malware.Investigations
malware.Tasks
malware.Campaign
malware.Course_of_action
malware.Exploit_target
malware.Incident
malware.Ttp
malware.Attack_pattern
malware.Identity
malware.Intrusion_set
malware.Malware
malware.Report
malware.Tool
malware.Vulnerability
```

Report

```
report.value
report.status_id
report.type_id
report.description
report.deleted_at
```

```
report.deleted
report.sources_count
report.id
report.status
report.type
report.touched_at
report.created_at
report.updated_at
report.Sources
report.Attributes
report.Indicators
report.Adversaries
report.Events
report.Attachments
report.Signatures
report.Investigations
report.Tasks
report.Campaign
report.Course_of_action
report.Exploit_target
report.Incident
report.Ttp
report.Attack_pattern
report.Identity
report.Intrusion_set
report.Malware
report.Report
report.Tool
report.Vulnerability
```

Tool

```
tool.value
tool.status_id
tool.type_id
tool.description
tool.deleted_at
tool.deleted
tool.sources_count
tool.id
tool.status
tool.type
tool.touched_at
tool.created_at
tool.updated_at
tool.Sources
tool.Attributes
tool.Indicators
tool.Adversaries
tool.Events
tool.Attachments
tool.Signatures
tool.Investigations
tool.Tasks
tool.Campaign
tool.Course_of_action
tool.Exploit_target
tool.Incident
tool.Ttp
tool.Attack_pattern
```

```
tool.Identity
tool.Intrusion_set
tool.Malware
tool.Report
tool.Tool
tool.Vulnerability
```

Vulnerability

```
vulnerability.value
vulnerability.status_id
vulnerability.type_id
vulnerability.description
vulnerability.deleted_at
vulnerability.deleted
vulnerability.sources_count
vulnerability.id
vulnerability.status
vulnerability.type
vulnerability.touched_at
vulnerability.created_at
vulnerability.updated_at
vulnerability.Sources
vulnerability.Attributes
vulnerability.Indicators
vulnerability.Adversaries
vulnerability.Events
vulnerability.Attachments
vulnerability.Signatures
vulnerability.Investigations
```

```
vulnerability.Tasks
vulnerability.Campaign
vulnerability.Course_of_action
vulnerability.Exploit_target
vulnerability.Incident
vulnerability.Ttp
vulnerability.Attack_pattern
vulnerability.Identity
vulnerability.Intrusion_set
vulnerability.Malware
vulnerability.Report
vulnerability.Tool
vulnerability.Vulnerability
```

Adding Differential Flags

You can use a differential flag in the Special Parameters section of your export output format to limit the output to new data. This will allow you to include only new data each time the export is run opposed to exporting all data.

Include the following to limit exports to new data only:

```
differential=1
```

If you have multiple systems pulling from the same Export, each system should use a unique differential value.

Example:
external system 1
https://{tq-host}/api/export/c2ab6df72e67ee13cef90f0e00981b62/?token=npc6z01pFXwfHYb5tm51hMvKQJNYecTG&**differential=1**

external system 2

https://{tq-host}/api/export/c2ab6df72e67ee13cef90f0e00981b62/?token=npc6z01pFXwfHYb5tm51hMvKQJNYecTG&**differential=2**

Adding Parameters to the end of the URL

You can append the same parameters listed above to the end of any export URL to achieve the same results. By pursuing this option, you will lose the option of having one place to manage what is being exported via that export.

Using Logical Operators in Export Filters

You can configure exports to output objects matching filter conditions that use logical AND and OR operators. Exports allow the following filters:

1. Searching using greater than, less than, or equal to
    - Examples in special parameters string section:

```
indicator.score>=5
```

```
indicator.score<=5
```

    - Examples in request URI:

```
&indicator.score=>=5
```

```
&indicator.score=<=8
```

2. Adding multiple criteria for a single field using an OR comparison

- Example in special parameters string section:

```
indicator.score=5&indicator.score=8
```

- Example in request URI:

```
&indicator.score[]=5&indicator.score[]=8
```

3. Adding multiple criteria for a single field using an AND comparison

- Example in special parameters string section:

```
indicator.score>=5&indicator.score<=8
```

- Example in request URI:

```
&indicator.score[]=>=5&indicator.score
[]=<=8
```

Customizing the Output Format Template

You can customize the output format template for an custom or duplicated export.

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Locate the export for which you want to customize the output format template.
3. Click **output format**.
4. In the Output Format dialog box, customize the output format template by putting your cursor where you want the variable to go and selecting the variable you'd like to use from the **Insert Variable** select box.

This template provides you with the ability to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop. Please refer to the following as an example:

```
{foreach $data as $indicator}

Your variables go here

{/foreach}
```

The Output Format Template is populated based on your selection.

5. Verify the information entered.
6. Click **Save Settings**.

Export Output Format Templates

The following topics contain template files that you can use to customize an export's output format.

The Output Format Template field for an export is found under its Output Format modal. You can access this by clicking on the **Output Format** link for an export from the main exports page.

- Export Adversaries Output Format Template
- Export Events Output Format Template
- Export Indicators Output Format Template
- Export Signatures Output Format Template

Export Adversaries Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
{foreach $data as $adversary}
ID: {$adversary.id}
Name: {$adversary.name}
Description: {$adversary.description}
Created At: {$adversary.created}
Updated At: {$adversary.updated_at}
Touched At: {$adversary.touched_at}
Deleted At: {$adversary.deleted_at}
Deleted: {$adversary.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $adversary.Sources item=source name-
e=Sources}{$source.value} {if !empty($source.tlp)}
({$source.tlp}){/if}
{/foreach}
```

Attributes

```
{foreach $adversary.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
{foreach $adversary.Adversaries item=adversary name-
e=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachments

```
{foreach $adversary.Attachments item=attachment
name=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Events

```
{foreach $adversary.Events item=event name=Events}
Name: {$event.name}
```

```
Value: {$event.value}
{/foreach}
```

Indicators

```
    {foreach $adversary.Indicators item=indicator name-
    e=Indicators}
    Name: {$indicator.name}
    Value: {$indicator.value}
    {/foreach}
```

Investigations

```
    {foreach $adversary.Investigations item-
    m=investigation name=Investigations}
    Name: {$investigation.name}
    Value: {$investigation.value}
    {/foreach}
```

Signatures

```
    {foreach $adversary.Signatures item=signature name-
    e=Signatures}
    Name: {$signature.name}
    Value: {$signature.value}
    {/foreach}
```

Tasks

```
{foreach $adversary.Tasks item=task name=Tasks}
Name: {$task.name}
Value: {$task.value}
{/foreach}
```

Export Events Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
{foreach $data as $event}

{$event.title} ID: {$event.id}
Title: {$event.title}
Type: {$event.type}
Happened: {$event.happened_at}
Description: {$event.description}
Created At: {$event.created}
Updated At: {$event.updated_at}
Touched At: {$event.touched_at}
Deleted At: {$event.deleted_at}
Deleted: {$event.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $event.Sources item=source name=Sources}
{$source.value} {if !empty($source.tlp)}{/if}
{/foreach}
```

Attributes

```
{foreach $event.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
{foreach $event.Adversaries item=adversary name-
e=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachments

```
{foreach $event.Attachments item=attachment name-
e=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Events

```
{foreach $event.Events item=event name=Events}
Name: {$event.name}
Value: {$event.value}
{/foreach}
```

Indicators

```
{foreach $event.Indicators item=indicator name-
e=Indicators}
Name: {$indicator.name}
Value: {$indicator.value}
{/foreach}
```

Investigations

```
{foreach $event.Investigations item=investigation
name=Investigations}
Name: {$investigation.name}
Value: {$investigation.value}
{/foreach}
```

Signatures

```
{foreach $event.Signatures item=signature name-
e=Signatures}
Name: {$signature.name}
```

```
Value: {$signature.value}
{/foreach}
```

Tasks

```
    {foreach $event.Tasks item=task name=Tasks}
    Name: {$task.name}
    Value: {$task.value}
    {/foreach}
```

Export Indicators Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
    {foreach $data as $indicator}

    {$indicator.value}
    ID: {$indicator.id}
    Value: {$indicator.value}
    Type: {$indicator.type}
    Status: {$indicator.status}
    Class: {$indicator.class}
    Description: {$indicator.description}
    Score: {$indicator.score}
    Hash: {$indicator.hash}
    Source Count: {$indicator.sources_count}
```

```
Whitelisted: {$indicator.whitelisted}
Last Detected At: {$indicator.last_detected_at}
Created At: {$indicator.created_at}
Updated At: {$indicator.updated_at}
Touched At: {$indicator.touched_at}
Since Deleted: {$indicator.sincedeleted}
Deleted At: {$indicator.deleted_at}
Deleted: {$indicator.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $indicator.Sources item=source name-
e=Sources}{$source.value} {if !empty($source.tlp)}
({$source.tlp})
{/foreach}
```

Attributes

```
{foreach $indicator.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
{foreach $indicator.Adversaries item=adversary name-
e=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachments

```
{foreach $indicator.Attachments item=attachment
name=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Events

```
{foreach $indicator.Events item=event name=Events}
Name: {$event.name}
Value: {$event.value}
{/foreach}
```

Indicators

```
{foreach $event.Indicators item=indicator name-
e=Indicators}
Name: {$indicator.name}
```

```
Value: {$indicator.value}
{/foreach}
```

Investigations

```
    {foreach $indicator.Investigations item-
    m=investigation name=Investigations}
    Name: {$investigation.name}
    Value: {$investigation.value}
    {/foreach}
```

Signatures

```
    {foreach $indicator.Signatures item=signature name-
    e=Signatures}
    Name: {$signature.name}
    Value: {$signature.value}
    {/foreach}
```

Tasks

```
    foreach $indicator.Tasks item=task name=Tasks}
    Name: {$task.name}
    Value: {$task.value}
    {/foreach}
```

Export Signatures Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
{foreach $data as $signature}

{$signature.name}
ID: {$signature.id}
Name: {$signature.name}
Value: {$signature.value}
Type: {$signature.type}
Status: {$signature.status}
Description: {$signature.description}
Hash: {$signature.hash}
Detected At: {$signature.last_detected_at}
Touched At: {$signature.touched_at}
Created At: {$signature.created}
Updated At: {$signature.updated_at}
Deleted At: {$signature.deleted_at}
Deleted: {$signature.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $signature.Sources item=source name-
e=Sources}{$source.value} {if !empty($source.tlp)}
({$source.tlp}){/if}
{/foreach}
```

Attributes

```
{foreach $signature.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
{foreach $signature.Adversaries item=adversary name-
e=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachments

```
{foreach $signature.Attachments item=attachment
name=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Events

```
{foreach $signature.Events item=event name=Events}
Name: {$signature.name}
Value: {$signature.value}
{/foreach}
```

Indicators

```
{foreach $signature.Indicators item=indicator name-
e=Indicators}
Name: {$indicator.name}
Value: {$indicator.value}
{/foreach}
```

Investigations

```
{foreach $signature.Investigations item-
m=investigation name=Investigations}
Name: {$investigation.name}
Value: {$investigation.value}
{/foreach}
```

Signatures

```
{foreach $signature.Signatures item=signature name-
e=Signatures}
Name: {$signature.name}
Value: {$signature.value}
{/foreach}
```

Tasks

```
{foreach $signature.Tasks item=task name=Tasks}
Name: {$task.name}
Value: {$task.value}
{/foreach}
```

Deleting an Export

While you cannot delete any of the exports included with your ThreatQ installation, you can delete any exports you have added or copies of the default exports.

To delete an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Locate the export(s) you wish to delete.
3. Select one or more exports.
4. Click the delete icon at the top right of the Exports table.

Specific Indicator Export Configuration Instructions

The following topics provide instructions on how to export specific indicators for use with an external threat detection system.

- Configuring Bro Exports
- Configuring Fidelis Exports
- Configuring Fortinet Fortigate Exports
- Configuring Lancope Exports
- Configuring Netwitness Exports

- Configuring OpenIOC Signature Exports
- Configuring Palo Alto Exports
- Configuring Palo Alto: PANOS and Panorama
- Configuring Reservoir Labs Exports
- Configuring Splunk Exports
- Configuring Symantec ProxySG
- Configuring Tenable Exports

Configuring Bro Exports

This topic explains how to export Bro indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to Bro:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**.

- Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N**
- Under **Output Format Template**, enter:

```
#fields{$tab}indicator{$tab}indicator_type{$tab}meta.source{$tab}meta.url

{foreach $data as $indicator}

{$indicator_type=""}

{$source_found=0}

{if $indicator.type eq "CIDR Block"}{$indicator_type="Intel::SUBNET"}{/if}

{if $indicator.type eq "IP Address"}{$indicator_type="Intel::ADDR"}{/if}

{if $indicator.type eq "URL"}{$indicator_type="Intel::URL"}{/if}

{if $indicator.type eq "Email Address"}{$indicator_type="Intel::EMAIL"}{/if}

{if $indicator.type eq "FQDN"}{$indicator_type="Intel::DOMAIN"}{/if}

{if $indicator.type eq "MD5"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-1"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-256"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-256"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-384"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-512"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "Filename"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator_type ne ""}
```

{$indicator.value}{$tab}{$indicator_type}{$tab}{foreach $indicator.Sources item=source name=Sources}{if $smarty.foreach.Sources.first == true}

{$source.value}{$source_found=1}{/if}{/foreach}{if $source_found == 0}-{/if}

{$tab}https://{$http_host}/indicators/{$indicator.id}/details

{/if}

{/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Cisco TID Exports

The exports and configurations below enable IOCs to be exported to Cisco TID via the Cisco FMC to be published to Cisco FTD Devices.

See Exports Overview for more details about configuring exports.

The constraints of the Cisco Threat Intelligence Director will only allow the following ThreatQ exports to be used:

- SHA-256
- Domain (FQDN)
- URL
- IPv4
- IPv6
- Email
  - To
  - From

- Sender
- Subject

To export to Cisco TID:

1. Log into your ThreatQ instance.
2. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

3. Click **Add New Export**.

   The Connection Settings dialog box appears.

4. Enter an **Export Name** from the tables listed below.
5. Click **Next Step**.

   The Output Format dialog box appears.

6. If using TLP, deselect any TLP grade(s) that you do not wish to export.
7. Use the tables below to provide the special parameters and output format template:

See the Using Logical Operators in Export Filters topic for more infrmation on using logical operators in exports.
If a specific score or ranges of scores is required, then the following should be added to the end of the special parameters configuration.

In the example below, this will ensure only IP Address IoCs that are equal to 7 or above are exported.

```
indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network&amp;indicator.score>=7
```

SHA-256

Field	Entry
Export Name	Cisco TID - SHA-256
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=SHA-256
Output Format Template	{foreach $data as $indicator} {$indicator.value} {/foreach}

FQDN

Field	Entry
Export Name	Cisco TID - FQDN
Which type of information	Indicator

Field	Entry
would you like to export?	
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=network&indicator.score>=11
Output Format Template	{foreach $data as $indicator} {$indicator.value} {/foreach}

URL

Field	Entry
Export Name	Cisco TID - URL
Which type of information would you	Indicator

Field	Entry
like to export?	
Output Type	Text/plain
Special Para-meters	indicator.status=Active&indicator.type=URL&indicator.class=network
Output Format Template	{foreach $data as $indicator} {$indicator.value} {/foreach}

IPv4 Address

Field	Entry
Export Name	Cisco TID - IPv4
Which type of inform-ation would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network
Output Format Tem-plate	{foreach $data as $indicator} {$indicator.value} {/foreach}

IPv6 Address

Field	Entry
Export Name	Cisco TID - IPv6
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	Indicator.Status=Active&Indicator.Type=IPv6 Address
Output Format Template	{foreach $data as $indicator} {$indicator.value} {/foreach}

Email Address

Field	Entry
Export Name	Cisco TID - Email Address
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters Email Address • To • From	indicator.status=Active&indicator.type=Email Address&indicator.class=network

Field	Entry
• Sender	
Output Format Template	{foreach $data as $indicator} {$indicator.value} {/foreach}

In turn click each of the URL's for the exports, a new browser widow will open displaying the first 10 results, make a note of this URL and the IoCs it is associated with it. The URL is made up off the following sections

```
https://<TQ Server>/api/export/<endpoint>/?limit=10&token=<token>
```

8. Remove the limit section and trailing & symbol, examples are below.

```
https://192.168.1.85/api/export/9bc092ce1e318f6c0d10009228729ad6/?token=uEyVyzIeYRGBdF2VKcHo9WKYDJvNftSo
```

This new URL format is needed to configure Cisco TID

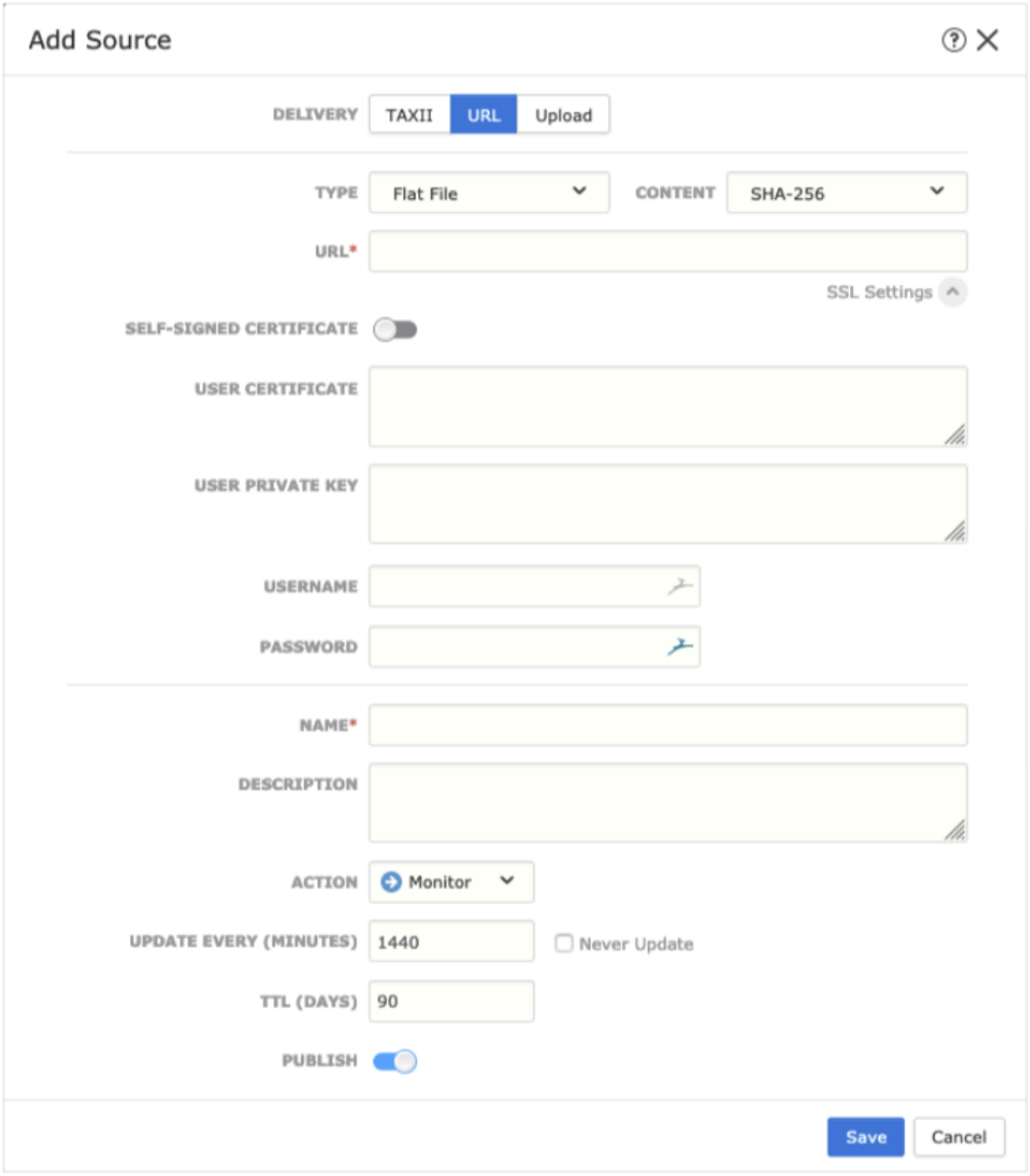
```
https://192.168.1.85/api/export/9bc092ce1e318f6c0d10009228729ad6/?token=uEyVyzIeYRGBdF2VKcHo9WKYDJvNftSo
```

9. Click **Save Settings**.
10. Under **On/Off**, toggle the switch to enable the export.

Cisco FMC Configuration:

1. Navigate to the Intelligence director on the Firepower Management Centre.
2. Choose **Intelligence > Sources**.
3. Click the **add icon (+)**.
4. Choose **URL** as the Delivery method for the source.

5. Complete the Add Source form.



Field	Entry
Type	Flat File

Field	Entry
Content	Select a Content type that describes the data contained within the source.
URL	Use the URL format outlined in step 8 of the *To export to Cisco TID* steps.
Self-Signed Certificate	Toggle the Self-Signed Certificate to active.
Name	Use a descriptive name as we used on the ThreatQ exports. **Example:** ThreatQ - IP Address This will help simplify sorting and handling of incidents based on TID indicators, use a consistent naming scheme across sources.
Action	You can either Block or Monitor.
Update Every	Select a time in minutes that the source is to be updated (the minimum is 30 mins, Maximum is 14,400).
TTL	Specify the number of days for the TTL interval. • TID deletes all the source's indicators that are not included in subsequent upload. • all observables not referenced by a surviving indicator.

6. Confirm that the **Publish** toggle is set to **Active** if you want to immediately being publishing to elements.

If you do not publish the source at ingestion, you cannot publish all source indicators at once later. Instead, you must publish each observable individually.

7. Click **Save**.

Configuring Fidelis Exports

This topic explains how to export Fidelis indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data for:

- Fidelis FQDN
- Fidelis FQDN Text
- Fidelis IP Address
- Fidelis IP Address Text
- Fildeis MD5
- Fidelis MD5 Text
- Fidelis URL
- Fidelis URL Text

To export to Fidelis FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:

   - For **Which type of information would you like to export?** Choose: **Indicators**
   - For **Output type**, choose **text/xml**.
   - Under **Special Parameters**, enter **indicator.status-s=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=host**
   - Under **Output Format Template**, enter:

     <MyMD5feed/>

     <description>FQDN feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

     <entries>

     <limit>{$row_count}</limit>

     <page>{$row_count}</page>

     <start>{$row_count}</start>

     <end>{$row_count}</end>

     <status>{$row_count}</status>

     <rows_returned>{$row_count}</rows_returned>

     <entry>

     {foreach $data as $indicator}

```
<hostname>{$indicator.value|escape:"url"}</hostname>

<extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

{/foreach}

</entry>

</entries>
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis FQDN Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=host**

- Under **Output Format Template**, enter:

  {foreach $data as $indicator}

  {$indicator.value}

  {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis IP Address:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/xml**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network**.
   - Under **Output Format Template**, enter:

     <MyMD5feed/>

<description>IP feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

<entries>

<limit>{$row_count}</limit>

<page>{$row_count}</page>

<start>{$row_count}</start>

<end>{$row_count}</end>

<status>{$row_count}</status>

<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<ip>{$indicator.value|escape:"url"}</ip>

<extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

{/foreach}

</entry>

</entries>

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis IP Address Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network**.
   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value}

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis MD5:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/xml**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=host.**
   - Under **Output Format Template**, enter:

     <MyMD5feed/>

     <description>MD5 feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

     <entries>

     <limit>{$row_count}</limit>

     <page>{$row_count}</page>

     <start>{$row_count}</start>

     <end>{$row_count}</end>

     <status>{$row_count}</status>

```
<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<md5>{$indicator.value|escape:"url"}}</md5>

<extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

{/foreach}

</entry>

</entries>
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis MD5 Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose: **text/plain**.

- Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=host**
- Under **Output Format Template**, enter:

  {foreach $data as $indicator}

  {$indicator.value}

  {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis URL:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter: **indicator.status=Active&indicator.deleted=N**

- Under **Output Format Template**, enter:

```
<MyMD5feed/>

<description>URL feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

<entries>

<limit>{$row_count}</limit>

<page>{$row_count}</page>

<start>{$row_count}</start>

<end>{$row_count}</end>

<status>{$row_count}</status>

<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<url>{$indicator.value|escape:"url"}}</url>

<extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

{/foreach}

</entry>

</entries>
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis URL Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**: choose **text/plain**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=URL&indicator.class=host**
   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value}

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Fortinet Fortigate Exports

This topic describes the implementation between ThreatQ and the Fortinet FortiGate firewall. The implementation is done using the Threat Feed Connectors feature available in FortiOS v6.0 and above. An export with IOCs is first created on ThreatQ and the export URL is installed FortiGate appliance.

This integration only works on FortiOS v6.0 and above.

Before starting the integration, users are encouraged to familiarize themselves with the following documents:

- Fortinet Fortigate cookbook on blocking malicious domains using threat feeds - https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/85580
- Using Threat Feed Connectors in FortiOS v6.0 and above - https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-security-profiles/Web_Filter/Overriding%20FortiGuard%20website%20categorization.htm#External
- The Exports section of the ThreatQ Help Center.

Confirm that there is a route between both hosts before you begin the integration between FortiGate and ThreatQ.

Create an Export in ThreatQ

The export is a dynamic list of IOCs which should be configured on ThreatQ and provided to a FortiGate instance to read from. To create an export in ThreatQ follow the steps in theAdding an Export topic.

Use the following information to configure the export:

Field	Selection
Type of	Indicators

<table>
<tr><th>Field</th><th>Selection</th></tr>
<tr><td>Inform-ation you would like to export.</td><td></td></tr>
<tr><td>Output Type</td><td>text/plain</td></tr>
<tr><td rowspan="3">Special Para-meters</td><td>There are two options for special parameters.</td></tr>
<tr><td>If security policy of your organization requires that all IP Addresses and FQDNs are sent to FortiGate, use these filters for the special parameters:

<code>indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&
indicator.type=FQDN</code></td></tr>
<tr><td>To send only the IOCs that have a custom status, e.g. Send to FortiGate, use the special parameters below.

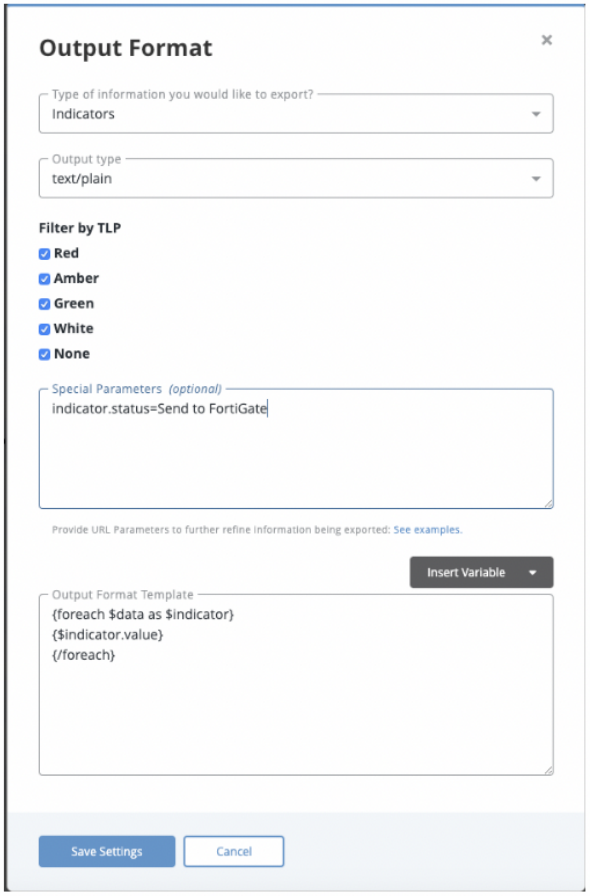
To create the custom status:

1. Follow the steps in the Adding an Indicator Status topic to create a status called Send to FortiGate.
2. Use the following special parameter:

<code>indicator.status=Send to FortiGate</code></td></tr>
</table>

Field	Selection
Output Format Template	{foreach $data as $indicator} {$indicator.value} {/foreach}

Once configured, the export will look similar to the snapshot below.



Configure FortiGate to Download Indicators from ThreatQ

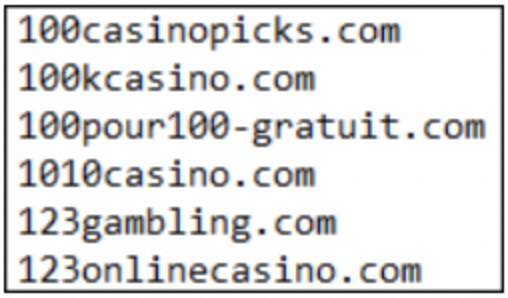
The following detailed steps have been copied from the FortiGate support center and provided here for convenience. The source is https://-docs.fortinet.com/document/fortigate/6.0.0/cookbook/85580

Blocking malicious domains using threat feeds

This example uses a domain name threat feed and FortiGate DNS filtering to block malicious domains. The text file in this example is a list of gambling site domain names.

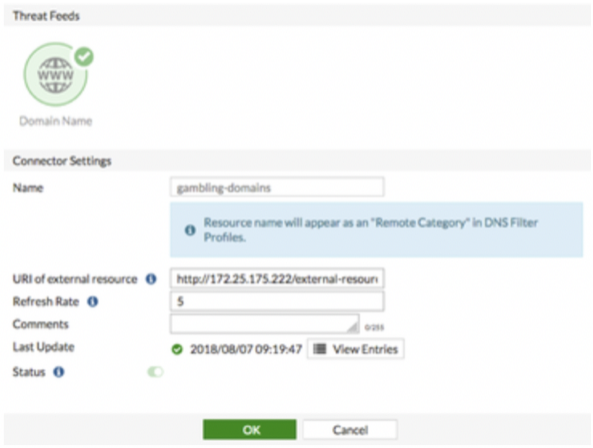
Threat feeds allow you to dynamically import external block lists in the form of a text file into your FortiGate. These text files, stored on an HTTP server, can contain a list of web addresses or domains. You can use threat feeds to deny access to a source or destination IP address in Web Filter and DNS Filter profiles, SSL inspection exemptions, and as a source/destination in proxy policies. You can use Fabric connectors for FortiGate that do not belong to a Fortinet Security Fabric.

1. Create an external block list. The external block list should be a plain text file with one domain name per line. The use of simple wildcards is supported. You can create your own text file or download it from an external service. Upload the text file to the HTTP file server.

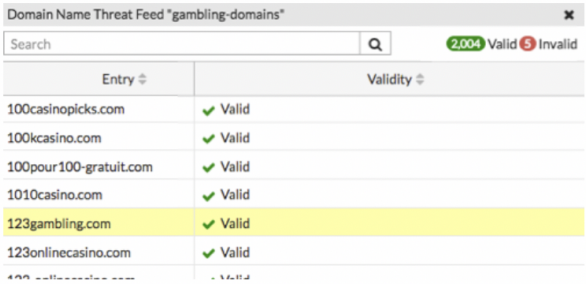


2. Configure the threat feed:
    a. In FortiOS, go to Security Fabric -> Fabric Connectors. Click Create New.
    b. Under Threat Feeds, select Domain Name.
    c. Configure the Name, URI of external resource, and Refresh Rate fields. In the URI of external resource field, enter the location of the text file on the HTTP file server. By default, the FortiGate rereads the file and uploads any

changes every five minutes.



d. Click View Entries to see the text file's domain list.



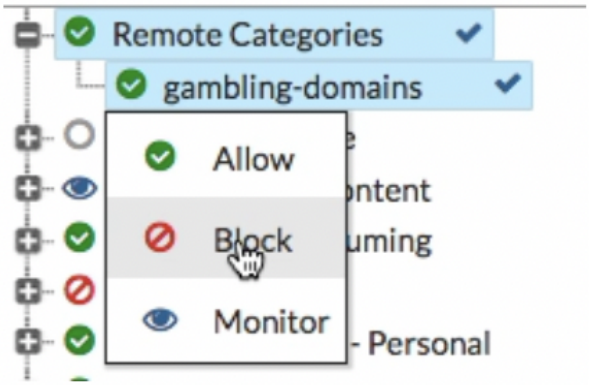
e. Click OK.

3. Add the threat feed to the DNS filter:

   a. Go to Security Profiles -> DNS Filter.

   b. Scroll to the list of preconfigured FortiGuard filters.

c. The resource file uploaded earlier is listed under Remote Categories. Set the action for this category to Block.



4. Configure the outgoing Internet policy:
   a. Go to **Policy & Objects -> IPv4 Policy**.
   b. Enable the **DNS Filter** under the *Security Profiles*.
   c. From the SSL Inspection dropdown list, select an SSL inspection profile.
5. View the results:
   a. Visit a domain on the external resource file. This example visits 123gambling.com. A Web Page Blocked! message appears.

   b. In FortiOS, go to **Log & Report -> DNS Query**. The logs show that the 123gambling.com domain belongs to a blocked category.

Configuring Lancope Exports

This topic explains how to export Lancope indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the

instructions below configure an export for your data.

To export to Lancope:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/csv; charset=utf-8**
   - Under **Special Parameters**, enter:

     indicator.status=Active&indicator.deleted=N&indicator.type=IP

     Address&indicator.type=CIDR Block&indicator.class=network

   - Under **Output Format Template**, enter:

     RECORD_NUMBER,GROUP_NAME,GROUP_ID,NETWORK_
     DEFINITION,PARENT_NAMESPACE

     0,ThreatQ,-1,,/

     {foreach $data as $indicator}

```
0,"{foreach $indicator.Sources item=source name=Sources}{$source.value}
{if $smarty.foreach.Sources.last != true},{/if}{/foreach}",-1,

{$indicator.value|regex_replace:"/[\r\t\n]/":""|replace:"\"":""},"/ThreatQ/"

{/foreach}
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Netwitness Exports

This topic explains how to export Netwitness indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data for:

- Netwitness FQDN
- Netwitness IP

To export to Netwitness FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/csv; charset=utf-8**.
   - Under **Special Parameters**, enter:

     indic-
     ator.status-
     =Ac-
     ctive&indicator.deleted=N&indicator.type=FQDN&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     "{$indicator.value}","{foreach $indicator.Sources as $source}{$source.value},

     {foreachelse}{/foreach}","https://{$http_host}/indicators/{$indicator.id}/details"

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Netwitness IP:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose Indicators.
   - For **Output type**, choose **text/csv; charset=utf-8**.
   - Under **Special Parameters**, enter:

     indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     "{$indicator.value}","{foreach $indicator.Sources as $source}{$source.value}, {foreachelse}{/foreach}","https://{$http_host}/indicators/{$indicator.id}/details"

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off,** toggle the switch to enable the export.

Configuring OpenIOC Signature Exports

This topic explains how to export OpenIOC signatures for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to OpenIOC CSV:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Signatures**.
   - For **Output type**, choose **text/csv**.
   - Under **Special Parameters**, enter:

     signature.status=Active&signature.deleted=N&signature.type=OpenIOC

   - Under **Output Format Template**, enter:

     {foreach $data as $signature}

     "{$signature.name|replace:"":'\"'}","{$signature.value|replace:"":'\"'}"

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Palo Alto Exports

This topic explains how to export Palo Alto indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the

instructions below to export your data.

To export to Palo Alto FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter:

     indic-
     ator.status-
     =Ac-
     ctive&indicator.deleted=N&indicator.type=FQDN&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value}

     ***.{$indicator.value}**

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Palo Alto: PANOS and Panorama

This topic describes the implementation between ThreatQ and Palo Alto firewall. The implementation is done using Palo Alto's External Dynamic List (EDL) functionality. An export with IOCs is first created on ThreatQ and the export URL is provided to Palo Alto as an EDL. The following details go over the steps to create, and add the EDL to ThreatQ.

Prerequisites

Before you begin the integration between Palo Alto and ThreatQ, confirm that there is a route between both hosts.

Create an export in ThreatQ

The export is a dynamic list of IOCs which should be configured on ThreatQ and provided to a Palo Alto instance to read from. To create an export in ThreatQ follow the steps in the provided link using the Adding an Export topic on the ThreatQ Help Center.

The following link lists the guidelines for the format of the export list in ThreatQ.

There are separate guidelines for IP, FQDN and URL lists.

These guidelines are both for PANOS and Panorama.:

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/formatting-guidelines-for-an-external-dynamic-list.html

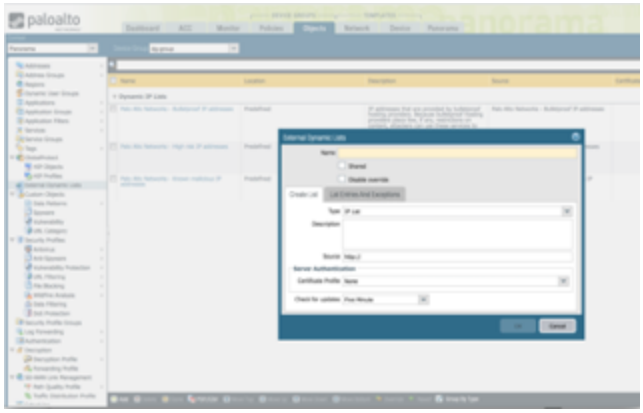
Configure an External Dynamic List (EDL) in PANOS

To add the dynamic list to Palo Alto, follow the instructions from here.

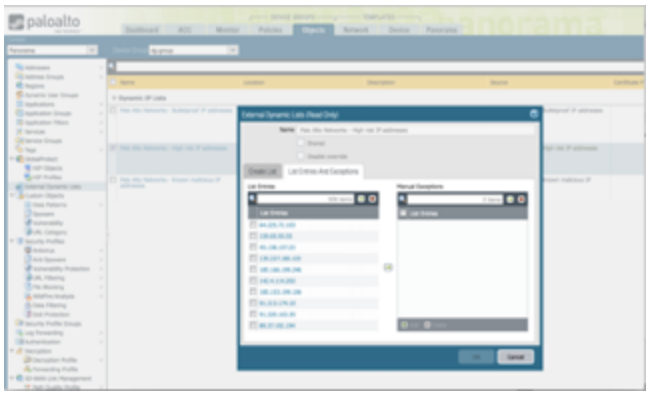
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/configure-the-firewall-to-access-an-external-dynamic-list.html

Configure an External Dynamic List (EDL) in Panorama

1. Navigate to **Device Groups > Objects**, and then click on the **External Dynamic List** in the left pane, about half way down.
2. Add a new dynamic list by clicking on the **Add** button at the bottom of the screen.



3. Provide a **Name**, **Type**, and for source provide the **ThreatQ exports URL**.



4. Click **OK**.

Retrieve an External Dynamic List from the Source

Once the list has been configured you can retrieve the indicators from that list.

Follow the steps from here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/-policy/use-an-external-dynamic-list-in-policy/retrieve-an-external-dynamic-list-from-the-web-server.html

Enforce Policy on an External Dynamic List

To create a policy to enforce rules for the indicators from the EDL, follow the steps from here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/enforce-policy-on-an-external-dynamic-list.html

Configuring Reservoir Labs Exports

This topic explains how to export Reservoir Labs indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to Reservoir Labs:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/plain**.

- Under **Special Parameters**, enter:

  indicator.status=Active&indicator.deleted=N

- Under **Output Format Template**, enter:

  #fields{$tab}indicator{$tab}indicator_type{$tab}meta.source{$tab}meta.url

  {foreach $data as $indicator}

  {if $indicator.type eq "CIDR Block"}{continue}{/if}

  {if $indicator.type eq "SHA-1"}{continue}{/if}

  {if $indicator.type eq "SHA-256"}{continue}{/if}

  {if $indicator.type eq "SHA-384"}{continue}{/if}

  {if $indicator.type eq "SHA-512"}{continue}{/if}

  {$indicator_type=""}

  {$source_found=0}

  {if $indicator.type eq "IP Address"}{$indicator_type="Intel::ADDR"}{/if}

  {if $indicator.type eq "URL"}{$indicator_type="Intel::URL"}{/if}

  {if $indicator.type eq "Email Address"}{$indicator_type="Intel::EMAIL"}{/if}

  {if $indicator.type eq "FQDN"}{$indicator_type="Intel::DOMAIN"}{/if}

  {if $indicator.type eq "MD5"}{$indicator_type="Intel::FILE_HASH"}{/if}

  {if $indicator.type eq "Filename"}{$indicator_type="Intel::FILE_HASH"}{/if}

  {if $indicator_type ne ""}

{$indicator.value}{$tab}{$indicator_type}{$tab}{foreach $indicator.Sources item=source name=Sources}{if $smarty.foreach.Sources.first == true}

{$source.value}{$source_found=1}{/if}{/foreach}{if $source_found == 0}-{/if}

{$tab}https://{$http_host}/indicators/{$indicator.id}/details

{/if}

{/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Splunk Exports

This topic explains how to export indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to Splunk:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

- Provide the following information:
- For **Which type of information would you like to export?** Choose **Indicators**.
- For **Output type**, choose **text/plain**.
- Under **Special Parameters**, enter:

  indicator.sincedeleted=Y

- Under **Output Format Template**, enter:

  #indicator{$tab}indicator_type{$tab}last_modified{$tab}reference_url{$tab}-source{$tab}campaign{$tab}status

  {foreach $data as $indicator}

  {$indicator.value}{$tab}{$indicator.type}{$indicator.updated_at}

  {$tab}https://{$http_host}/indicators/{$indicator.id}/details{$tab}{foreach $indicator.Sources item=source name=Sources}{$source.value}{if $smarty.-foreach.Sources.last == false}, {/if}{/foreach}{$tab}{foreach $indicator.Adversaries item=adversary name=Adversaries}{$adversary.value}{if $smarty.foreach.Adversaries.last == false}, {/if}{/foreach} {$tab}{$indicator.status}

  {/foreach}

5. Click **Save Settings**.
6. Under **On/Off**, toggle the switch to enable the export.

Configuring Symantec ProxySG

Topic Sections:

This topic describes the implementation between ThreatQ and the Symantec ProxySG appliance. The implementation is done using the Local Database Content Filtering functionality available in the ProxySG. An export with IOCs is first created on ThreatQ and the export URL is installed on the proxy.

Before starting the integration, users are encouraged to familiarize themselves with the following documents:

- Symantec ProxySG CLI: https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10456/en_US/6.7CLI.pdf?__gda__=1582794846_0c0b5ae73454290ea953391b8aa5f508
- Local Content Filtering Database: https://origin-symwisedownload.symantec.com/resources/webguides/managementcenter/2.0.1.1/Content/ConfigurationManagementGuide/6_Policy/local_db.htm

Before you begin the integration between Symantec ProxySG and ThreatQ, confirm that there is route between both hosts.

Create an Export in ThreatQ

The export is a dynamic list of IOCs which should be configured on ThreatQ and provided to a ProxySG instance to read from. To create an export in ThreatQ follow the steps in the Adding an Export topic on the ThreatQ Help Center.

The export script should be the following. This will strip the port and URL path from the IOCs.

```
define category threatq_iocs
{foreach $data as $indicator}
{assign var=parts value="/"|explode:$indicator.value}
{assign var=hostname value=":"|explode:$parts[2]}
{assign var=fqdn value=":"|explode:$parts[0]}
{if $fqdn[0] eq "http" or $fqdn[0] eq "https"}
{assign var=domain value=$hostname[0]}
{else}{assign var=domain value=$fqdn[0]}{/if}
{$domain}
{/foreach}
end
```

Configure ProxySG to Download Indicators from ThreatQ

There are two methods to install the dynamic list in the ProxySG -

- via the Management Console
- via the Proxy's CLI

The management console UI can accept only a single block list. Starting with ProxySG v6.7.4, you can configure the proxy to read from up to seven dynamic lists. The following two sections go over the methods for installing dynamic block lists.

Via the Management Console

1. Open the ProxySG management console.
2. Navigate to **Configuration > Content Filtering Local Database**.

   The following screen will load.

3. Insert the **export URL** from TQ in the **URL** space and click on the **Download now** button.

   This will initiate a pull of the indicators from the ThreatQ into the proxy. To check on the status of the download, click on **View Download Status**. Any download related messages will be shown in the download status window.

Via the ProxySG CLI

In addition to the Management Console UI, the proxy has a CLI which provides more configuration options. In the reference section at the end of this document, you can find a PDF document with the CLI commands. To help with testing of the integration below is a sequence of commands that allows a user to install the exports from ThreatQ in a local content database on the proxy.

1. Log into the Blue Coat CLI:

```
ssh <username>@<BlueCoat Hostname/IP>
```

Use the password set in the initial configuration.

2. Enable the admin mode:

```
enable
```

You will be prompted for a password which is usually the account password.

3. Enter the following command access the config model of the appliance.

```
config
```

4. Select **TERMINAL** at the prompt.
5. Start working with the content filtering database:

```
content-filter
```

6. Enter the Local Content Filtering DB mode.

```
local
```

7. Create a new database name if needed.

```
create tq_test
```

8. Enter db edit mode to download the URL.

```
edit tq_test
```

9. Bind the URL of the ThreatQ export to the content database on the ProxySG.

Put double quotes around the URL.

```
download url
"https://<TQ>/api/export/<hash>/?limit=1000&tok
en=<token>"
```

10. Download the database now.

```
download get-now
```

11. View the status of the current, and older, download

```
view
```

12. Show the contents of the downloaded local database file.

```
source
```

13. If you want to configure auto downloads there are various options available. To list all the download options use the following command

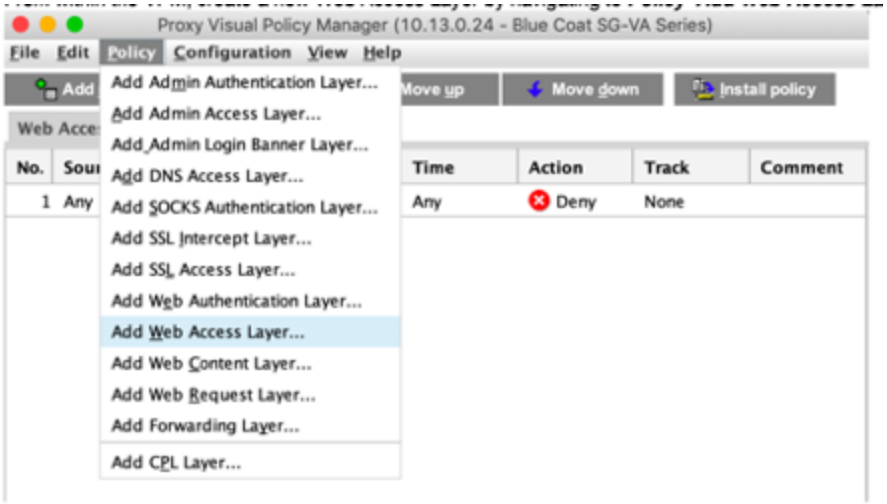
```
download ?
```

Create and Install a Content Filtering Policy

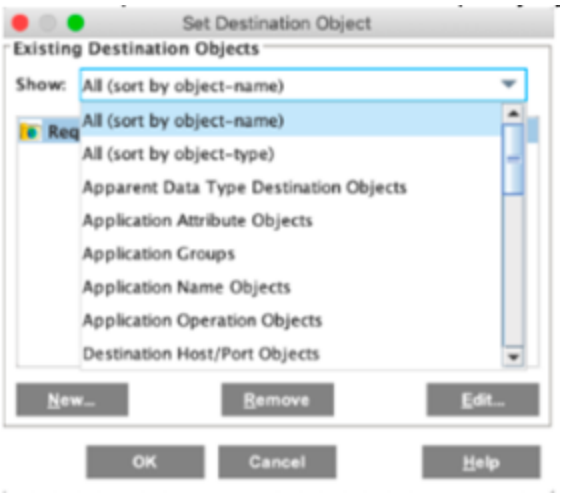
The final step is to install a content filtering policy using the indicators from the ThreatQ export which are being downloaded to a content filtering database on the proxy.

1. Open ProxySG (the example here uses the virtual proxy appliance).
2. Navigate to **Configuration Policy > Visual Policy Manager** and click on **Launch Java VPM**.

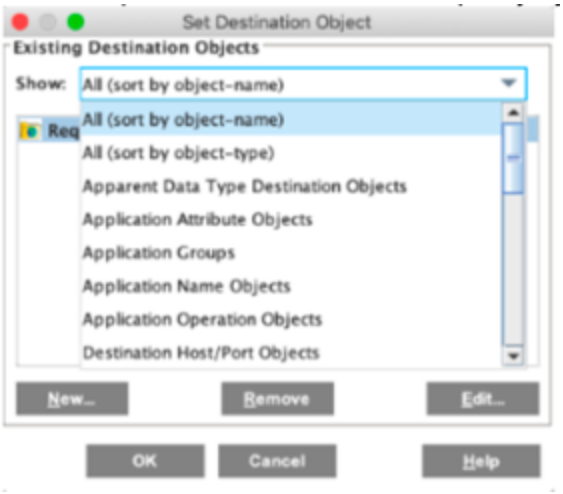
3. From within the VPM, create a new **Web Access Layer** by navigating to **Policy Add > Web Access Layer**.



4. Assign a name for the new layer, and after it's created right click on the **Destination object** and select **Set**.



5. Under the drop down in the modal window select **All (sort by object name)** and then click on **Edit** in the lower right corner.



This will open a new window, in which you can select all the categories to be blocked by the ProxySG appliance. The list of URLs exported from ThreatQ will be available under the Local category.

6. Expand **Local** and select the name you've given the export from ThreatQ. In this example, the name is **tq_malicious_url**.

7. Click **OK**, and then again **OK** to go back to the **VPM**.
8. Highlight the newly created policy layer, and click on the **Install policy** button in the upper right corner.

> Before installing the policy, make sure that the type of **Action** on the policy is **Deny**. If it shows **Allow**, make sure to change it to **Deny**. The action instruction what type action ProxySG should enforce when it detects that a user sends a request to any of the indicators in the list exported from ThreatQ.

9. The new policy is now installed and any active indicators exported from ThreatQ will be blocked by the ProxySG.

Configuring Tenable Exports

This topic explains how to export Tenable indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data for:

- Tenable FQDN
- Tenable IP Address
- Tenable MD5 Address

To export to Tenable FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:

   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose text/plain.
   - Under **Special Parameters**, enter:

     indic-
     ator.status-
     =Ac-
     ctive&indicator.deleted=N&indicator.type=FQDN&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value},{foreach $indicator.Sources item=source name=Sources}

     {$source.value}{if $smarty.foreach.Sources.last == false}/{/if}{/foreach}

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Tenable IP Address:

1. From the navigation menu, choose the **gear icon > Exports**.
2. The Exports page appears.
3. Click **Add New Export**.
4. The Connection Settings dialog box appears.
5. Enter an **Export Name**.

6. Click **Next Step**.
7. The Output Format dialog box appears.
8. Provide the following information:
    - For **Which type of information would you like to export?** Choose **Indicators**.
    - For **Output type**, choose **text/plain**.
    - Under **Special Parameters**, enter:

      indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network

    - Under **Output Format Template**, enter:

      {foreach $data as $indicator}

      {$indicator.value},{foreach $indicator.Sources item=source name=Sources}

      {$source.value}{if $smarty.foreach.Sources.last == false}/{/if}{/foreach}

      {/foreach}
9. Click **Save Settings**.
10. Under **On/Off**, toggle the switch to enable the export.

To export to Tenable MD5 Address:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

5. The Output Format dialog box appears.
6. Provide the following information:
    - For **Which type of information would you like to export?** Choose **Indicators**.
    - For **Output type**, choose **text/plain**.
    - Under **Special Parameters**, enter:

      indic-
      ator.status-
      s=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=network

    - Under **Output Format Template**, enter:
    - **{foreach $data as $indicator}**
    - **{$indicator.value},{foreach $indicator.Sources item=source name-**
      e=Sources}
    - **{$source.value}{if $smarty.foreach.Sources.last == false}/{/if}{/foreach}**
    - **{/foreach}**
7. Click **Save Settings**.
8. Under **On/Off**, toggle the switch to enable the export.

Common Enrichment and Audit Log Questions

The ThreatQ Audit Log tracks every change made to every object in the system. If there is a change to an object, that change is displayed in the audit log. The audit log is only updated if the data itself changes, not just the **updated_at** value.

The following questions below address further details about the audit logging process.

In the case where an activity is triggered (with nothing updated), where will the activity be logged?

The activity will not show in the audit log, as there were no changes to report. While ThreatQ does not track duplicate objects that enter the application, there is a **touched_at** date field on primary objects (Adversaries, Files, Events, Indicators, and Signatures) that indicates when a relation of the object has been changed.

Is there another raw audit log within the system where events are logged?

No, there are no other raw audit logs where events are logged.

Is there an option in the User Interface to enable all activities to be shown in the Audit Log?

There is no option in the User Interface to limit or expand the audit log. All entries are pulled for an object when the Audit Log panel is opened. The audit log displays changes to the individual fields of an object; object comments, sources, attributes, and tags; as well as to object links, object link comments, and object link attributes. Additionally, any changes to the score of an Indicator are included.

Air Gapped Data Sync (AGDS)

The following explains how to configure and complete an Air Gapped Data Sync from a source ThreatQ instance to a target air-gapped ThreatQ instance.

Air Gapped Data Sync Overview

Air Gapped Data Sync (AGDS) allows you to transfer data from a source ThreatQ installation to a target air-gapped ThreatQ installation. ThreatQ defines an air-gapped system as one that is not connected to a public network. This means that **external** feed ingestion will not occur on the air-gapped installation.

You should consult with ThreatQ Support or a Threat Intelligence Engineer prior to performing an Air Gapped Data Sync.

Air Gapped Data Sync consists of two synchronization commands:

- **threatq:sync-export**: the read command that copies data from the source ThreatQ installation
- **threatq:sync-import**: the write command that copies data to the target ThreatQ installation

If you are using LDAP or SAML authentication on your **Source** ThreatQ instance, and require users transferred via import to have authentication

capabilities on your **Target** ThreatQ instance, then you must enable the same authentication method on your **Target** ThreatQ instance prior to performing import.

This section includes deployment details and configurations that should not be deviated from or changed without first consulting with ThreatQuotient. Any deviation of the ThreatQuotient recommended settings could result in system and platform instability, may render the system non-operational, and are not supported.

Air Gapped Data Sync System Requirements

To use Air Gapped Data Sync, ThreatQ installations must meet the following requirements:

- ThreatQ v4.15 or later must be installed.
- All ThreatQ installations must run the same software version.
- All ThreatQ installations must be set to the correct time, time zone, and date, and using a clock source available to all. UTC is recommended.

Understanding threatq:sync-export

The purpose of this command is to pull all objects, object context, tags, and object links from the source ThreatQ installation and then store them in CSV data dump files. You can specify which objects are pulled, based on a date or via configuration. All data pulled into the CSV data dump files can then be transferred to a target air-gapped ThreatQ installation for validation and import. Each run of this command also generates a sync report with output logs for the run.

threatq:sync-export Parameters

The following table outlines the parameters for the command. All parameters for the threatq:sync-export command are optional. If you do not set any parameters, the system runs a default configuration as explained in threatq:sync-export Configuration.

Parameter	Explanation
--target	Target directory where the output file should be placed. This value is required. Default: /tmp example: --target=/my/directory
--start-date	The start date for data selection. This value is required. ex: --start-date="2018-01-01 00:00:00"
--end-date	The end date for data selection. This value is required. Applies only to objects themselves, not object context or object links.

Parameter	Explanation
	example: --end-date="2018-01-02 00:00:00"
--include-deleted	Determines whether objects that have been soft-deleted are included in the result set. Options are Y(es) or N(o). Default: N example: --include-deleted=Y
--include-investigations	Determines whether Investigations and Tasks are included in the result set. This value is required. Options are Y(es) or N(o). Default: N example: --include-investigations=N
--meta-only	If present, tells the command to only include meta data (no object data) in the result set. No value necessary.
--memory-limit	Sets the PHP memory limit in Megabytes or Gigabytes. This value is required. Default: 2G example: --memory-limit=4G

Parameter	Explanation
--object-limit	Sets the limit on the number of objects selected at a time. Recommended use is to set the limit to a number smaller than the default (50,000) on boxes with very large data sets. Default: 50,000 example: --object-limit=10000
--ignore-file-types	Defines a comma-delimited list of ThreatQ File Types for which physical files stored on the source ThreatQ installation should not be transferred to the target air-gapped ThreatQ installation. Database records are still included in the export tarball. example: --ignore-file-types="Malware Analysis Report" example: --ignore-file-types="Malware Analysis Report,Malware Sample"

threatq sync-export Examples

This command should be run from inside the `/var/www/api directory`. The following examples provide use cases for air gapped data sync.

No Time Limit, Default Configuration

```
sudo ./artisan threatq:sync-export
```

This example will pull all objects in the system (with the exception of Investigations, Tasks, and soft-deleted Objects). The output will appear in /tmp.

Meta Data Only

```
sudo ./artisan threatq:sync-export --meta-only
```

This example will pull only meta data objects from the system (Attributes, Sources, Object Statuses and Types, and so on).

Time Limit

```
sudo ./artisan threatq:sync-export --start-date
="2018-10-01 00:00:00" --end-date="2018-11-01
00:00:00"
```

This example will pull objects whose `updated_at` or `touched_at` occurs between the start and end date.

Exclude Malware Files

```
sudo ./artisan threatq:sync-export --ignore-file-
types="Malware Sample"
```

This example will pull all objects, but will exclude the physical files attached to any File objects with the type Malware Sample. The File objects themselves (as well as their context and relationships) will still be included in the export tarball.

Any File Type can be used with this option, and multiple File Types can be included as a comma-delimited list.

```
sudo ./artisan threatq:sync-export --ignore-file-
types="STIX,PDF,Malware Sample"
```

Cron Configuration

```
sudo ./artisan threatq:sync-export
--target=/my/directory --include-deleted=Y
--include-investigations=N
```

This example will do a search for a previous synchronization record with the same hash (comprised of the three options provided). If any hash matches are found, the run will use the `started_at` date of the most recent previous record as the start date for the current run.

If you do not require soft-deleted Objects, Investigations, or Tasks to be transferred to the target ThreatQ installation, then only the `--target option` is necessary (as the defaults for the other two options are both (N)o).

threatq sync-export Initial Cron Setup for First Time Use

Basic Instructions

Determine what the cron configuration options should be:

- target directory
- whether investigations/tasks should be included
- whether deleted objects should be included

The cron configuration options must be the same for every run, but they only need to be specified if different from the defaults.

Run the command with the cron configuration options:

```
php artisan threatq:sync-export
--target=/my/directory --include-investigations=Y
--include-deleted=N
```

Instructions for Larger Data Sets (Starting from the Beginning of Time)

For larger data sets, it is undesirable to do a full run from the beginning of time (performance will suffer).

ThreatQuotient recommends that you use the `--end-date` option to specify an upper limit on the date range pulled. Multiple runs will be necessary to process all data up to the current date.

Determine what the cron configuration options should be:

- target directory
- whether investigations/tasks should be included
- whether deleted objects should be included

The cron configuration options will need to be the same for every run, but they only need to be specified if different from the defaults.

For each of the runs, provide the configuration options along with the `--end-date` option:

```
php artisan threatq:sync-export
--target=/my/directory --include-investigations=Y
--end-date="2017-01-01 00:00:00"
```

Once the current date has been reached, the `--end-date` option will no longer be necessary.

Instructions for Larger Data Sets (Starting from a Specified Date)

For larger data sets, it is undesirable to do a full run from the beginning of time (performance will suffer).

> ThreatQuotient recommends that you use the `--end-date` option to specify an upper limit on the date range pulled. Multiple runs will be necessary to process all data up to the current date.

If only a subset of data needs to be processed up to the current date, then you should use the `--initial-start-date` option.

Determine what the cron configuration options should be:

- target directory
- whether investigations/tasks should be included
- whether deleted objects should be included

The cron configuration options will need to be the same for every run, but they only need to be specified if different from the defaults.

For the first run, provide the configuration options along with the `--initial-start-date` option.

```
php artisan threatq:sync-export
--initial-start-date="2017-01-01 00:00:00" --tar-
get=/my/directory
--include-investigations=Y --end-date="2017-02-01
00:00:00"
```

For each of the runs, provide the configuration options along with the `--end-date` option:

```
php artisan threatq:sync-export
--target=/my/directory --include-investigations=Y
--end-date="2017-01-01 00:00:00"
```

Once the current date has been reached, the `--end-date` option will no longer be necessary.

threatq sync-export Run Scenarios

Success

When a run of this command completes successfully, a tarball of data will appear in the target directory you specified (or /tmp by default). A report file describing the run will be available in the data tarball, under the /sync directory. There will also be a record in the database synchronizations table for the run.

Errors

If a run of this command fails before completion, the tarball will not be created. There will be a data directory in the target directory (where the data is stored before it is compressed) that contains all the data that was processed before the failure. The report file will appear in this directory under /sync. Error messages will not appear in the report file - though they will appear in the laravel log and in the console.

Regardless of whether the run was part of a cron configuration, it can simply be restarted. The cron configuration will look for the last completed run to find the next start date.

threatq:sync-export Dates

Start Date

A start date is applied to objects according to the column available - `touched_at or updated_at`.

`touched_at Objects`

Adversaries, Attachments, Events, Indicators, Signatures, Custom Objects

`updated_at Objects`

Investigations, Tasks, Object Links, Tagged Objects

End Date

An end date is applied only if you provide one at run time. It is applied everywhere a start date is used.

threatq:sync-export Configuration

The configuration used for each run of this command consists of the `--target`, `--include_deleted`, and `--include_investigations` command line options and is stored in the `config_json` column of the Synchronization record. The hash column of each Synchronization record is a md5 hash of the `config_json` column.

Default

The default configuration is used if the command is run with no options provided:

- target_directory = /tmp
- include_deleted = false
- include_investigations = false

In this configuration, the initial run start date will default to 1970-01-01 00:00:00.

Cron

If the command is run with the `--target`, `--include_deleted`, and `--include_investigations` parameters, the hash of these values will be compared against the hash column of previous runs. Using these three options on every run allows for the command to be incorporated into a scheduled task.

If any hash matches are found, the start date for the run will be set to the `started_at` date in the Synchronization record of the previous run with the same hash.

If no hash matches are found, the start date will be set to 1970-01-01 00:00:00.

Start Date Provided

If a start date is included in the command run using the `--start-date` option, any other options also provided will be honored. However, if the `--target`, `--include_deleted` and `--include_investigations` options are also included, a Cron check against the hash of these three options will **not** occur. The start date provided will be included in `config_json` as the **manual_start_date** so that the run does not collide with any Cron-related runs.

If a "beginning of time" run is necessary, use the option as `--start-date="1970-01-01 00:00:00"`.

threatq:sync-export Output and Sync Report

The following sections detail the data you may find in the export output and sync report.

threatq:sync-export Meta Data

Meta data is transferred with every run of this command by default. You can specify that only meta data (no object data) should be pulled in a run by using the `--meta-only` option.

Meta data includes information about Sources, Attributes, Tags, as well as Object Statuses and Types (both seeded and user-provided).

While meta data like Connectors and Operations are included in this list, they are not installed on the target ThreatQ installation as part of the air gapped data sync process. They are only placed in the requisite tables for use as Sources of Objects that are transferred. The same is true of any Users that are copied - these will not be enabled Users on the target installation; they will be transferred as disabled.

Meta Data Objects:

- Attributes
- Clients
- Connectors
- Connector Categories
- Connector Definitions
- Content Types
- Groups
- Investigation Priorities
- <Object Type> Statuses
- <Object Type> Types
- Other Sources
- Operations
- Sources
- Tags
- TLP
- Users

threatq:sync-export Objects

This command covers any objects installed on the system by default, and any custom objects that have been installed by the user. The only objects that can be excluded are Investigations and Tasks (using the `--include-investigations` command line option).

> ⚠ Custom Objects that are installed on a source ThreatQ installation that have NOT been installed on a target ThreatQ installation will NOT be installed by the air gapped data sync process. If an object is included in the export data, but is not found on the target, it will be ignored.

Default Objects:

- Adversaries
- Attachments (Files)
- Events
- Indicators
- Signatures
- Campaigns
- Courses of Action
- Exploit Targets
- Incidents
- TTPs

Storage:

The data for each object is copied as a dump file in CSV format using "SELECT * INTO OUTFILE..." MariaDB syntax. The full query for the data is built up using the options you provided (start date, end date, etc).

Dump files contain a maximum object limit of 50,000 (set in the Synchronization base class). Dump files are created (with a counter appended to the file name) until the entire object result has been covered.

To ensure that any Objects present in Object Context (Attributes, Comments, and Sources), Object Links, Tagged Objects, or Investigation Timeline Objects are also included in the base Object data, CSV dump files for each Object type are also created from queries against each of these tables. This is necessary because of the differing date columns used in each query (an object may appear in an Object Link in the specified date range according to the Object Link's `updated_at` date, even though the Objects themselves saw no change to their `touched_at` date in that date range). When the data from all of these object files is transferred to the target ThreatQ installation, any duplicates across dump files will be consolidated. Files that contain Object data will always include "_obj_" in the file title.

Sample Object File List (all of these files will contain Adversary records):

- adversaries/adversaries_obj_0.csv
- adversaries/adversaries_obj_attributes_0.csv
- adversaries/adversaries_obj_comments_0.csv
- adversaries/adversaries_obj_investigation_timelines_0.csv
- adversaries/adversaries_obj_object_links_dest_0.csv
- adversaries/adversaries_obj_object_links_src_0.csv
- adversaries/adversaries_obj_sources_0.csv
- adversaries/adversaries_obj_tags_0.csv

threatq:sync-export Object Context

The date range for queries on Object Context tables uses the `updated_at` date column, with the exception of Adversary Descriptions, which uses the `created_at` date column.

Adversary Descriptions are handled as part of the Object Context gathering process. The `adversary_descriptions` table is queried using the created_at date column, and the entirety of the `adversary_description_values` table is pulled, as it doesn't have a date column.

Not all Objects have all Object Contexts (Attributes, Attribute Sources, Comments, and Sources). Tables are only polled if they exist.

Tables Covered for each Object Type:

- <object type>_attributes
- <object type>_attribute_sources
- <object type>_comments
- <object type>_sources

Sample Object Context File List (Indicator Object Type):

- indicators/indicator_attribute_sources_0.csv
- indicators/indicator_attributes_0.csv
- indicators/indicator_comments_0.csv
- indicators/indicator_sources_0.csv

threatq:sync-export Other Data

Attachment Files

Physical files for all attachments included in the date range are copied into the attachments/files directory of the data tarball.

Object Links

The date range for queries on Object Links uses the `updated_at` date column.

Tables Covered (Object Links and Object Link Context):

- object_links
- object_link_attributes
- object_link_attribute_sources
- object_link_comments
- object_link_sources

Sample Object Link File List:

- object_links/object_links_0.csv
- object_links/object_link_attributes_0.csv
- object_links/object_link_attribute_sources_0.csv
- object_links/object_link_comments_0.csv
- object_links/object_link_sources_0.csv

Tags

The date range for queries on Tagged Objects uses the `updated_at` date column.

Tables Covered (Tags themselves are covered in the Meta Data):

tagged_objects

Sample Tagged Objects File List:

tagged_objects/tagged_objects_0.csv

Spearphish

The date range for queries on Spearphish uses the `updated_at` date column.

Tables Covered:

spearphish

Sample Spearphish File List (Spearphish files are stored with Event data):

events/spearphish_0.csv

Investigations

The date range for queries on additional Investigation context tables uses the `updated_at` column.

Tables Covered:

- investigation_nodes
- investigation_node_properties
- investigation_timelines
- investigation_timeline_objects
- investigation_viewpoints

Sample Investigation additional context File List:

- investigations/investigation_node_properties_0.csv
- investigations/investigation_nodes_0.csv
- investigations/investigation_timeline_objects_0.csv

- investigations/investigation_timelines_0.csv
- investigations/investigation_viewpoints_0.csv

threatq:sync-export File Output

threatq:sync-export Data Tarball

Once all data has been processed, a tarball is created containing all output files. This tarball will be dropped in the directory specified in the `--target option`, or the /tmp directory by default.

Tarball Naming Convention: `tqSync_<run date>.tar.gz`

Example: tqSync-19-01-16-1547649934-0849.tar.gz

threatq:sync-export Sync Report

The output for each run is stored in a Sync Report output file, which is located in the sync directory of the data tarball. The file is always named sync-export.txt.

threatq:sync-export Command Line Output

Command line output displays command progress, object totals, and files written.

threatq:sync-export Synchronizations

Table

synchronizations

- `id` - The auto-incremented id for the Synchronization record
- `type` - The Synchronization direction (options are "export" or "import")

- `started_at` - The date and time the command run was started
- `finished_at` - The date and time the command run completed
- `config_json` - A JSON representation of the command run configuration
- `report_json` - A JSON representation of the command run parameters (command line options, object counts, files created, etc)
- `pid` - The process id of the command run
- `hash` - Unique identifier for a command run (md5 hash of the config_json column)
- `created_at` - The date and time the Synchronization record was created
- `updated_at` - The date and time the Synchronization record was updated

Record Handling

Hash

The Synchronization record hash column is automatically calculated as an md5 of the `config_json` column on record creation.

Initial Creation

A Synchronization record is created at the beginning of a command run, right after all command line options have been processed. Initial creation only covers the `type`, `started_at`, `pid`, and `config_json` columns. For this command (`threatq:sync-export`), the type will be "export". The command line option portion of the `report_json` is added as well, but this column will not be complete until the record is finalized. The `finished_at` column remains NULL.

Finalization

A Synchronization record is finalized when the command run has completed. At this time, the `finished_at` column is filled with the completion datetime, and the `report_json`

column is updated to include information about the run (object counts, files created, etc).

Understanding threatq:sync-import

The purpose of this command is to process the tarball of object data created by the threatq:-sync-export command. Temporary sync tables are created on the target to house this object data, and integrity checks are run against existing data to verify IDs and check for duplicate objects. Duplicate objects from the source ThreatQ installation are updated, and new objects are inserted. The temporary sync tables are dropped when data processing is complete. Each run of this command also generates a sync report without output logs for the run.

threatq:sync-import Parameters

The following table outlines the parameters for the command. With the exception of `--file`, which is required, all parameters for the threatq: sync-import command are optional.

Parameter	Explanation
--file	File path to the tarball created by the `threatq:sync-export` command. This command is required to run the `threatq:sync-import` command. example: --file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz

Parameter	Explanation
--keep-created-at	Determines whether the oldest `created_at` date between the source and target ThreatQ installations should be maintained, or a new `created_at` is set on the target system. The default if this option is not provided by the user is for the oldest `created_at` date to be maintained. This value is required. Options are Y(es) or N(o). Default: Y example: --keep-created-at=N
--object-limit	Integer value used as the limit for the number of objects updated or inserted at a time. This value is required. When using this option, the size of the data sets on both source and target ThreatQ installations should be taken into account. Setting the limit too high may hinder performance. Default: 1000 example: --object-limit=50000
--memory-limit	Sets the PHP memory limit in Megabytes or Gigabytes. This value is required. Default: 2G example: --memory-limit=4G
--override-description	Determines whether or not the descriptions on existing objects on the target ThreatQ installation will be updated. If an existing object has a NULL description, it will be updated

Parameter	Explanation
	regardless of the use of this flag. Default: Y example: --override-description=N

threatq:sync-import Examples

This command should be run from inside the `/var/www/api` directory.

Basic Run

```
sudo ./artisan threatq:sync-import
--file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz
```

This example will process all the data in the tarball provided in the `--file` option, using an object limit of 1000 for all inserts and updates. The `created_at` date of all transferred objects will be updated on the target ThreatQ installation if it is older than the current `created_at` date (if the object is already present on the source ThreatQ installation). Newly inserted objects will keep the `created_at` date of the source ThreatQ installation.

Set New created_at Dates on the Write System

```
sudo ./artisan threatq:sync-import
--file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz
--keep-created-at=N
```

This example will process all the data in the tarball provided in the `--file` option using an object limit of 1000 for all inserts and updates. The `created_at` date of all transferred will

be left alone in the case of object updates, and to the current time in the case of new object inserts.

Increase the Object Limit

```
sudo ./artisan threatq:sync-import
--file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz
--object-limit=50000
```

This example will process all the data in the tarball provided in the `--file` option using an object limit of 50000 for all inserts and updates. The `--keep-created-at` option has been left out, so it will use the default setting of Y(es) and `created_at` dates will be maintained from the read system.

threatq:sync-import Initial Setup

You **must** run the `threatq:fill-sync-hash-column` command, before running the `threatq:sync-import` command on an air gapped ThreatQ installation. This command prepares the database of an air gapped installation to run the threatq:sync-import command. Upon upgrade to ThreatQ version 4.17 and later, several tables will include a sync_hash column, which stores an MD5 hash of the unique fields for records in each table. This command fills in the data in this column, before attempting an Air Gapped Data Sync import. Data added after upgrade will automatically have their sync_hash columns populated on insert and update, so it is only necessary to run this command once.

The threatq:sync-import command checks for any NULL values in the sync_hash column in the events, indicators, and object_links tables before importing any data, and will fail if any NULL values are found. If the threatq:fill-sync-hash-column command is not run and sync_hash columns are found on the indicators, events, or object_links tables, the import will fail and ask you to run the command to fill that column before continuing.

Running the threatq:fill-sync-hash-column Command

1. SSH to your target ThreatQ installation.
2. Change directories to `/var/www/api`.
3. Run `php artisan down` to place ThreatQ into maintenance mode.
4. Run the following command:

   ```
   sudo ./artisan threatq:fill-sync-hash-column
   ```

5. Run `php artisan up` to bring ThreatQ out of maintenance mode.

threatq:sync-import Run Scenarios

Success

When a run of this command completes successfully, a report will appear in the directory the command was run in (/var/www/api). There will also be a record in the database synchronizations table for the run. Both of these will contain data describing performance metrics and object counts.

Excluded Files

If the `--ignore-file-types` option was used during creation of the export tarball, then the physical files associated with File objects that have the File Types specified in that option will not be available during the import of those objects. If the import command detects that a file is missing from the export tarball, it will create a placeholder file under the same file path as was set on the read box (this is defined in the path field of the File). This placeholder file will be a simple text file with the phrase "File excluded from export.". Please be aware that because the original physical file associated to the File object has been replaced, it will no longer be possible to open the physical file on the Details page for that File object.

Errors

If a run of this command fails before completion, error messages will not appear in the report file - though they will appear in the laravel log and in the console. There is not currently a means of restarting the command from where it left off. The command will need to be restarted and will run through all the data again. Any data from the tarball that was written during the previous failed run will simply be updated (rather than inserted again), meaning the end result will be the same - all data will be transferred from the tarball to the target system.

threatq:sync-import Data Processing

Data found in CSV dump files for a table from the tarball provided in the `--file option` is inserted into a corresponding sync table. A sync table is just a copy of a base table, with column structure maintained but indexes excluded. Indexes are added to unique columns on sync tables (which will later be used in table joins and where clauses) once data insertion from dump files is complete, since indexes slow the insertion process down.

The naming convention for a sync table is sync_import_<base table name>_<process id>.

Example:

Base table: adversaries

Sync table: sync_import_adversaries_12345

All sync tables are removed from the target ThreatQ installation's database once data processing is complete.

threatq:sync-import Basic Table

A basic table has no foreign keys pointing to other tables in the database. It has a single identifier (id) column for each record. Once all the data stored in the tarball for a basic table has been transferred to a sync table, the sync table has an `existing_id` column added with a default value of NULL for each record. This column is used to determine whether the record already exists on the target ThreatQ installation. The id for the record on the target system may be different from that of the record from the source ThreatQ installation, so this `existing_id` column ensures that data integrity is maintained between the two.

Sample Basic Table:

`attachment_type`s - (id, name, is_parsable, parser_class, created_at, updated_at, deleted_at)

Sample Sync Table created from Basic Table:

`sync_import_attachment_types_12345` - (existing_id, id, name, is_parsable, parser_class, created_at, updated_at, deleted_at)

threatq:sync-import Tables with Pivots

A pivot table has one or more foreign keys pointing to other tables in the database. Once all the data stored in the tarball for a table with pivots has been transferred to a sync table, the sync table has an `existing_<pivot>_id` column added for each foreign key column, as well as an `existing_id` column for the record itself (all set to a default value of NULL).

threatq:sync-import File Output

threatq sync-import File Output and Sync Report

Once all data has been processed, a Sync Report will be generated in the `/var/www/api` directory (where the command is run). This file will be named after the tarball used in the run, with the extension "-sync-import.txt"

Example:

> Tarball used: tqSync-19-01-16-1547660837-8345.tar.gz
>
> Sync Report name: tqSync-19-01-16-1547660837-8345-sync-import.txt

threatq:sync-import Command Line Output

Command line output displays command progress and object totals. It will be similar to the output in the Sync Report.

threatq:sync-import Synchronizations

Table

synchronizations

- `id` - The auto-incremented id for the Synchronization record
- `type` - The Synchronization direction (options are "export" or "import")
- `started_at` - The date and time the command run was started
- `finished_at` - The date and time the command run completed
- `config_json` - A JSON representation of the command run configuration
- `report_json` - A JSON representation of the command run parameters (command line options, object counts, tables created, etc)
- `pid` - The process id of the command run
- `hash` - Unique identifier for a command run (md5 hash of the config_json column)
- `created_at` - The date and time the Synchronization record was created
- `updated_at` - The date and time the Synchronization record was updated

Record Handling

Hash

The Synchronization record hash column is automatically calculated as an md5 of the `config_json` column on record creation.

Initial Creation

A Synchronization record is created at the beginning of a command run, right after all command line options have been processed. Initial creation only covers the type, `started_at`, `pid`, and `config_json` columns. For this command (`threatq:sync-import`), the type

will be "import". The command line option portion of the `report_json` is added as well, but this column will not be complete until the record is finalized. The `finished_at` column remains NULL.

Finalization

A Synchronization record is finalized when the command run has completed. At this time, the `finished_at` column is filled with the completion date and time, and the `report_json` column is updated to include information about the run (object counts, tables created, etc).

Executing Air Gapped Data Sync

Using artisan commands at the command line of the ThreatQ installation, you execute air gapped data sync in two steps:

1. You run the **threatq:sync-export** command on the source ThreatQ installation; see Understanding threatq:sync-export.
2. You run the **threatq:sync-import** command on the target ThreatQ installation, see Understanding threatq:sync-import.

Running the threatq:sync-export Command

To run the threatq:sync-export command, complete the following steps:

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Run the following command appended by the necessary parameters, as described in threatq:sync-export Parameters:

```
sudo ./artisan threatq:sync-export
```

4. Review the Output and Sync report; see threatq:sync-export Output and Sync Report.

Running the threatq:sync-import Command

To run the threatq:sync-import command, complete the following steps:

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Run the following command appended by the necessary parameters, as described in Running the threatq:sync-import Command:

```
sudo ./artisan threatq:sync-import
```

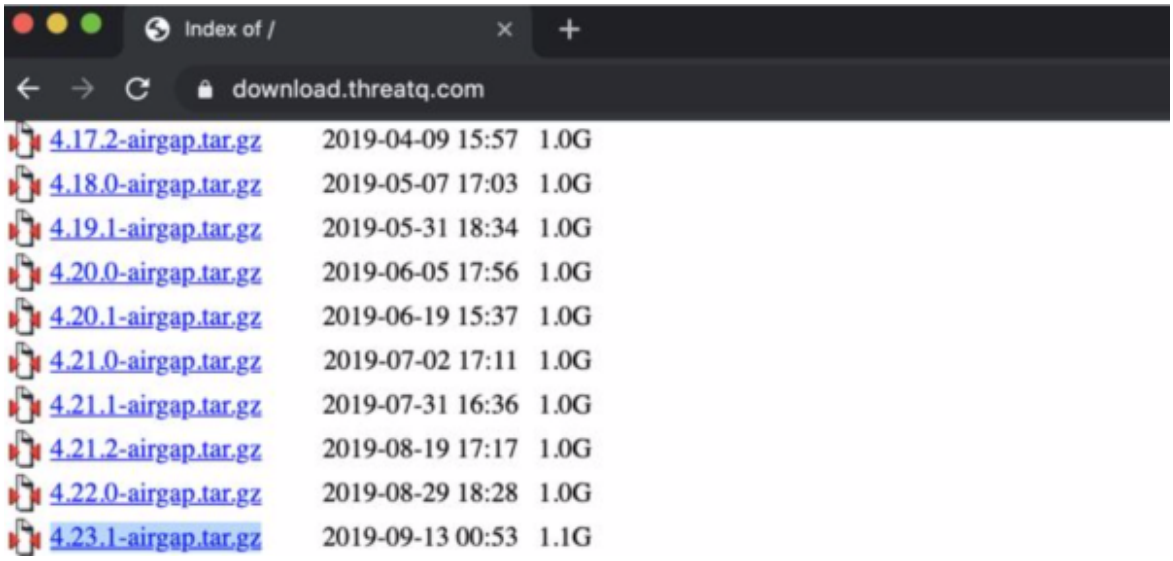
4. Review the Output and Sync report; see threatq sync-import File Output and Sync Report.

Upgrading an Air Gapped ThreatQ Instance

Contact ThreatQ Support if you encounter any issues during the upgrade or require assistance.

1. Log into the ThreatQ download repository, https://download.threatq.com, using your YUM credentials.

2. Locate and download the appropriate airgap upgrade file.



3. Open the CLI of the device to upgrade and run the following:

```
mkdir /var/tmp/upgrade
```

4. Copy the upgrade file you downloaded in step 2 to the newly created directory `/var/tmp/upgrade` using the scp client of your choice.
5. Return to the CLI of the device and confirm that the upgrade file is present.
6. Use the following commands to unpack and run the upgrade file:

```
sudo su -
screen -S threatq
cd /var/tmp/upgrade
ls -al
tar -xzvf /var/tmp/upgrade/<upgrade filename>
/var/tmp/upgrade/upgrade.sh
```

7. Allow the upgrade process to complete. When complete, the output should resemble the following:

```
Installed:
  chrony.x86_64 0:3.2-2.el7
  device-mapper-event.x86_64 7:1.02.149-10.el7_6.7
  device-mapper-event-libs.x86_64 7:1.02.149-10.el7_6.7
  device-mapper-persistent-data.x86_64 0:0.7.3-3.el7
  dnsmasq.x86_64 0:2.76-7.el7
  gnutls.x86_64 0:3.3.29-9.el7_6
  gsettings-desktop-schemas.x86_64 0:3.28.0-2.el7
  libXfont.x86_64 0:1.5.4-1.el7
  libgnome-keyring.x86_64 0:3.12.0-1.el7
  libgudev1.x86_64 0:219-62.el7_6.6
  libldb.x86_64 0:1.3.4-1.el7
  librabbitmq-devel.x86_64 0:0.8.0-2.el7
  libtalloc.x86_64 0:2.1.13-1.el7
  libtdb.x86_64 0:1.3.15-1.el7
  libtevent.x86_64 0:0.9.36-1.el7
  libtirpc.x86_64 0:0.2.4-0.15.el7
  libzip-last.x86_64 0:1.1.3-1.el7.remi
  lm_sensors.x86_64 0:3.4.0-6.20160601gitf9185e5.el7
  lvm2.x86_64 7:2.02.180-10.el7_6.7
  lvm2-libs.x86_64 7:2.02.180-10.el7_6.7
  mlocate.x86_64 0:0.26-8.el7
  net-snmp-libs.x86_64 1:5.7.2-37.el7
  net-snmp-utils.x86_64 1:5.7.2-37.el7
  nettle.x86_64 0:2.7.1-8.el7
  postgresql-libs.x86_64 0:9.2.24-1.el7_5
  python-markdown.noarch 0:2.4.1-2.el7
  rpcbind.x86_64 0:0.2.0-47.el7
  samba-common.noarch 0:4.8.3-4.el7
  trousers.x86_64 0:0.3.14-2.el7

Complete!
[root@support02 upgrade]#
[root@support02 upgrade]#
[root@support02 upgrade]#
```

If your terminal session should end prematurely at any point during the upgrade, you can return to it by logging back into the CLI and running the command below.

```
screen -r threatq
```

Backup and Restore

The following describes how to back up and restore a ThreatQ instance.

ThreatQ Backup

Before performing a backup of a ThreatQ instance, note the following:

- The backup process stops and starts all ThreatQ services automatically in order to prevent modifications to the file system and database. Requests made during this time are queued and resumed once the backup process completes.
- The time it takes to back up ThreatQ depends primarily on the size of the database. For this reason, we recommend performing a backup when system availability is not critical, such as during a scheduled maintenance window.
- The resulting backup file can be large. We recommend that you write it to a mounted drive or file location rather than the local file system. For instructions on how to mount a network-available drive, contact ThreatQ Support. If the backup file must be stored locally, you should move it off the local file system at the earliest opportunity.
- By default, the system creates a backup of the threat intelligence data index required for improved search performance and includes it in the backup file. This operation may take hours. You can omit this portion of the backup by running the backup command with the --exclude-solr option. However, this means that your threat intelligence data must be re-indexed during or after the restore process.

Backing Up a ThreatQ Instance

By default, the system creates a backup of the threat intelligence data index required for improved search performance and includes it in the backup file. This operation may take hours. You can omit this portion of the backup by running the backup command with the --exclude-solr option. However, this means that your threat intelligence data must be re-indexed during or after the restore process.

Before you begin, refer to ThreatQ Backup.

To perform a ThreatQ backup:

1. SSH to the ThreatQ command line and elevate your user privilege to root or sudo.
2. Change the directory to **/var/www/api**.
3. Choose one of the following options:
   - To create a backup that includes a Threat Library re-index, run the following command: `sudo php artisan threatq:backup`
   - To create a backup that excludes a Threat Library re-index, run the following command: `sudo php artisan threatq:backup --exclude-solr`
4. When prompted, provide the **root mysql** password you configured during first boot.

   You will only be prompted for a password and file path with the first initial backup. You will not be prompted for either of these items for any subsequent backups. Contact ThreatQ Support if you need to update either of these items.

5. Provide the path to the file location where you want to create the backup.

The script generates a backup file in the specified file location. The name of the file will be **threatq_backup_x.x.x_yyyy-mm-dd.tgz**, where **x.x.x** is the TQ version and **yyyy-mm-dd** is the date when the backup was performed.

ThreatQ Restore

To restore from a ThreatQ backup, note the following:

- The target machine must be an existing ThreatQ instance running the same version of the instance captured in the backup.
- The restore process completely overwrites the current installation.
- The backup file needs to be accessible by the target ThreatQ instance, either locally or on a mounted drive.
- The backup file will be unzipped in the same directory where it resides. Ensure that the available disk has sufficient space to hold both the backup archive and the extracted directory. The extracted directory can be removed after the restore is complete.
- Depending on the size of the instance being restored, the process can take a while.
- The machine running the target ThreatQ instance automatically restarts once the restore process is complete.

How to Restore from a ThreatQ Backup

Before you begin, refer to ThreatQ Restore.

To restore from a ThreatQ backup, perform the following procedure on the target ThreatQ instance.

1. Complete the first boot process on the new host by navigating to its IP address in a web browser and entering your credentials. If this step is not completed, the remaining steps are not successful.
2. SSH to the command line and elevate your user privileges to root or sudo.

3. Verify that you have the necessary utilities in place by running: **yum install policycoreutils-python-2.2.5-20.el7.x86_64**.
4. Change directory to **/var/www/api**.
5. Issue the following commands:
   - **php artisan threatq:restore </path/to/backup_file>**
   - **php artisan threatq:update-events**
6. When prompted, provide the root mysql password you configured during first boot.
7. If the backup file does not include the intelligence data index required for improved search performance, the system prompts you to either allow an automatic re-index or manually perform it later.

   This operation may take hours.

8. After the restore completes, you should reboot the target ThreatQ system to ensure that the system processes start up correctly.

Command Line Interface (CLI)

You can use the CLI to perform tasks and initiate specific platform processes.

Important Notes

- You should SSH into your ThreatQ installation as root or have sudo permission.
- Some CLI commands require you to be in a specific directory to execute. Review the help center topic for each command before running.
- Most CLI commands require that the ThreatQ application be placed into maintenance mode before proceeding. Placing the application in maintenance mode allows you to perform operations which would be delayed or otherwise impeded by regular API operation. Review the Maintenance Mode topic before executing CLI commands.

  ### Related Topics

  - Maintenance Mode
  - ThreatQ Purge Command
  - Command Reference Table

Maintenance Mode

Command Line Interface (CLI) commands and other processes, such as backup and restore, require that you place the ThreatQ application into maintenance mode. Placing the application in maintenance mode allows you to perform operations which would be delayed or otherwise impeded by regular API operation.

Some CLI commands will automatically place the ThreatQ application into maintenance mode when executed. The help center topics for these com-

mands will indicate if the command will automatically place the ThreatQ application into maintenance mode.

Placing the ThreatQ Application into Maintenance Mode

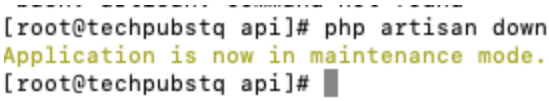
1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Run the following command:

```
sudo php artisan down
```

The platform will now be in maintenance mode.



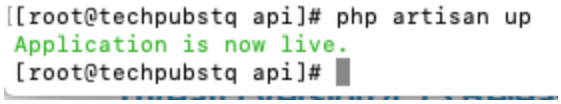
Taking the ThreatQ Application out of Maintenance Mode

The following steps assume you are already in the CLI. If not, complete steps 1-2 from above before proceeding.

1. While under the /var/www/api directory, run the following command:

```
sudo php artisan up
```

The platform will now be out of maintenance mode.



ThreatQ Purge Command

Read this topic carefully before running the ThreatQ Purge Command. After running this command, your threat intelligence data cannot be recovered.

The ThreatQ Purge command will **permanently** delete all object-related threat intelligence data from your ThreatQ installation, including audit logs. It will maintain any configuration-related settings, such as expiration, scoring, and so on.

Running the ThreatQ Purge Command

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Place the application into maintenance mode - see the Maintenance Mode topic.
4. Run the following command:

```
sudo php artisan threatq:purge-threat-intel-
ligence
```

5. You will be presented the following prompt:

```
You are about to erase all of your data, are
you sure?
```

6. Enter **Yes** or **No**.
7. Bring the application out of maintenance mode - see the Maintenance Mode topic.

Auto Configuration MariaDB Command

The Auto Configuration MariaDB command will execute a script that will update your MariaDB configurations based on your available system resources. The script is executed automatically during the platform install/upgrade process but can executed manually by using the command below. You will typically use this command after making a change to the size of your ThreatQ instance or system memory.

MariaDB will need to be restarted after the script has completed its updates.

```
/etc/my.cnf.d/config_gen/mysql_config_generator
```

Command Reference Table

The table below contains a list of Command Line Interface (CLI) commands available for the ThreatQ application.

Command	Topic
Platform Configuration	
Auto Configuration MariaDB Script	• Auto Configuration MariaDB Command
System Objects	
System ThreatQ Purge	• ThreatQ Purge Command

Command	Topic
Feeds	
Add/Upgrade CDF	• Adding/Upgrading CDF Command
Source Consolidation	• Source Consolidation Command
Source Merge	• Source Merge Command
Historic Pull	• General Historic Pull Commands
iSight Historic Pull	• iSight Historic Pull Command
User Management	
Reset User Password	• Resetting User Passwords from the Command Line
TLP	
Update TLP Designations	• Update TLP Schema using TLP Default - Command
Convert TLP	• Convert TLP Command
AirGap Data Sync	
Airgap Import	• Running the threatq:sync-import Command
Airgap Export	• Running the threatq:sync-export Command